Communication Complexity of Remote State Preparation

by

Shima Bab Hadiashar

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization - Quantum Information

Waterloo, Ontario, Canada, 2014

© Shima Bab Hadiashar 2014

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Superdense coding and quantum teleportation are two phenomena which were not possible without prior entanglement. In superdense coding, one sends n bits of information using $\frac{n}{2}$ qubits in the presence of shared entanglement. However, we show that n bits of information cannot be sent with less than n bits of communication in LOCC protocols even in the presence of prior entanglement. This is an interesting result which will be used in the rest of this thesis.

Quantum teleportation uses prior entanglement and classical communication to send an unknown quantum state. Remote state preparation (RSP) is the same distributed task, but in the case that the sender knows the description of the state to be sent, completely. We study the communication complexity of approximate remote state preparation in which the goal is to prepare an approximation of the desired quantum state. Jain showed that the worst-case error communication complexity of RSP can be bounded from above in terms of the maximum possible information in an encoding [18]. He also showed that this quantity is a lower bound for communication complexity of exact remote state preparation [18].

In this thesis, we characterize the worst-case error and average-case error communication complexity of remote state preparation in terms of non-asymptotic information-theoretic quantities. We also utilize the bound we derived for the communication complexity of LOCC protocols in the first part of the thesis, to show that the average-case error communication complexity of RSP can be much smaller than the worst-case.

Acknowledgements

I would like to express my deep gratitude to my supervisor, Ashwin Nayak, for continuous support, many fruitful discussions, and his comments on the draft of this thesis. I also like to thank Renato Renner for extremely helpful discussion in the beginning of this work, and Marco Tomamichel for fruitful discussions during my internship in National University of Singapore. I would also like to thank the readers of this thesis, Debbie Leung and Robert Konig, for their valuable comments on my thesis. I want to thank my friends in IQC, specially Sadegh Raeisi, for their continuous help during writing this thesis.

I am deeply grateful to my wonderful parents for their unconditional love and support. Thank you both very much, you are far beyond any appreciation!

At the end, I would like to extend my especial thank to my friend and beloved, my husband, Ala Shayeghi, whose supports, guidance and encouragements were endless. Ala, I am sure that I would not have finished this thesis without your support.

Dedication

This thesis is dedicated to Ala, my husband, and my parents in appreciation of all their support throughout this journey.

Table of Contents

List of Tables

Chapter 1

Introduction

It is known that a general superposition over n qubits can carry a large amount of information which cannot be accessed by an observer. In [14], Holevo showed that the amount of accessible information in n qubits is at most n bits. This implies that sending qubits instead of classical bits does not yield any decrease in the communication complexity of transmitting an n bit string. However, quantum communication is not the only resource in quantum computing. Another resource that can be utilized in a quantum protocol is shared entanglement. Quantum teleportation [1] and superdense coding [4] are two significant examples where prior entanglement allows us to do certain tasks better than classical protocols.

Superdense coding is the process of sending n classical bits of information using $n/2$ qubits in the presence of prior shared entanglement. The question which arises is whether prior entanglement can lead to additional reduction in the communication cost. In [26], Nayak and Salzman showed that using shared entanglement, the communication cost of transmitting classical messages cannot decrease more. In particular, suppose that Alice wants to send a uniformly random n bit string to Bob using an arbitrary entanglement-assisted quantum protocol with success probability $p > 0$. Then, she has to send at least $\frac{1}{2}(n + \log p)$ qubits during the protocol, independent of the number of qubits Bob sends to Alice. However, we show that this reduction can happen only when quantum communication and shared entanglement is utilized in a protocol simultaneously. In other words, using prior entanglement while we are restricted to classical communication, one still requires at least n bits of communication to send n bits of information.

The second process which is not achievable without entanglement is quantum teleportation [1]. In quantum teleportation, one sends a qubit to another person using two classical bits of communication and some previously shared entanglement. In order to teleport one qubit, two classical bits of communication and a maximally entangled pair of qubits is necessary and sufficient, and there is no trade-off between the number of communication bits and shared entangled bits. Note that in quantum teleportation, the sender, called Alice, does not have any description of the quantum state she wants to send.

In [24], Lo introduced a similar distributed task in which Alice knows a classical description of the quantum state. This task is called “remote state preparation” abbreviated as RSP. In particular, remote state preparation is the process involving two parties Alice and Bob with some shared entangled qubits, Alice is given the description of a state, $Q(x)$, chosen from a subset of quantum states $\{Q(1), \ldots, Q(n)\}$, and their goal is to prepare that quantum state on Bob's side using an LOCC (Local Operations and Classical Communication) protocol. An RSP protocol is said to be *oblivious to Bob* if he can get information about the prepared state not more than is contained in a single copy of the state [23]. A relaxed version of RSP is *approximate remote state preparation* (ARSP) in which preparing an approximation σ_x of a quantum state $Q(x)$ is desired. We define the error of a protocol for approximate remote state preparation in terms of the fidelity between $Q(x)$ and σ_x. We say a protocol has *worst-case error* at most ϵ, if for every $x \in \{1, \ldots, n\}$, $\mathrm{F}(Q(x), \sigma_x) \geq \sqrt{1-\epsilon^2}$. Similarly, a protocol has *average-case error* at most ϵ with respect to a probability distribution p, if $\sum_{x=1}^{n} p_x \mathrm{F}(Q(x), \sigma_x) \geq \sqrt{1-\epsilon^2}$.

In [24], Lo gave several examples of ensembles which can be remotely prepared using a one-way communication protocol with classical communication cost less than quantum teleportation. However, he conjectured that to prepare N arbitrary pure qubit states remotely, Alice needs to send the same number of classical bits as in quantum teleportation i.e., $2N$ classical bits [24].

In [2], Bennett *et al.* showed that in the presence of a large amount of shared entanglement, Alice can prepare general quantum states in Bob's side with the asymptotic classical communication rate of one bit per qubit. This amount of classical communication from Alice to Bob is also necessary [24] by causality. They also showed that unlike quantum teleportation, there is a trade-off between the communication cost and the amount of entanglement in remote state preparation. In particular, it was shown that at the cost of using more entanglement, the communication cost of preparing a one-qubit state ranges from one bit in the high entanglement limit to an infinite number of bits in the case of no previously shared entanglement [2]. In addition, they suggested that Lo's conjecture is true in a more restricted setting, such as when the protocol is *faithful*[1] and oblivious to Bob [2].

[1] A protocol is said to be *faithful* if it is exact and deterministic.

In [11], Devetak and Berger found an analytic expression for the trade-off curve between shared entangled bits and classical communication bits of *teleportation based RSP protocols* on the *low- entanglement* region (< 1 singlet state per qubit), and they conjectured that teleportation based protocols are optimal among all low-entanglement protocols.

Later in [23], Lo's conjecture was proved for an special case. In particular, Leung and Shor proved that if a one-way RSP protocol for a *generic ensamble* of pure states is faithful and oblivious to Bob, then it must uses at least as much classical communication as teleportation. A *generic ensemble* is an ensemble of states whose density matrices span the operators in the input Hilbert space [23].

Hayashi *et al.* [13] showed that in order to remotely prepare one qubit in a general state using a one-way faithful but not necessarily oblivious protocol, Alice needs to send 2 classical bits to Bob as in teleportation.

Berry and Sanders [5] studied ARSP of an ensemble $\mathcal{E}$ of mixed states which are entangled with some other system on Alice's part such that their entanglement with other systems does not change significantly, and showed that approximate remote state preparation with arbitrary small average-case error ϵ can be done asymptotically using communication per prepared state arbitrarily close to the Holevo information $\chi(\mathcal{E})$[2] of the ensemble.

Later in [3], Bennett *et al.* proved that approximate remote state preparation with small worst-case error ϵ requires asymptotic rate of one bit of classical communication per qubit from Alice to Bob. They also showed that this amount of classical communication is sufficient. Moreover, they derived the exact trade-off curve between shared entangled bits and classical communication bits for an arbitrary ensemble of candidate states.

In [18], Jain studied remote state preparation in one-shot scenario. He considered the total communication cost instead of the rate of communication in the case that there is no limit on the amount of entanglement. He showed that the communication cost required for exact remote state preparation is at least $\mathsf{T}(Q)/2$ and the RSP with worst-case error at most ϵ can be solved with communication at most $\frac{8}{\left(1-\sqrt{1-\epsilon^2}\right)^2}(4\mathsf{T}(Q)+7)$, where $\mathsf{T}(Q)$[3] denotes the maximum possible information in an encoding Q. All these works on remote state preparation are summarized in Table 1.1 .

In this work, we characterize the communication complexity of remote state preparation in two different cases. First, we consider RSP with average-case error at most ϵ, and bound its communication complexity by the notion of smooth max-information[4] Bob has about

[2] An exact definition can be found in Section 2.2.4.

[3] An exact definition can be found in Section 2.2.4.

[4] We define this formally in Section 2.2.4.

Protocol Type	Conditions	Entanglement	Classical Communication
Faithful RSP [2]	an arbitrary state, one-way communication, in asymptotics	high entanglement	$= 1$ classical bit per qubit
Faithful RSP [13]	one pure qubit in a general state, one-way communication	$= 1$ ebit(singlet) per qubit	$= 2$ classical bit
Faithful and oblivious RSP [23]	a generic ensemble of pure states, one-way communication	$= 1$ ebit(singlet) per qubit	$= 2$ classical bit per qubit
ARSP with small average-case error [5]	an ensemble $\mathcal{E}$ of mixed states preserving their entanglement, one-way communication, in asymptotics	no limit	$\approx \chi(\mathcal{E})$ classical bits per prepared state
ARSP with small worst-case error [3]	an arbitrary pure state, two-way communication, in asymptotics	$= 1$ ebit(singlet) per qubit	$= 1$ classical bit per qubit from Alice to Bob
Exact RSP [18]	an arbitrary state, two-way communication, in one-shot scenario	no limit	$\geq \mathsf{T}(Q)/2$
ARSP with worst-case error ϵ [18]	an arbitrary state, one-way communication, in one-shot scenario	no limit	$\leq \frac{8}{\left(1-\sqrt{1-\epsilon^2}\right)^2}(4\mathsf{T}(Q)+7)$

Table 1.1: A summary of previous works on communication cost of Remote State Preparation

Alice's input. Then, we consider RSP with worst-case error at most ϵ, and give lower and upper bounds for its communication complexity in terms of smooth max-relative entropy and show that our bounds are $\log\log N$ times tighter than that of [18]. Our results about remote state preparation problem are summarized in Theorem 1.0.1.

Theorem 1.0.1. *For any finite set S, and function $\mathsf{Q} : S \to \mathsf{D}(\mathcal{H})$, , let p be a probability distribution over S and $\rho_{AB}(p) \in \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ be the bipartite quantum state $\rho_{AB}(p) = \sum_{x\in S} p_x |x\rangle\langle x|_A \otimes Q(x)_B$. Then,*

1. *For some fixed $\epsilon \in (0,1]$, we have*

$$\mathrm{I}^{\epsilon}_{\max}(A:B)_{\rho(p)} \quad \leq \quad \mathsf{Q}^*_p(\mathrm{RSP}(S,Q,\epsilon)) \quad \leq \quad \mathrm{I}^{\frac{\epsilon}{2\sqrt{1+\epsilon^2}}}_{\max}(A:B)_{\rho(p)} + \mathrm{O}(1) \ ,$$

   where $\mathsf{Q}^*_p(\mathrm{RSP}(S,Q,\epsilon))$ denotes the average-case error communication complexity of approximate remote state preparation of the set of quantum states $\{Q(x) : x \in S\}$.

2. *For some fixed $\epsilon \in (0,1]$, we have*

$$\begin{aligned}\min_{\sigma\in\mathsf{D}(\mathcal{H})} \max_{x\in S} \mathrm{D}^{\sqrt{2(\epsilon^2+\delta)}}_{\max}(Q(x)\|\sigma) + \mathrm{O}(1) \quad &\leq \quad \mathsf{Q}^*(\mathrm{RSP}(S,Q,\epsilon)) \\ &\leq \quad \min_{\sigma\in\mathsf{D}(\mathcal{H})} \max_{x\in S} \mathrm{D}^{\frac{\epsilon}{\sqrt{1+\epsilon^2}}}_{\max}(Q(x)\|\sigma) + \mathrm{O}(1) \ ,\end{aligned}$$

   for any $0 < \delta < \epsilon$, where $\mathsf{Q}^*(\mathrm{RSP}(S,Q,\epsilon))$ the worst-case error communication complexity of approximate remote state preparation of the set of quantum states $\{Q(x) : x \in S\}$.

Note that smooth max-information and smooth max-relative entropy are continuous in ϵ.

Also, we show that the communication cost may reduce dramatically by allowing more error and considering average-case error instead of worst-case error. In particular, We show that for every $\epsilon \in [0, \frac{1}{\sqrt{2}})$, there exists a set of quantum states for which there is a $\log N$ gap between the worst-case error and average-case error remote preparation of that set. In addition, for a special set of quantum states, we derive the gap between the worst-case error and average-case error communication complexity in terms of ϵ, and show that the more the probability distribution drops quickly, the bigger the gap between worst-case and average-case error can be.

The organization of this thesis is as follows. In Chapter 2, we provide some background materials to review existing concepts and fix notation and terminology through out the thesis. In Section 2.1, we review some relevant results of Linear Algebra including Hilbert space and operators. Then in Section 2.2,we introduce some basic notions in quantum computing like quantum states and quantum operations, some quantum information concepts like different kinds of entropy and information, and quantum protocols and communication complexity.

In Chapter 3, we show that in any one-way LOCC protocol sending a uniformly random n bit string with success probability p, the communication is at least $n + \log p$ bits (Section 3.2). We also extend this result to general LOCC protocols in Section 3.3. This is an interesting result by itself which we need to utilize to show the gap between the worst-case error and average-case error communication complexity.

In Chapter 4, we first define approximate remote state preparation(ARSP) formally. Then in Section 4.1, we explain a protocol for this problem, and in Section 4.2 and Section 4.3 we give bounds on average-case error and worst-case error communication complexity of ARSP, respectively. Finally, we compare our results with previous works in Section 4.4.

The thesis ends with a summary of our results and an outlook in Chapter 5.

Chapter 2

Preliminaries

2.1 Mathematical Preliminaries

2.1.1 Hilbert space

A *Hilbert space* is a vector space over the complex numbers equipped with an inner product and an induced norm. In this thesis, we denote Hilbert spaces by capital script letters like $\mathcal{H}$, $\mathcal{K}$ and $\mathcal{M}$. The *dual space* $\mathcal{H}^*$ is the space of all continuous linear functions from $\mathcal{H}$ to $\mathbb{C}$. In the following, we use the Dirac bra-ket notation to show elements of a Hilbert space and its dual. We denote every element of a Hilbert space $\mathcal{H}$ by a ket, e.g. $|\psi\rangle \in \mathcal{H}$, and every element of the dual space $\mathcal{H}^*$ by a bra, e.g. $\langle\psi|$.

Let $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ be two elements of Hilbert space $\mathcal{H}$. The inner product of $|\psi\rangle$ and $|\phi\rangle$ is denoted by

$$\langle\psi|\phi\rangle \coloneqq \langle|\psi\rangle, |\phi\rangle\rangle \ ,$$

which is also called the bra-ket product. The bra-ket product has the following properties which are derived directly from properties of the underlying inner-product.

1. $\langle\psi|\phi\rangle \quad = \quad \overline{\langle\phi|\psi\rangle}$

2. If $|\phi\rangle = \alpha_1|\xi_1\rangle + \alpha_2|\xi_2\rangle$ for some $|\xi_1\rangle, |\xi_2\rangle \in \mathcal{H}$ and $\alpha_1, \alpha_2 \in \mathbb{C}$, then

$$\langle\psi|\phi\rangle \quad = \quad \alpha_1\langle\psi|\xi_1\rangle + \alpha_2\langle\psi|\xi_2\rangle \ , \text{ and}$$

$$\langle\phi|\psi\rangle \quad = \quad \overline{\alpha_1}\langle\xi_1|\psi\rangle + \overline{\alpha_2}\langle\xi_2|\psi\rangle \ .$$

3. For every $|\phi\rangle \in \mathcal{H}$, $\langle\phi|\phi\rangle \geq 0$.

The inner product can be used to define a norm in a Hilbert space. The Euclidean norm of an element $|\psi\rangle \in \mathcal{H}$ is defined as

$$\||\psi\rangle\| \quad := \quad \sqrt{\langle\psi|\psi\rangle} \ .$$

Let $\mathcal{S}$ be the set of vectors $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_i\rangle \in \mathcal{H}$. We define the span of $\mathcal{S}$ as

$$\mathrm{span}\{\mathcal{S}\} \quad = \quad \mathrm{span}\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{\mathrm{i}}\rangle\} \quad := \quad \{\sum_{k=1}^{i} a_k|\psi_k\rangle : a_k \in \mathbb{C}\} \ .$$

Two vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ are said to be orthogonal, if and only if $\langle\phi|\psi\rangle = 0$. A set of unit vectors $\mathcal{S} = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\} \subset \mathcal{H}$ is called a basis for $\mathcal{H}$, if $\mathrm{span}\{\mathcal{S}\} = \mathcal{H}$, and it is called an orthonormal basis if and only if it is a basis and its elements are mutually orthogonal. Note that if $\mathcal{S}$ is an orthonormal basis for $\mathcal{H}$, then $|\mathcal{S}| = \dim(\mathcal{H})$.

Tensor product space

Let $\mathcal{H}$ and $\mathcal{H}'$ be two Hilbert spaces of dimension m and n, respectively. Then, $\mathcal{H}\otimes\mathcal{H}'$, the tensor product of $\mathcal{H}$ and $\mathcal{H}'$, is an mn dimensional Hilbert space. Let $\{|h_i\rangle\}_{i=1}^{m}$ and $\{|h_i'\rangle\}_{i=1}^{n}$ be orthonormal bases for $\mathcal{H}$ and $\mathcal{H}'$, then $\{|h_i\rangle \otimes |h_j'\rangle : i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}\}$ is an orthonormal basis for $\mathcal{H}\otimes\mathcal{H}'$. For vectors $|\psi\rangle \in \mathcal{H}$ and $|\psi'\rangle \in \mathcal{H}'$, $|\psi\rangle \otimes |\psi'\rangle \in \mathcal{H}\otimes\mathcal{H}'$ refers to the vector for which

$$(\langle h_i| \otimes \langle h_j'|)(|\psi\rangle \otimes |\psi'\rangle) \quad = \quad \langle h_i|\psi\rangle\langle h_j'|\psi'\rangle \ .$$

It is also true that

$$\mathcal{H}\otimes\mathcal{H}' \quad := \quad \mathrm{span}\left\{\{|\psi\rangle \otimes |\psi'\rangle : |\psi\rangle \in \mathcal{H}, |\psi'\rangle \in \mathcal{H}'\}\right\} \ .$$

We usually abbreviate $|\psi\rangle \otimes |\psi'\rangle$ as $|\psi\rangle|\psi'\rangle$.The following lemma will be useful in the following chapters.

Lemma 2.1.1. *Let $\mathcal{H}$ and $\mathcal{H}'$ be two Hilbert spaces, and $|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}'$ be a quantum state in the tensor product space $\mathcal{H}\otimes\mathcal{H}'$. Then, $|\psi\rangle$ can be written as*

$$|\psi\rangle \quad = \quad \sum_i \sqrt{\lambda_i}|a_i\rangle|b_i\rangle \ , \tag{2.1.1}$$

where $\{|a_i\rangle\}_i$ and $\{|b_i\rangle\}_i$ are orthonormal sets of states in $\mathcal{H}$ and $\mathcal{H}'$, respectively, and all λ_i are non-negative real numbers with $\sum_i \lambda_i = 1$.

Equation (2.1.1) is called the *Schmidt decomposition* of the vector $|\psi\rangle$.

2.1.2 Operators in Hilbert spaces

Linear operators

Let $\mathcal{H}$ and $\mathcal{K}$ be two Hilbert spaces. An operator $A : \mathcal{H} \to \mathcal{K}$ is called a Linear Operator if :

1. For any $a \in \mathbb{C}$ and $|\psi\rangle \in \mathcal{H}$: $(aA)|\psi\rangle = aA|\psi\rangle$
2. For any two vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}$: $A(|\psi\rangle + |\phi\rangle) = A|\psi\rangle + A|\phi\rangle$

We denote the set of all linear operators from $\mathcal{H}$ to $\mathcal{K}$, by $\mathsf{L}(\mathcal{H}, \mathcal{K})$. In the case that $\mathcal{H} = \mathcal{K}$, we avoid writing the Hilbert space twice and denote the set of linear operators as $\mathsf{L}(\mathcal{H})$ instead of $\mathsf{L}(\mathcal{H}, \mathcal{H})$.

Every linear operator$A \in \mathsf{L}(\mathcal{H}, \mathcal{K})$, can be represented as a matrix. Let $\{|e_i\rangle\}$ and $\{|e'_i\rangle\}$ be orthonormal bases for $\mathcal{H}$ and $\mathcal{K}$, respectively. The linear operator can be uniquely decomposed as

$$A = \sum_{i,j} \langle e'_i|A|e_j\rangle |e'_i\rangle\langle e_j| \ ,$$

so it can be represented as a $\dim(\mathcal{H}) \times \dim(\mathcal{K})$ matrix in these bases such that $[A]_{ij} = \langle e'_i|A|e_j\rangle$.

For every operator $A \in \mathsf{L}(\mathcal{H}, \mathcal{K})$, three additional operators, $\bar{A} \in \mathsf{L}(\mathcal{H}, \mathcal{K})$ and $A^T, A^* \in \mathsf{L}(\mathcal{K}, \mathcal{H})$, are defined as follows:

- The operator $\overline{A} \in \mathsf{L}(\mathcal{H}, \mathcal{K})$ is the operator with the matrix representation

  $$[\overline{A}]_{ij} = \overline{[A]_{ij}} \text{ , for all } i, j \ ,$$

  and it is called the entry-wise conjugate operator of A.

- The operator $A^T \in \mathsf{L}(\mathcal{K}, \mathcal{H})$ is the operator with the matrix representation

  $$[A^T]_{ij} = [A]_{ji} \text{ , for all } i, j \ ,$$

  and it is called the transpose operator of A.

- The operator $A^* \in \mathsf{L}(\mathcal{K}, \mathcal{H})$ is the operator defined as

  $$A^* = \overline{A^T} \ ,$$

  and is called the *adjoint operator* of A.

Trace and inner product of operators

Let $A \in \mathsf{L}(\mathcal{H})$ be a linear operator. The *trace* of A is defined as the sum of the diagonal entries of its matrix representation, i.e.

$$\mathrm{Tr}(A) \quad := \quad \sum_i [A]_{ii} \ .$$

The trace function has the *cyclic property* which means that for any choice of Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ and operators $A \in \mathsf{L}(\mathcal{K}, \mathcal{H})$ and $B \in \mathsf{L}(\mathcal{H}, \mathcal{K})$,

$$\mathrm{Tr}(AB) \quad = \quad \mathrm{Tr}(BA) \ .$$

Using the trace function, an inner product on $\mathsf{L}(\mathcal{H}, \mathcal{K})$ can be defined as

$$\langle A, B \rangle \quad := \quad \mathrm{Tr}(A^* B) \ \text{ for all } A, B \in \mathsf{L}(\mathcal{H}, \mathcal{K}) \ .$$

It can be easily verified that this definition satisfies the required properties of an inner product.

Eigenvalues and eigenvectors of an operator

Let $A \in \mathsf{L}(\mathcal{H})$ be a linear operator on a Hilbert space $\mathcal{H}$ and $|\psi\rangle \in \mathcal{H}$ be a non-zero vector such that

$$A|\psi\rangle \quad = \quad \lambda|\psi\rangle \ ,$$

for some $\lambda \in \mathbb{C}$. The vector $|\psi\rangle$ is called an eigenvector of A and λ is an eigenvalue of A.

Normal, Hermitian, positive semi-definite and density operators

- For some Hilbert space $\mathcal{H}$, an operator $A \in \mathsf{L}(\mathcal{H})$ is *normal* if and only if $AA^* = A^*A$.
- An operator $A \in \mathsf{L}(\mathcal{H})$ is *Hermitian* if and only if $A = A^*$. Note that any Hermitian operator is also a normal operator.
- An operator $A \in \mathsf{L}(\mathcal{H})$ is *positive semi-definite* if and only if A is Hermitian and has non-negative eigenvalues. Let $\mathsf{Pos}(\mathcal{H})$ denotes the set of all positive semi-definite operators in $\mathcal{H}$.
- An operator $A \in \mathsf{Pos}(\mathcal{H})$ is called a *density operator* if its trace is equal to 1. Let $\mathsf{D}(\mathcal{H})$ denote the set of density operators in Hilbert space $\mathcal{H}$. Note that the set $\mathsf{D}(\mathcal{H})$ is a compact and convex set.

Isometries and unitary operators

An operator $A \in \mathsf{L}(\mathcal{H}, \mathcal{K})$ is called an *isometry* if and only if $A^*A = \mathbb{1}$. Equivalently, we say that a linear operator A is an isometry if it preserves the Euclidean norm, i.e. $\|A|\psi\rangle\| = \||\psi\rangle\|$ for all $u \in \mathcal{H}$.

An isometry A which maps $\mathcal{H}$ to itself, i.e. $A \in \mathsf{L}(\mathcal{H})$ is called a *unitary operator* . We denote the set of all unitary operators in $\mathsf{L}(\mathcal{H})$ by $\mathsf{U}(\mathcal{H})$.

Spectral decomposition

One of the important operator decompositions is the *spectral decomposition.* This decomposition exists only for normal operators. The following theorem (Spectral theorem) gives the exact form of this decomposition.

Theorem 2.1.2. *Let $\mathcal{H}$ be a Hilbert space and let $A \in \mathsf{L}(\mathcal{H})$ be a normal operator. Suppose that $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$ are the eigenvalues of A. Then there exists an orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$ of $\mathcal{H}$ such that*

$$A \quad = \quad \sum_{i=1}^{n} \lambda_i |\psi_i\rangle\langle\psi_i| \ . \tag{2.1.2}$$

Equation (2.1.2) is called the *spectral decomposition* of the normal operator A. Note that in the spectral decomposition expression, each vector $|\psi_i\rangle$ is in fact an eigenvector of A corresponding to an eigenvalue λ_i.

Functions of normal operator

Let $\mathcal{H}$ be a Hilbert space. Using the spectral decomposition of normal operators, one can extend every function $f : \mathbb{C} \to \mathbb{C}$ to the set of normal operators in $\mathsf{L}(\mathcal{H})$. Suppose that f is a function on complex scalars and $A \in \mathsf{L}(\mathcal{H})$ is a normal operator with spectral decomposition $A = \sum_{i=1}^{n} \lambda_i |\psi_i\rangle\langle\psi_i|$. Then, one defines

$$f(A) \quad := \quad \sum_{i=1}^{n} f(\lambda_i) |\psi_i\rangle\langle\psi_i| \ .$$

2.1.3 The minimax theorem

The minimax theorem is a helpful rule used in game theory, statistics and etc, which provides conditions under which one can reverse a minimum and a maximum without changing the value of the expression containing them.

Theorem 2.1.3. *[30] Let A_1, A_2 be non-empty, convex and compact subsets of $\mathbb{R}^n$ for some positive integer n. Let $f : A_1 \times A_2 \to \mathbb{R}$ be a continuous function such that*

1. *$\forall a_2 \in A_2$, the set $\{a_1 \in A_1 : (\forall a'_1 \in A_1) f(a_1, a_2) \geq f(a'_1, a_2)\}$ is convex.*
2. *$\forall a_1 \in A_1$, the set $\{a_2 \in A_2 : (\forall a'_2 \in A_2) f(a_1, a_2) \leq f(a_1, {a'}_2)\}$ is convex.*

Then,

$$\max_{a_1 \in A_1} \min_{a_2 \in A_2} f(a_1, a_2) \quad = \quad \min_{a_2 \in A_2} \max_{a_1 \in A_1} f(a_1, a_2) \ .$$

2.2 Background in quantum computing

In this section, we first review some basic notions of quantum computing, such as quantum states, separability and entanglement. Then, we review notions of LOCC protocols and quantum communication complexity. At the end, we mention two types of non-asymptotic information-theoretic quantities, max-relative entropy and hypothesis testing entropy.

2.2.1 Some basic notions

In quantum computing, we model any physical system which may change over the time and has the ability of storing some amount of data as a *register*. In this thesis, we denote any register with capital letters, e.g. X, Y and Z. The state of a register X is modeled as a density operator and is called a *quantum state*.

Suppose that X is a register in the Hilbert space $\mathcal{H} \otimes \mathcal{K}$, and $\rho \in \mathsf{D}(\mathcal{H})$ is the quantum state of X. We say that X is a classical register if every possible state of X is a diagonal density operator in the standard basis. In addition, X is called a *classical-quantum* register, if ρ is classical in Hilbert space $\mathcal{H}$, i.e.

$$\rho \quad = \quad \sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \rho_x \ \ ,$$

where $n = \dim(\mathcal{H})$, the set $\{|x\rangle\}_x \in \{1, \ldots, n\}$ is the standard basis of $\mathcal{H}$ and $\rho_x \in \mathsf{D}(\mathcal{K})$ for all x.

Pure states and mixed states

A quantum state $\rho \in \mathsf{D}(\mathcal{H})$ is called a *pure state* if there exists a unit vector $|\psi\rangle \in \mathcal{H}$ such that

$$\rho \quad = \quad |\psi\rangle\langle\psi| \ ,$$

otherwise it is called a *mixed state* and it can be written as a convex combination of some pure states.

Separable and entangled states

A quantum state $\rho \in \mathsf{D}(\mathcal{H} \otimes \mathcal{K})$ is called *separable* on $\mathcal{H}$ and $\mathcal{K}$ if and only if there exist two sets of quantum states $\{\sigma_a \in \mathsf{D}(\mathcal{H}) : a = 1, \ldots, m\}$ and $\{\xi_a \in \mathsf{D}(\mathcal{K}) : a = 1, \ldots, m\}$ and a probability distribution p over m elements such that

$$\rho \quad = \quad \sum_{a=1}^{m} p_a \sigma_a \otimes \xi_a \ .$$

A quantum state is called *entangled* if it is not a separable state.

The partial trace and purification of a quantum state

Let $\rho_{AB} \in \mathsf{D}(\mathcal{H} \otimes \mathcal{K})$ be a bipartite state with parts A and B in Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, respectively. The linear mapping $\mathrm{Tr}_{\mathcal{K}} : \mathsf{L}(\mathcal{H} \otimes \mathcal{K}) \to \mathsf{L}(\mathcal{H})$ defined as

$$\mathrm{Tr}_{\mathcal{K}}(\rho_{AB}) \quad := \quad (\mathbb{1}_{\mathcal{H}} \otimes \mathrm{Tr})(\rho_{AB}) \ ,$$

is called the *partial trace* mapping over Hilbert space $\mathcal{K}$, and the quantum state $\rho_A = \mathrm{Tr}_{\mathcal{K}}(\rho_{AB})$ is called the *reduced state* of ρ_{AB}. Alternatively, one may denote the partial trace by $\mathrm{Tr}_B(\rho_{AB})$, in which the name of traced-out Hilber space is replaced by the name of the traced-out register. We may use either of these notations in this thesis.

Conversely, suppose that $\rho_A \in \mathsf{D}(\mathcal{H})$ is a quantum state in the Hilbert space $\mathcal{H}$. We say that $\rho_{AB} \in \mathsf{D}(\mathcal{H} \otimes \mathcal{K})$ is an *extension* of ρ_A if

$$\mathrm{Tr}_{\mathcal{K}}(\rho_{AB}) \quad = \quad \rho_A \ .$$

If ρ_{AB} is also a pure state, then it is called a *purification* of ρ_A on Hilbert space $\mathcal{H}$. It has been shown that any two purifications of a quantum state in the same Hilbert space can be transformed to each other by performing a unitary operator on the purification part [21]. This result is stated formally in the following theorem which is called *unitary equivalence of purifications*.

Theorem 2.2.1. *Let $\sigma \in \mathsf{D}(\mathcal{H})$ be a quantum state, and $|u\rangle, |v\rangle \in \mathcal{H} \otimes \mathcal{K}$ be any two purifications of σ in the Hilbert space $\mathcal{H}\otimes\mathcal{K}$. Then there exists a unitary operator $U \in \mathsf{U}(\mathcal{K})$ such that*

$$|u\rangle \quad = \quad (\mathbb{1} \otimes U)|v\rangle \ .$$

Quantum operations

A linear mapping $\Phi : \mathsf{L}(\mathcal{H}) \to \mathsf{L}(\mathcal{K})$ is *completely positive* if and only if

$$(\Phi \otimes \mathbb{1}_{\mathsf{L}(\mathcal{M})})(\rho) \in \mathsf{D}(\mathcal{K} \otimes \mathcal{M}) \ ,$$

for every choice of $\mathcal{M}$ and every quantum state $\rho \in \mathsf{D}(\mathcal{H} \otimes \mathcal{M})$. Moreover, Φ is *trace-preserving* if and only if

$$\mathrm{Tr}(\Phi(A)) \quad = \mathrm{Tr}(A) \ ,$$

for all Hermitian operators A.

A *quantum operation* (*quantum channel*) is a completely positive and trace-preserving linear mapping. A wide variety of evolutions of quantum states can be described by quantum operations.

Quantum operations have different representations. One of the important representations of a quantum operation is called *Kraus representation* which is given in the following theorem.

Theorem 2.2.2. *Let $\Phi : \mathsf{L}(\mathcal{H}) \to \mathsf{L}(\mathcal{K})$ be a quantum operation. There exists a collection of operators $\{A_a : a \in \Gamma\} \subset \mathsf{L}(\mathcal{H}, \mathcal{K})$ such that $\sum_{a\in\Gamma} A_a^* A_a = \mathbb{1}$, and*

$$\Phi(X) = \sum_{a\in\Gamma} A_a X A_a^* \ ,$$

for all $X \in \mathsf{L}(\mathcal{H})$.

The above expression is called *Kraus representation* and all A_a are called *Kraus operators* of quantum operation Φ.

Measurements

A *general measurement* of a register X (in Hilbert space $\mathcal{H}$) with the outcome set Γ is a collection of operators $\{E_a : a \in \Gamma\}$ such that for all $a \in \Gamma$, $E_a \in \mathsf{Pos}(\mathcal{H})$ and $\sum_a E_a = \mathbb{1}$.

Each E_a is called the *measurement operator* or *POVM element* associated with the outcome $a \in \Gamma$. Suppose that $\rho \in \mathsf{D}(\mathcal{H})$ is the state of register X initially. Then after performing such a measurement on register X, the outcome is an element $a \in \Gamma$ with probability

$$p(a) \quad = \quad \langle E_a, \rho \rangle \ ,$$

and the register X goes to the state

$$\frac{\sqrt{E_a}\rho\sqrt{E_a}}{\langle E_a, \rho \rangle} \ .$$

An *orthogonal projective measurement* is a measurement for which the measurement operators are orthogonal projection operators, i.e. $E_a^2 = E_a$ for all $a \in \Gamma$.

The following theorem states that any general measurement can be implemented by a unitary followed by an orthogonal projective measurement. The proof can be found in [29].

Theorem 2.2.3. *Let $\mathcal{H}$ be a Hilbert space and $\rho \in \mathsf{D}(\mathcal{H})$ be a quantum state. Any measurement described by measurement operators $\{E_a\}_{a=1}^m$ on ρ can be implemented as a unitary operator $U \in \mathsf{U}(\mathcal{H} \otimes \mathbb{C}^m)$, followed by an orthogonal projection $\{P_a\}_{i=a}^m$ acting on the state $\rho \otimes |\bar{0}\rangle\langle\bar{0}| \in \mathsf{D}(\mathcal{H} \otimes \mathbb{C}^m)$, where $|\bar{0}\rangle$ is a fixed state in $\mathbb{C}^m$, $P_a = \mathbb{1}_{\mathcal{H}} \otimes |a\rangle\langle a|$ for $a \in \{1, \ldots, m\}$, and U is chosen such that for all $|\phi\rangle \in \mathcal{H}$*

$$U|\phi\rangle|0\rangle \quad = \quad \sum_{a=1}^{m} \sqrt{E_a}|\phi\rangle|a\rangle \ .$$

In the next chapter, we utilize this theorem to study quantum states after performing a general measurement on them. Note that because of the special form of the orthogonal projection in this theorem, we can conclude that any general measurement can be implemented as a unitary operator followed by the orthogonal projection in the standard basis on $\log m$ qubits.

Also, one can define a measurement as a quantum channel. Suppose that the set $\{E_a : a \in \Gamma\}$ is the collection of POVM elements of a measurement with the outcome set Γ. Then, its corresponding quantum channel $\Phi : \mathsf{L}(\mathcal{H}) \to \mathsf{L}(\mathcal{H} \otimes \mathbb{C}^\Gamma)$ is defined as a quantum channel with Kraus operators $\{\sqrt{E_a} \otimes |a\rangle : a \in \Gamma\}$. In other words, for every $X \in \mathsf{L}(\mathcal{H})$,

$$\Phi(X) \quad = \quad \sum_{a \in \Gamma} (\sqrt{E_a} X \sqrt{E_a}) \otimes |a\rangle\langle a| \ .$$

The fidelity function

Let $P, Q \in \mathsf{Pos}(\mathcal{H})$ be positive semi-definite operators. The fidelity between P and Q , $\mathrm{F}(P, Q)$, is defined as

$$\mathrm{F}(P, Q) \quad := \quad \mathrm{Tr}\sqrt{\sqrt{P}Q\sqrt{P}} \ ,$$

where $\sqrt{P} = \sum_i \sqrt{\lambda_i}|\psi_i\rangle\langle\psi_i|$ in which λ_i is the i-th eigenvalue of P, and $|\psi_i\rangle$ is its corresponding eigenvector.

For any two quantum states $\rho, \sigma \in \mathsf{D}(\mathcal{H})$, the fidelity between ρ and σ, $\mathrm{F}(\rho, \sigma)$, varies between 0 and 1, and quantifies the similarity between two quantum states, as the more two states are similar, their fidelity is closer to 1.

Here we mention some properties of fidelity which are useful in the rest of this thesis.

1. Fidelity is a symmetric function, i.e. for any $P, Q \in \mathsf{Pos}(\mathcal{H}) : \mathrm{F}(P, Q) = \mathrm{F}(Q, P)$.

2. For any $P, Q \in \mathsf{Pos}(\mathcal{H})$:

$$\mathrm{F}(P, Q)^2 \leq \mathrm{Tr}(P)\mathrm{Tr}(Q) \ . \tag{2.2.1}$$

3. For any $P_1, P_2, Q_1, Q_2 \in \mathsf{Pos}(\mathcal{H})$, we have

$$\mathrm{F}(P_1 + P_2, Q_1 + Q_2) \quad \geq \quad \mathrm{F}(P_1, Q_1) + \mathrm{F}(P_2, Q_2) \ . \tag{2.2.2}$$

4. Fidelity is monotone under the application of quantum operations [29], i.e. for any quantum operation Φ,

$$\mathrm{F}(\Phi(\rho), \Phi(\sigma)) \quad \geq \quad \mathrm{F}(\rho, \sigma) \ .$$

5. The Uhlmann theorem [35]: For any two quantum states $\rho, \sigma \in \mathsf{D}(\mathcal{H})$, let $|\psi\rangle$ be a purification of ρ. Then,

$$\mathrm{F}(\rho, \sigma) \quad = \quad \max_{|\phi\rangle} |\langle\psi|\phi\rangle| \ ,$$

where the maximum is over all purification $|\phi\rangle$ of σ, $|\phi\rangle$.

6. Let $\rho \in \mathsf{D}(\mathcal{H})$ and $\sigma \in \mathsf{D}(\mathcal{H})$ be two quantum states. Then [27]

$$1 + \mathrm{F}(\rho, \sigma) \quad = \quad \max\{\mathrm{F}(\rho, \xi)^2 + \mathrm{F}(\sigma, \xi)^2 : \xi \in \mathsf{D}(\mathcal{H})\} \ . \tag{2.2.3}$$

A metric for quantum states

In this thesis, we need a metric for sub-normalized states, i.e. positive semi-definite operators with trace at most one. One of the distance measures based on fidelity is the *purified distance* [33]. Suppose that ρ and σ are two sub-normalized states. Then the purified distance of ρ and σ is defined as

$$\mathrm{P}(\rho,\sigma) \quad := \quad \sqrt{1-\mathrm{F}(\rho,\sigma)^2} \ .$$

Let $\rho \in \mathsf{D}(\mathcal{H})$ be a quantum state and $\epsilon \in [0,1)$. Then

$$\mathsf{B}^{\epsilon}(\rho) := \{\tilde{\rho} \in \mathsf{Pos}(\mathcal{H}) : \mathrm{P}(\rho,\tilde{\rho}) \leq \epsilon, \mathrm{Tr}\,\tilde{\rho} \leq 1\}$$

is the ball of ϵ-close states around ρ. We say that σ is *ϵ-close* to ρ (or equivalently σ is an *ϵ-approximation* of ρ) if and only if σ belongs to the set $\mathsf{B}^{\epsilon}(\rho)$.

The Uhlmann theorem can be easily extended to purified distance. The following lemma is a corollary of the Uhlmann theorem for purified distance, that we will use in the rest of this thesis.

Lemma 2.2.4. *Let $\rho_A \in \mathsf{D}(\mathcal{H}_A)$ be a quantum state in the Hilbert space $\mathcal{H}_A$ and $\rho_{AB} \in \mathsf{D}(\mathcal{H}_A \otimes \mathcal{H}'_B)$ be an extension of ρ_A over the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}'_B$, i.e. $\rho_A = \mathrm{Tr}_B(\rho_{AB})$. Let $\rho'_A \in \mathsf{B}^{\epsilon}(\rho_A)$ be an ϵ-approximation of ρ_A. Then there exists $\rho'_{AB} \in \mathsf{B}^{\epsilon}(\rho_{AB})$ such that $\rho'_A = \mathrm{Tr}_B(\rho'_{AB})$.*

Proof: Let $|v\rangle \in \mathsf{D}(\mathcal{H}_{A'} \otimes \mathcal{H}'_{B'} \otimes \mathcal{H}_A \otimes \mathcal{H}'_B)$ be a purification of ρ_{AB} and therefore also of ρ_A, and $|v'\rangle \in \mathsf{D}(\mathcal{H}_{A'} \otimes \mathcal{H}'_{B'} \otimes \mathcal{H}_A \otimes \mathcal{H}'_B)$ be a purification of ρ'_A, such that $\mathrm{F}(\rho_A, \rho'_A) = |\langle v|v'\rangle|$. Such $|v\rangle$ and $|v'\rangle$ exist by the Uhlmann theorem. Define $\rho'_{AB} = \mathrm{Tr}_{A'B'}(|v'\rangle\langle v'|)$. By definition, we have $\mathrm{F}(\rho_A, \rho'_A) = \mathrm{F}(\rho_{AB}, \rho'_{AB})$. Therefore $\rho'_{AB} \in \mathsf{B}^{\epsilon}(\rho_{AB})$. ■

Note that other metrics can be defined for quantum states, like *trace distance*. However, we choose purified distance since it is more appropriate in non-asymptotic quantum information theory to quantify the distance between two sub-normalized states.

2.2.2 LOCC protocols

The notion of LOCC, short for local operations and classical communication, plays an important role in quantum information, especially in the study of properties of entanglement.

This notion has been described exactly in terms of *quantum instruments* in [8]. The LOCC paradigm can be implemented by a protocol between two or more parties. In this thesis, we only study two-party protocols. Suppose that we have two parties, Alice and Bob, who can communicate with each other using only classical bits, share parts of a possibly entangled quantum state, and are allowed to perform any local quantum operations or measurements. Alice and Bob may be given inputs. Let X^A and X^B be the registers which hold Alice's and Bob's inputs, respectively, Y^A and Y^B be parts of a bipartite register distributed between Alice and Bob, and Z^A and Z^B be two empty registers with Alice and Bob which will hold the transcript during the protocol. Note that Z^A and Z^B are classical registers, and Y^A and Y^B are quantum registers between which may be some entanglement.

A one-way LOCC protocol is an LOCC protocol in which the communication consists of one message either from Alice to Bob (A-to-B protocol) or Bob to Alice (B-to-A protocol), but not both. In other words, an A-to-B LOCC protocol consists of the following steps.

1) Alice performs a general measurement on her register Y^A, and adds the outcome of measurement M to the register Z^A. The measurement is controlled by her input X^A.

2) Alice sends a copy of her measurement outcome to Bob, using m classical bits, and Bob adds the received message to Z^B

3) Bob performs a general measurement on his register Y^B. The measurement is controlled by his input X^B, and the register Z^B.

A B-to-A LOCC protocol contains the same steps as an A-to-B protocol, with the roles of Alice and Bob switched.

A two-way LOCC protocol is a general LOCC protocol, i.e. the communication is in both directions, from Alice to Bob and Bob to Alice. A two-way LOCC protocol consists of several alternations of measurement and communication similar to the one-way case. There are several rounds of communication in which the two parties alternately do a local measurement and send a message. Either party may start or end the protocol. Suppose in round i, it is Alice's turn. Then

1) First, Alice performs a general measurement on her register in that round, Y^A_{i-1}, controlled by her input, X^A and the register Z^A_{i-1}. She adds the outcome M_i of her measurement to the register Z^A_{i-1} and calls it Z^A_i.

2) Then, Alice sends a copy of her measurement outcome at that round, M_i, to Bob using m_i classical bits, and Bob adds the received message M_i to his transcript register Z^B_{i-1} and calls it Z^B_i.

Bob's actions are similar in a round in which it is his turn. At the end of a protocol with N rounds of communication, the recipient of the final message, say Bob, makes a measurement on his quantum register Y_N^B controlled by Z_N^B, and he adds the outcome M_{N+1} of his measurement to the register Z_N^B and calls it Z_{N+1}^B. Then, he outputs the final result which is either a part of Z_{N+1}^B or a part of Y_{N+1}^B.

In the above protocol, Y_i^A, Y_i^B, Z_i^A, and Z_i^B denote registers Y^A, Y^B, Z^A, and Z^B after the i-th round, respectively. Also, M_i denotes Alice's or Bob's message in the i-th round.

2.2.3 Quantum communication complexity

The notion of quantum communication complexity was firstly introduced by Yao [37]. Here we review the definition of quantum communication complexity for LOCC protocols. A comprehensive introduction to the notion of communication complexity can be found in [22].

Let X, Y be two finite sets, Z be a set but not necessarily finite, and $f \subseteq X \times Y \times Z$ be a relation such that for every $(x, y) \in X \times Y$, there exists some $z \in Z$ such that $(x, y, z) \in f$. In an LOCC protocol, Alice and Bob get as an input $x \in X$ and $y \in Y$, respectively, and their goal is to output an element $z \in Z$ such that $(x, y, z) \in f$. In the protocols we consider, one party may not get any input, so e.g., Y may be empty. Also, in general the output of the protocol is probabilistic. If $W_{x,y}$ is the random output that the protocol produces on inputs (x, y), we define the error as $\delta = \Pr((x, y, W_{x,y}) \notin f)$. We say the protocol *computes* f if δ is a constant $< 1/2$. The *entanglement-assisted communication complexity* of f is defined as the minimum number of bits exchanged in an LOCC protocol computing f, and denoted by $\mathsf{Q}^*(f)$.

Now consider the relation $f' \subseteq X \times Y \times Z$ such that for every $(x, y, z) \in f$, the tuple (x, y, z') belongs to f' if and only if z' is an approximation of z, i.e., the fidelity between z and z' is close enough to 1. Let $w_{x,y}$ be the average of the random output $W_{x,y}$ that a protocol produces on inputs (x, y), and p be a probability distribution over $X \times Y$. We say a protocol computes an approximation f' of f with average-case error at most ϵ if $\delta = \Pr((x, y, W_{x,y}) \notin f)$ is a constant $< 1/2$ and $\sum_{(x,y,z)\in f} p(x, y)\mathrm{F}(w_{x,y}, z) \geq \sqrt{1 - \epsilon^2}$. The *average-case error communication complexity of* f is defined as the minimum number of bits exchanged in an LOCC protocol computing an approximation f' of f with average-case error at most ϵ, and denoted by $\mathsf{Q}_p^*(f, \epsilon)$. Similarly, we say a protocol computes an approximation f' of f with worst-case error at most ϵ if $\delta = \Pr((x, y, W_{x,y}) \notin f)$ is a constant $< 1/2$ and for every $(x, y, z) \in f$, $\mathrm{F}(w_{x,y}, z) \geq \sqrt{1 - \epsilon^2}$. The *worst-case error communication complexity of* f is defined as the minimum number of bits exchanged in an

LOCC protocol computing an approximation f' of f with worst-case error at most ϵ, and is denoted by $\mathsf{Q}^*(f,\epsilon)$.

2.2.4 Different kinds of quantum entropy and mutual information

Asymptotic Information theory

In [28], von Neumann extended the notion of Shannon entropy in classical information theory to the quantum information theory. Let X be a register in quantum state $\rho \in \mathsf{D}(\mathcal{H})$. Then the *von Neumann entropy* $\mathrm{S}(\rho)$ of X is defined as

$$\mathrm{S}(\rho) \quad := -\mathrm{Tr}(\rho \log \rho) \ .$$

One can easily show that for a classical state this quantity is equivalent to Shannon entropy.

Let X and Y be two registers in quantum states $\rho_X \in \mathsf{D}(\mathcal{H})$ and $\rho_Y \in \mathsf{D}(\mathcal{H})$, respectively. Then, the *relative entropy* denoted by $\mathrm{S}(\rho_X||\rho_Y)$ is defined as

$$\mathrm{S}(\rho_X||\rho_Y) \quad := \quad \mathrm{Tr}\left(\rho_X \log \rho_X - \rho_X \log \rho_Y\right) \ .$$

Suppose that $\rho_{XY} \in \mathsf{D}(\mathcal{H} \otimes \mathcal{K})$ is the joint state of registers X and Y, then the *mutual information* of Y and X is defined as

$$\mathrm{I}(X:Y)_\rho \quad := \quad \mathrm{S}(\rho_X) + \mathrm{S}(\rho_Y) - \mathrm{S}(\rho_{XY}) \ ,$$

where $\rho_X = \mathrm{Tr}_Y(\rho_{XY})$ and $\rho_Y = \mathrm{Tr}_X(\rho_{XY})$. Note that when the state ρ is clear from the context, we do not include it as a subscript.

Another notion in quantum information theory is *observational divergence* defined by Jain *et al.* [16]. Let $\rho, \sigma \in \mathsf{D}(\mathcal{H})$. Then, their *observational divergence* is defined as

$$\mathrm{D}(\rho||\sigma) \quad := \quad \sup\left\{\mathrm{Tr}(M\rho)\log\frac{\mathrm{Tr}(M\rho)}{\mathrm{Tr}(M\sigma)} : 0 \leq M \leq \mathbb{1}, \mathrm{Tr}(M\sigma) \neq 0\right\} \ .$$

Let $\mathcal{E} = \{(p_j, \rho_j) : 1 \leq j \leq n\}$ be an ensemble of quantum states, i.e. $\sum_{j=1}^n p_j = 1$, and for every $j \in \{1, \ldots, n\}$, $0 \leq p_j \leq 1$ and ρ_j is a quantum state. The *Holevo information* of $\mathcal{E}$, denoted as $\chi(\mathcal{E})$, is defined as

$$\chi(\mathcal{E}) \quad := \quad \sum_{j=1}^n p_j \mathrm{S}(\rho_j||\rho) \ ,$$

where ρ is the ensemble average, i.e. $\rho = \sum_{j=1}^{n} p_j \rho_j$. Similarly, we can define the *divergence information* of $\mathcal{E}$, denoted as $\mathrm{D}(\mathcal{E})$, as

$$\mathrm{D}(\mathcal{E}) \quad := \quad \sum_{j=1}^{n} p_j \mathrm{D}(\rho_j || \rho) \ ,$$

where again ρ is the ensemble average.

Let S be a set, and $Q : S \to \mathsf{D}(\mathcal{H})$ be a function which encodes each $x \in S$ to a quantum state. Let p be a probability distribution over S, and $\rho_{AB}(p)$ be the bipartite state $\rho_{AB}(p) = \sum_x p_x |x\rangle\langle x|_A \otimes Q(x)_B$. Then, we define the *maximum possible information* in Q , denoted by $\mathsf{T}(Q)$, as

$$\mathsf{T}(Q) \quad := \max_p \ \mathrm{I}(A:B)_{\rho(p)} \ ,$$

where the maximum is over all probability distributions p.

Note that for a classical-quantum state $\rho_{AB} = \sum_{j=1}^{n} p_j |j\rangle\langle j| \otimes \rho_j$, the mutual information of A and B is equal to the Holevo information of the quantum ensemble $\mathcal{E} = \{(p_j, \rho_j) : 1 \leq j \leq n\}$, i.e. $\chi(\mathcal{E}) = \mathrm{I}(A:B)$, and therefore $\mathsf{T}(Q) \geq \chi(\mathcal{E})$.

Each of these quantities characterize processes with the assumption that the available resources are *i.i.d.*(independent and identically distributed), i.e., the process can be repeated with an arbitrary large number of times such that the repetitions are independent of each other.

Non-asymptotic information theory

In reality many scenarios do not have i.i.d. resources, for example many channels are not memoryless and may output correlated states for different inputs. Nowadays, researchers have put a great amount of effort on studying settings in which the resources are not i.i.d., called *one-shot settings*. One-shot concepts were implicit in traditional information theory and also in communication complexity. For example, Jain, Radhakrishnan and Sen mentioned implicitly the concept of *smooth max-relative entropy* in [16]. However, non-asymptotic information theory has been introduced formally by defining smooth *min- and max-entropies* [31, 32]. Later in [10], *max- and min-relative entropies* has been defined. Similar to quantum relative entropy, other information theoretic quantities like min- and max-entropies can be derived from max- and min-relative entropies. In this thesis, we use max-relative entropy and max-information defined as follows, to characterize communication complexity of remote state preparation.

Let $\rho, \sigma \in \mathsf{D}(\mathcal{H})$ be two quantum states. The *max-relative entropy* of ρ with respect to σ is defined as

$$\mathrm{D}_{\max}(\rho\|\sigma) \quad := \quad \min\{\lambda : \rho \leq 2^{\lambda}\sigma\} \ .$$

This notion actually quantifies how much σ behaves similarly to ρ under application of a measurement.

For a bipartite quantum state $\rho_{AB} \in \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$, the *max-information* part B has about part A is defined as [7]

$$\mathrm{I}_{\max}(A : B)_{\rho} \quad := \quad \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}_{\max}(\rho_{AB}\|\rho_A \otimes \sigma) \ .$$

Note that this quantity is asymmetric with respect to the parts A and B. Similar to the mutual information, we mention the state as a subscript only when it is not clear from the context. We can also generalize these notions and define the smoothed versions of these quantities as

$$\mathrm{D}^{\epsilon}_{\max}(\rho\|\sigma) \quad := \quad \min_{\tilde{\rho} \in \mathsf{B}^{\epsilon}(\rho)} \mathrm{D}_{\max}(\tilde{\rho}\|\sigma) \ ,$$

and

$$\mathrm{I}^{\epsilon}_{\max}(A : B)_{\rho} \quad := \quad \min_{\tilde{\rho} \in \mathsf{B}^{\epsilon}(\rho)} \mathrm{I}_{\max}(A : B)_{\tilde{\rho}} \ .$$

Note that there is no unique way to define max-information using max-relative entropy [9]. We choose this definition in this work since it can be used to characterize average-case communication complexity of the remote state preparation problem.

The following are some properties of max-information used in this thesis. One of the important properties of the max-information is monotonicity under application of a quantum channel, proved in Lemma 2.2.5.

Lemma 2.2.5. *[7] Let $\Phi : \mathrm{L}(\mathcal{H}') \rightarrow \mathrm{L}(\mathcal{K})$ be a quantum operation that maps states over the Hilbert space $\mathcal{H}'$ to states over the Hilbert space $\mathcal{K}$. Let $\rho \in \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ be any bipartite quantum state. Then*

$$\mathrm{I}_{\max}(A' : B)_{\rho'} \quad \leq \quad \mathrm{I}_{\max}(A : B)_{\rho} \ ,$$

where A, B denote the two parts of ρ, and A', B those of the state $\rho' = (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{H})})(\rho)$.

Proof: By the definition of max-mutual entropy,

$$\mathrm{I}_{\max}(A : B)_{\rho} \quad = \quad \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}_{\max}(\rho_{AB}\|\rho_A \otimes \sigma) \ .$$

Suppose that $\mathrm{D}_{\max}(\rho_{AB} \| \rho_A \otimes \sigma) = \lambda$ for an arbitrary $\sigma \in \mathsf{D}(\mathcal{H})$ i.e., $2^\lambda \rho_A \otimes \sigma - \rho_{AB} \geq 0$. Since Φ is completely positive, $2^\lambda \Phi(\rho_A) \otimes \sigma - (\Phi \otimes \mathbb{1})(\rho_{AB}) \geq 0$. In other words, $\mathrm{D}_{\max}(\rho'_{A'B} \| \rho'_{A'} \otimes \sigma) \leq \lambda$. Minimizing over such σ, we get

$$\begin{aligned} \mathrm{I}_{\max}(A' : B)_{\rho'} &\leq \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}_{\max}(\rho'_{A'B} \| \rho'_{A'} \otimes \sigma) \\ &\leq \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}_{\max}(\rho_{AB} \| \rho_A \otimes \sigma) \\ &= \mathrm{I}_{\max}(A : B)_\rho \ . \end{aligned}$$

■

In the following lemma, we extend this property to smooth max-information.

Lemma 2.2.6. *[7] Let $\Phi : \mathrm{L}(\mathcal{H}') \to \mathrm{L}(\mathcal{K})$ be a quantum operation that maps states over Hilbert space $\mathcal{H}'$ to states over Hilbert space $\mathcal{K}$. Let $\rho \in \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ be any bipartite quantum state. Then*

$$\mathrm{I}^\epsilon_{\max}(A' : B)_{\rho'} \quad \leq \quad \mathrm{I}^\epsilon_{\max}(A : B)_\rho \ ,$$

where A, B denote the two parts of ρ, and A', B those of the state $\rho' = (\Phi \otimes \mathbb{1}_{\mathrm{L}(\mathcal{H})})(\rho)$.

Proof: Using Lemma 2.2.5 (in the first inequality) and monotonicity of fidelity (in the second inequality),

$$\begin{aligned} \mathrm{I}^\epsilon_{\max}(A : B)_\rho &= \min_{\tilde{\rho}_{AB} \in \mathsf{B}^\epsilon(\rho_{AB})} \mathrm{I}_{\max}(A : B)_{\tilde{\rho}} \\ &\geq \min_{\tilde{\rho}_{AB} \in \mathsf{B}^\epsilon(\rho_{AB})} \mathrm{I}_{\max}(A' : B)_{(\Phi \otimes \mathbb{1}_{\mathcal{H}})(\tilde{\rho})} \\ &\geq \min_{\hat{\rho}_{A'B} \in \mathsf{B}^\epsilon(\rho_{AB})} \mathrm{I}_{\max}(A' : B)_{\hat{\rho}} \\ &= \mathrm{I}^\epsilon_{\max}(A' : B)_{\rho'} \ , \end{aligned}$$

as required. ■

The following lemma states that for a classical-quantum state ρ_{AB}, the value of smooth max-information is achieved by another classical-quantum state ρ'_{AB} which is ϵ-close to ρ_{AB}.

Lemma 2.2.7. *Let $\epsilon \geq 0$ and $\rho_{AB} \in \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ be a bipartite quantum state classical on A. There exists $\rho'_{AB} \in \mathsf{B}^\epsilon(\rho_{AB}) \cap \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ classical on A such that*

$$\mathrm{I}^\epsilon_{\max}(A : B)_\rho \quad = \quad \mathrm{I}_{\max}(A : B)_{\rho'} \ .$$

Proof: Let $\lambda = \mathrm{I}^{\epsilon}_{\max}(A:B)_\rho$, and $\tilde{\rho}_{AB} \in \mathsf{B}^{\epsilon}(\rho_{AB})$ and $\sigma_B \in \mathsf{D}(\mathcal{H})$ be two quantum states for which

$$\tilde{\rho}_{AB} \quad \leq \quad 2^{\lambda}\tilde{\rho}_A \otimes \sigma_B \ .$$

We can assume that $\tilde{\rho}_{AB}$ has trace equal to one i.e., $\tilde{\rho}_{AB} \in \mathsf{B}^{\epsilon}(\rho_{AB}) \cap \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$, since otherwise we can consider $\frac{\tilde{\rho}_{AB}}{\mathrm{Tr}(\tilde{\rho}_{AB})}$ instead of $\tilde{\rho}_{AB}$. Let $\Phi_A : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H})$ be a quantum-to-classical channel such that:

$$\Phi_A(X) = \sum_i \langle x_i|X|x_i\rangle |x_i\rangle\langle x_i|$$

for all $X \in \mathrm{L}(\mathcal{H})$, where $\{|x_i\rangle\}$ is the orthonormal basis for $\mathrm{L}(X)$ in which the input is specified. Let $\rho'_{AB} = (\Phi_A \otimes \mathbb{1}_B)(\tilde{\rho}_{AB})$. By monotonicity of purified distance and definition of ρ'_{AB}, $\rho'_{AB} \in \mathsf{B}^{\epsilon}(\rho_{AB}) \cap \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$. Hence by optimality of $\tilde{\rho}_{AB}$, we have

$$\mathrm{I}^{\epsilon}_{\max}(A:B)_\rho \quad = \quad \mathrm{I}_{\max}(A:B)_{\tilde{\rho}} \quad \leq \quad \mathrm{I}_{\max}(A:B)_{\rho'} \ ,$$

and by Lemma 2.2.5, we have

$$\mathrm{I}_{\max}(A:B)_{\rho'} \quad \leq \quad \mathrm{I}_{\max}(A:B)_{\tilde{\rho}} \ .$$

Therefore, we conclude that

$$\mathrm{I}^{\epsilon}_{\max}(A:B)_\rho \quad = \quad \mathrm{I}_{\max}(A:B)_{\rho'} \ ,$$

in which $\rho'_{AB} \in \mathsf{B}^{\epsilon}(\rho_{AB}) \cap \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ and is classical on A. ■

In [36], another one-shot entropy has been defined and used in *hypothesis testing* and *channel coding*. This one-shot entropy is called *ϵ-hypothesis testing relative entropy* and is defined as

$$\mathrm{D}^{\epsilon}_{\mathrm{h}}(\rho||\sigma) \quad := \quad -\log\frac{\beta^{\epsilon}(\rho||\sigma)}{1-\epsilon} \ ,$$

where

$$\beta^{\epsilon}(\rho||\sigma) \quad := \quad \inf\{\langle Q,\sigma\rangle | 0 \leq Q \leq \mathbb{1} \wedge \langle Q,\rho\rangle \geq 1-\epsilon\} \ . \tag{2.2.4}$$

In this definition, $\{Q, \mathbb{1}-Q\}$ can be considered as a measurement for distinguishing ρ from σ. So, $\beta^{\epsilon}(\rho||\sigma)$ corresponds to minimizing the probability of producing a wrong guess on σ while ρ will be always distinguished correctly with probability at least $1-\epsilon$, in a strategy $\{Q, \mathbb{1}-Q\}$.

Some useful properties of these quantities are mentioned in the following lemmas.

Lemma 2.2.8. *[36] Let $\rho, \sigma \in \mathsf{D}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$, and $\Phi : \mathsf{L}(\mathcal{H}) \to \mathsf{L}(\mathcal{K})$ be a quantum operation. Then,*

$$\beta^\epsilon(\rho||\sigma) \quad \leq \quad \beta^\epsilon(\Phi(\rho)||\Phi(\sigma)) \ .$$

This property is known as data processing inequality of β^ϵ. The proof can be found in [36].

The following lemmas have been proved implicitly in [25]. Here we prove them in a similar way.

Lemma 2.2.9. *Let $\rho, \sigma \in \mathsf{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be two bipartite quantum states with parts A and B which are both classical on their A part. Then, there exists a POVM element Q that achieves the optimum in Equation (2.2.4) and has the following form:*

$$Q \quad = \quad \sum_a |a\rangle\langle a| \otimes Q^a \ ,$$

where the set $\{|a\rangle\}_a$ is an orthonormal basis for the Hilbert space $\mathcal{H}_A$, and $0 \leq Q^a \leq \mathbb{1}$ for all a.

Proof: Let Q' be some POVM that achieves $\beta^\epsilon(\rho||\sigma)$, i.e., we have $0 \leq Q' \leq \mathbb{1}$, $\langle Q', \rho \rangle \geq 1 - \epsilon$, and

$$\beta^\epsilon(\rho||\sigma) \quad = \quad \langle Q', \sigma \rangle \ .$$

Let $\Phi_A : \mathsf{L}(\mathcal{H}) \to \mathsf{L}(\mathcal{H})$ be a quantum-to-classical channel such that

$$\Phi_A(X) = \sum_a \langle a|X|a\rangle |a\rangle\langle a| \ ,$$

for all $X \in \mathsf{L}(\mathcal{H})$. Then $\tilde{Q} = (\Phi_A \otimes \mathbb{1}_B)(Q')$ is a POVM element, i.e., $0 \leq \tilde{Q} \leq \mathbb{1}$, which is in the form of $\tilde{Q} = \sum_a |a\rangle\langle a| \otimes \tilde{Q}^a$ for some $\tilde{Q}^a \in \mathsf{Pos}(\mathcal{H}_B)$. By definition of Φ_A, we have $\langle (\Phi_A \otimes \mathbb{1}_B)(Y), X \rangle = \langle Y, (\Phi_A \otimes \mathbb{1}_B)(X) \rangle$ for any choices of $X, Y \in \mathsf{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$. In addition, since ρ and σ are classical on A part, $(\Phi_A \otimes \mathbb{1})(\rho) = \rho$ and $(\Phi_A \otimes \mathbb{1})(\sigma) = \sigma$. Therefore, for $\tilde{Q} = (\Phi_A \otimes \mathbb{1})(Q')$,

$$\langle \tilde{Q}, \rho \rangle \quad = \quad \langle Q', \rho \rangle \quad \geq \quad 1 - \epsilon \ ,$$

and

$$\langle \tilde{Q}, \sigma \rangle \quad = \quad \langle Q', \sigma \rangle \ ,$$

as required. ■

Lemma 2.2.10. *Let $\rho_{AB}(p) \in \mathsf{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be a quantum state classical on A such that the distribution on A is given by the probability vector p. Let $\sigma \in \mathsf{D}(\mathcal{H}_B)$ be a quantum state on Hilbert space $\mathcal{H}_B$. Then the function $\beta^\epsilon(\rho_{AB}(p)||\rho_A(p) \otimes \sigma)$ is convex with respect to p where $\rho_A(p) = \mathrm{Tr}_B(\rho_{AB}(p))$.*

Proof: Let p_1 and p_2 be two arbitrary probability distributions. We want to show that

$$\beta^\epsilon(\rho_{AB}(q)||\rho_A(q) \otimes \sigma) \quad \leq \quad \lambda\beta^\epsilon(\rho_{AB}(p_0)||\rho_A(p_0) \otimes \sigma) + (1-\lambda)\beta^\epsilon(\rho_{AB}(p_1)||\rho_A(p_1) \otimes \sigma) \ ,$$

for all $\lambda \in [0,1]$, where $q = \lambda p_0 + (1-\lambda)p_1$.

Suppose that $\rho_{AB}(p) = \sum_a p(a)|a\rangle\langle a| \otimes \rho_B^a$. Let $\Phi : \mathsf{L}(\mathcal{H}_A) \to \mathsf{L}(\mathbb{C}^2 \otimes \mathcal{H}_A)$ be the quantum operation with Kraus operators $A_{a,x} = \sqrt{\alpha_x^a}|x\rangle \otimes |a\rangle\langle a|$ for all a and $x \in \{0,1\}$, where $\alpha_0^a := \lambda\frac{p_0(a)}{\lambda p_0(a)+(1-\lambda)p_1(a)}$ and $\alpha_1^a = 1-\alpha_0^a$. Then we have

$$\rho_{XAB}(q) \quad = \quad (\Phi \otimes \mathbb{1}_B)(\rho_{AB}(q)) \quad = \quad \sum_{a,x} q(a)\alpha_x^a|x\rangle\langle x| \otimes |a\rangle\langle a| \otimes \rho_B^a \ .$$

Since $\rho_{XAB}(q)$ is an extension of $\rho_{AB}(q)$, we have

$$\beta^\epsilon(\rho_{AB}(q)||\rho_A(q) \otimes \sigma) \quad = \quad \beta^\epsilon(\rho_{XAB}(q)||\rho_{XA}(q) \otimes \sigma) \ ,$$

by using Lemma 2.2.8 twice.

For each $x \in \{0,1\}$, let Q^x be the POVM element that achieves $\beta^\epsilon(\rho_{AB}(p_x)||\rho_A(p_x)\otimes\sigma)$, i.e. $0 \leq Q^x \leq \mathbb{1}$, $\mathrm{Tr}\left(Q^x\rho_{AB}(p_x)\right) \geq 1-\epsilon$ and $\beta^\epsilon(\rho_{AB}^x||\rho_A^x \otimes \sigma) = \langle Q^x, \rho_A^x \otimes \sigma\rangle$. By Lemma 2.2.9, we can assume that $Q^x = \sum_a |a\rangle\langle a| \otimes Q^{x,a}$ for all $x \in \{0,1\}$. We choose $Q = \sum_{a,x} |x\rangle\langle x| \otimes |a\rangle\langle a| \otimes Q^{x,a}$ which satisfies

$$\begin{aligned}
\mathrm{Tr}(Q\rho_{XAB}(q)) \quad &= \quad \sum_{a,x} q(a)\alpha_x^a \mathrm{Tr}(Q^{x,a}\rho_B^a) \\
&= \quad \sum_a \left[\lambda p_0(a)\mathrm{Tr}(Q^{0,a}\rho_B^a) + (1-\lambda)p_1(a)\mathrm{Tr}(Q^{1,a}\rho_B^a)\right] \\
&= \quad \lambda\sum_a p_0(a)\mathrm{Tr}(Q^{0,a}\rho_B^a) + (1-\lambda)\sum_a p_1(a)\mathrm{Tr}(Q^{1,a}\rho_B^a) \\
&\geq \quad 1-\epsilon \ ,
\end{aligned}$$

by optimality of Q^0 and Q^1. So,

$$\begin{aligned}
\beta^\epsilon(\rho_{AB}(q)||\rho_A(q) \otimes \sigma) \quad &\leq \quad \mathrm{Tr}\left(Q(\rho_{XA}(q) \otimes \sigma)\right) \\
&= \quad \lambda\sum_a p_0(a)\mathrm{Tr}(Q^{0,a}\sigma) + (1-\lambda)\sum_a p_1(a)\mathrm{Tr}(Q^{1,a}\sigma) \\
&= \quad \lambda\beta^\epsilon(\rho_{AB}(p_0)||\rho_A(p_0) \otimes \sigma) + (1-\lambda)\beta^\epsilon(\rho_{AB}(p_1)||\rho_A(p_1) \otimes \sigma) \ ,
\end{aligned}$$

where the first inequality is true by definition of β^ϵ. ■

Lemma 2.2.11. *Let $\rho, \sigma \in \mathsf{D}(\mathcal{H})$ be two quantum states. Then the function $\beta^\epsilon(\rho||\sigma)$ is a convex function with respect to σ.*

Proof: For any choices of $\sigma_1, \sigma_2 \in \mathsf{D}(\mathcal{H})$ and $\lambda \in [0,1]$, let Q be the POVM that achieves $\beta^\epsilon(\rho||\lambda\sigma_1 + (1-\lambda)\sigma_2)$, then

$$\begin{aligned}\beta^\epsilon(\rho||\lambda\sigma_1 + (1-\lambda)\sigma_2) &= \langle Q, \lambda\sigma_1 + (1-\lambda)\sigma_2\rangle \\ &= \lambda\langle Q, \sigma_1\rangle + (1-\lambda)\langle Q, \sigma_2\rangle \\ &\geq \lambda\beta^\epsilon(\rho||\sigma_1) + (1-\lambda)\beta^\epsilon(\rho||\sigma_2) \ ,\end{aligned}$$

where the last inequality is true since $0 \leq Q \leq \mathbb{1}$ and $\langle Q, \rho\rangle \geq 1-\epsilon$. ■

The following lemma gives bounds for ϵ-hypothesis testing entropy in terms of smooth max-relative entropy. The proof can be found in [12, 34].

Lemma 2.2.12. *[12, 34] Let $\rho, \sigma \in \mathsf{D}(\mathcal{H})$ be two quantum states in Hilbert space $\mathcal{H}$. The following inequalities hold for any $0 < \epsilon \leq 1$ and $0 < \delta < \epsilon$:*

$$\mathrm{D}_{\max}^{\sqrt{2(1-\epsilon)}}(\rho||\sigma) \leq \mathrm{D}_h^\epsilon(\rho||\sigma) \ , \text{ and} \tag{2.2.5}$$

$$\mathrm{D}_{\max}^{\sqrt{1-\epsilon}}(\rho||\sigma) \geq \mathrm{D}_h^{\epsilon-\delta}(\rho||\sigma) - \log\frac{\epsilon(1-\epsilon+\delta)}{\delta^3} - 3\log 3 \ . \tag{2.2.6}$$

Chapter 3

Protocols for classical messages

As we mentioned in the Introduction, in order to convey n bits of information to Bob with success probability p using quantum communication, Alice needs to send at least $\frac{1}{2}(n + \log p)$ qubits to Bob in an entanglement-assisted quantum protocol [26]. On the other hand, consider a classical communication protocol in which Alice sends exactly $n - \log \frac{1}{p}$ bits of her n bit string input, and Bob randomly chooses the remaining bits. Then the probability that Bob correctly decodes Alice's message is p. In this section, we show that even if we allow shared entanglement, without quantum communication the communication complexity does not decrease, i.e., in any LOCC protocol for this task Alice needs to send at least $n + \log p$ bits in order to get success probability p. This result is a strengthening of the proof in [26].

3.1 Preparations

In the following sections, we assume that Alice and Bob have access to an arbitrarily large supply of private qubits in some fixed basis state, say $|\bar{0}\rangle$. So by Theorem 2.2.3, we can assume that during the protocol, each party performs a unitary followed by a projection in the standard basis instead of a general measurement. Therefore, in the rest of this chapter, we consider a unitary operation followed by a projection in the standard basis on m qubits, instead of a general measurement with 2^m outcomes.

In addition, we first mention some lemmas which will be useful in the rest of this chapter.

Lemma 3.1.1. *[26] In any quantum communication protocol with prior entanglement, we may assume that the initial shared state is of the form*

$$(\mathbb{1}_A \otimes \Lambda) \sum_{r\in\{0,1\}^E} |r\rangle_A |r\rangle_B \ \ ,$$

for some $\Lambda = \sum_{r\in\{0,1\}^E} \sqrt{\lambda_r}|r\rangle\langle r|$ *with* $\lambda_r \geq 0$ *and* $\sum_{r\in\{0,1\}^E} \lambda_r = 1$*.*

Proof: Without loss of generality, assume that Alice and Bob hold E_A and E_B qubits of the initial state, respectively, where $E_B \geq E_A$. Let $|\phi\rangle = \sum_{i\in\{0,1\}^{E_A}} \sqrt{\gamma_i}|a_i\rangle_A|b_i\rangle_B$ be the spectral decomposition of the initial shared state. Let Alice and Bob start with the shared state $|\psi\rangle = \sum_{r\in\{0,1\}^{E_B}} \sqrt{\lambda_r}|r\rangle_A|r\rangle_B$, where $\lambda_{\bar{0}s} = \gamma_s$ for $s \in \{0,1\}^{E_A}$, and is zero otherwise, which can be simplified to

$$\sum_{i\in\{0,1\}^{E_A}} \sqrt{\gamma_i}|\bar{0}, i\rangle_A|\bar{0}, i\rangle_B \ \ .$$

It is easy to see that using proper unitary operators, Alice and Bob are able to produce the state $|\phi\rangle$ (tensored with some fixed pure state) and the protocol proceeds exactly the same. ■

Lemma 3.1.2. *[26] For any linear transformation A on E qubits and any orthonormal set* $\{|\phi_a\rangle : a \in \{0,1\}^E\}$ *over* $E' \geq E$ *qubits,*

$$\sum_{a\in\{0,1\}^E} A|a\rangle \otimes |\phi_a\rangle \quad = \quad \sum_{a\in\{0,1\}^E} |a\rangle \otimes \tilde{A}|\phi_a\rangle \ \ ,$$

where $\tilde{A}$ *is any transformation on* E' *qubits such that for all* $a,a' \in \{0,1\}^E$, $\langle\phi_a|\tilde{A}|\phi_{a'}\rangle = \langle a'|A|a\rangle$*.*

Proof: Since the set $\{|a\rangle : a \in \{0,1\}^E\}$ is an orthonormal basis for the Hilbert space of E qubits, we have

$$\begin{aligned}
\sum_{a\in\{0,1\}^E} A|a\rangle|\phi_a\rangle \quad &= \quad \sum_a \sum_{a'} \langle a'|A|a\rangle|a'\rangle|\phi_a\rangle \\
&= \quad \sum_a \sum_{a'} \langle\phi_a|\tilde{A}|\phi_{a'}\rangle|a'\rangle|\phi_a\rangle \\
&= \quad \sum_{a'} |a'\rangle \sum_a \langle\phi_a|\tilde{A}|\phi_{a'}\rangle|\phi_a\rangle \\
&= \quad \sum_{a'} |a'\rangle\tilde{A}|\phi_{a'}\rangle \ \ ,
\end{aligned}$$

as required. ■

Corollary 3.1.3. *For any linear operation A on E qubits*

$$\sum_{a\in\{0,1\}^E} A|a\rangle \otimes |a\rangle \quad = \quad \sum_{a\in\{0,1\}^E} |a\rangle \otimes A^T|a\rangle \ .$$

3.2 One-way communication LOCC protocols

In this section, we consider one-way LOCC protocols and prove that $n + \log p$ is a lower bound for the number of bits that one needs to communicate in order to send n bits with success probability p. The following theorem states it in a more formal way.

Theorem 3.2.1. *Let X be a uniform random variable over bit strings of length n which is given as input to Alice in an entanglment-assisted one-way LOCC protocol using m bits of communication. Let Y be any random variable over n bit strings corresponding to Bob's output, and let $p = \Pr[X = Y]$ be the probability that Bob gets the output X. Then,*

$$m \quad \geq \quad n - \log\frac{1}{p} \ ,$$

where m is the number of classical bits Alice sends to Bob in the protocol.

Proof: By Lemma 3.1.1, we can assume that the shared entanglement is in the form of $\sum_{r\in\{0,1\}^E} |r\rangle\Lambda|r\rangle$ for some $\Lambda = \sum_{r\in\{0,1\}^E} \sqrt{\lambda_r}|r\rangle\langle r|$ with $\lambda_r \geq 0$ and $\sum_{r\in\{0,1\}^E} \lambda_r = 1$. As mentioned in Section 2.2.2, any one-way LOCC protocol consists of three steps. In the first step, Alice performs a unitary transformation based on her input followed by a projection in the standard basis. Let U_x be Alice's unitary when Alice is given x as her input. After performing the unitary U_x, the joint state of Alice and Bob is

$$\begin{aligned}(U_x \otimes \mathbb{1})(\mathbb{1} \otimes \Lambda) \sum_{r\in\{0,1\}^E} |r\rangle \otimes |r\rangle \quad &= \quad (\mathbb{1} \otimes \Lambda)(U_x \otimes \mathbb{1}) \sum_{r\in\{0,1\}^E} |r\rangle \otimes |r\rangle \\ &= \quad (\mathbb{1} \otimes \Lambda)(\mathbb{1} \otimes U_x^T) \sum_{r\in\{0,1\}^E} |r\rangle \otimes |r\rangle \\ &= \quad \sum_{r\in\{0,1\}^E} |r\rangle \Lambda U_x^T |r\rangle \ .\end{aligned}$$

Then, Alice performs the projective measurement with projection operators $\{|\mu\rangle\langle\mu| \otimes \mathbb{1}\}_{\mu\in\{0,1\}^m}$, and in the second step Alice sends the outcome of her measurement, μ, to Bob. So, the joint state of Alice and Bob after the second step is

$$\begin{aligned}
& \sum_{\mu\in\{0,1\}^m} \sum_{r,r'\in\{0,1\}^E} (|\mu\rangle\langle\mu| \otimes \mathbb{1})\, |r\rangle\langle r'|\, (|\mu\rangle\langle\mu| \otimes \mathbb{1}) \otimes |\mu\rangle\langle\mu| \otimes \Lambda U_x^T |r\rangle\langle r'| \bar{U}_x \Lambda^* \\
= & \sum_{\mu\in\{0,1\}^m} \sum_{l,k\in\{0,1\}^{E-m}} |\mu l\rangle\langle\mu k| \otimes |\mu\rangle\langle\mu| \otimes \Lambda U_x^T |\mu l\rangle\langle\mu k| \bar{U}_x \Lambda^* \ ,
\end{aligned}$$

and therefore Bob's state after the second step is

$$\sum_{\mu\in\{0,1\}^m} \sum_{l\in\{0,1\}^{E-m}} |\mu\rangle\langle\mu| \otimes \Lambda U_x^T |\mu l\rangle\langle\mu l| \bar{U}_x \Lambda^* \ ,$$

in other words, Bob has the mixed states over $m + E$ qubits of

$$\{(\mathbb{1}_{\mathcal{M}} \otimes \Lambda)|\phi_{x,\mu,l}\rangle\}_{\substack{\mu\in\{0,1\}^m \\ l\in\{0,1\}^{E-m}}} \ ,$$

where $|\phi_{x,\mu,l}\rangle = |\mu\rangle \otimes U_x^T |\mu l\rangle$, and $\mathcal{M}$ is the Hilbert space corresponding to Alice's message μ.

Finally, Bob performs a projective measurement $\{P_x\}_{x\in\{0,1\}^n}$ on his qubits, and gets the random variable Y. Therefore, p, the success probability of the protocol, is

$$\begin{aligned}
\Pr[X = Y] \quad & = \quad \sum_{x\in\{0,1\}^n} \Pr[X = x] \Pr[Y = x | X = x] \\
& = \quad \sum_{x\in\{0,1\}^n} \frac{1}{2^n} \mathrm{Tr} \left(P_x \sum_{\mu\in\{0,1\}^m} \sum_{l\in\{0,1\}^{E-m}} (\mathbb{1}_{\mathcal{M}} \otimes \Lambda)\, |\phi_{x,\mu,l}\rangle\langle\phi_{x,\mu,l}|\, (\mathbb{1}_{\mathcal{M}} \otimes \Lambda^*) \right) \\
& = \quad \frac{1}{2^n} \sum_{x,\mu,l} \mathrm{Tr}(P_x (\mathbb{1}_{\mathcal{M}} \otimes \Lambda) |\phi_{x,\mu,l}\rangle\langle\phi_{x,\mu,l}| (\mathbb{1}_{\mathcal{M}} \otimes \Lambda^*)) \\
& = \quad \frac{1}{2^n} \sum_{x} \mathrm{Tr}\big(P_x (\mathbb{1}_{\mathcal{M}} \otimes \Lambda) (\sum_{\mu,l} |\phi_{x,\mu,l}\rangle\langle\phi_{x,\mu,l}|) (\mathbb{1}_{\mathcal{M}} \otimes \Lambda^*)\big) \\
& \leq \quad \frac{1}{2^n} \sum_{x} \mathrm{Tr}\big(P_x (\mathbb{1}_{\mathcal{M}} \otimes \Lambda\Lambda^*)\big) \\
& = \quad \frac{1}{2^n} \mathrm{Tr}(\mathbb{1}_{\mathcal{M}} \otimes \Lambda\Lambda^*) \\
& = \quad \frac{2^m}{2^n} \ ,
\end{aligned}$$

where the first inequality is true since the set $\{|\phi_x, \mu, l\rangle\}_{\mu,l}$ is an orthonormal set and hence $\sum_{\mu,l} |\phi_{x,\mu,l}\rangle\langle\phi_{x,\mu,l}| \leq \mathbb{1}$, and the second last equality is derived using $\sum_x P_x = \mathbb{1}$. Therefore, we conclude that $m \geq n + \log p$. ■

3.3 The extension to general LOCC protocols

In this section, we extend the result we derived in Section 3.2 to any two-way LOCC protocol. To achieve this goal, we prove in Lemma 3.3.1 that after each round of an LOCC protocol, the joint state of Alice and Bob is in a special form. Then we use this property to prove our desired result in Theorem 3.3.2.

Lemma 3.3.1. *Let Π be any LOCC protocol with a finite number of rounds in which the initial number of qubits with each of Alice and Bob is E, the number of qubits sent by Alice to Bob is m, and the number of qubits sent by Bob to Alice is m'. Then the joint state of Alice and Bob at the end of the protocol can be written as*

$$\sum_{l,k \in \{0,1\}^{E-m}} \sum_{\substack{\mu \in \{0,1\}^m \\ \nu \in \{0,1\}^{m'}}} |l, \mu, \nu\rangle\langle k, \mu, \nu| \otimes \Lambda |\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}| \Lambda^* \ ,$$

where

1. *Λ is a linear transformation that maps $E + m + m'$ qubits to $E + m$ qubits, depends only on the initial joint state of Alice and Bob and the unitary transformations of Bob, and satisfies $\mathrm{Tr}(\Lambda\Lambda^*) = 2^m$, and*
2. *$\{|\phi_{\mu,\nu,l}\rangle\}$ is an orthonormal set of states over $E + m + m'$ qubits, and depends only on the unitary transformation of Alice.*

Proof: We prove this Lemma using induction on the number of rounds t.

Base Case: By Lemma 3.1.1, we assume that the initial joint state of Alice and Bob (for $t = 0$) is

$$\sum_{l,k \in \{0,1\}^E} |l\rangle\langle k| \otimes \Lambda |l\rangle\langle k| \Lambda^* \ ,$$

where $\Lambda = \sum_{l \in \{0,1\}^E} \sqrt{\lambda_l} |l\rangle\langle l|$ with $\lambda_l \geq 0$ and $\sum_l \lambda_l = 1$. So $\mathrm{Tr}(\Lambda\Lambda^*) = \sum_l \lambda_l = 1$ and for $t = 0$, the joint state of Alice and Bob is in the desired form.

Induction Hypothesis: Let m_t and m'_t be the total number of bits sent by Alice and Bob, respectively. The joint state of Alice and Bob at this stage can be expressed as

$$\sum_{l,k\in\{0,1\}^{E-m_t}} \sum_{\substack{\nu\in\{0,1\}^{m'_t} \\ \mu\in\{0,1\}^{m_t}}} |l,\mu,\nu\rangle\langle k,\mu,\nu| \otimes \Lambda_t|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}|\Lambda_t^* \ ,$$

where Λ_t and $|\phi_{\mu,\nu,l}\rangle$ satisfy the required conditions stated in the lemma (in terms of E, m_t, m'_t).

Inductive Step: We show that after $(t+1)$-th round, the joint state of Alice and Bob has the required form stated in the lemma. There are two possible cases for each round.

Case (1): Alice applies a unitary transformation U and then performs the projection to the standard basis on her p rightmost qubits, and sends the outcome π of her measurement to Bob. The joint state after applying U is

$$\begin{aligned}
&(U\otimes\mathbb{1})(\mathbb{1}_A\otimes\Lambda_t) \sum_{l,k\in\{0,1\}^{E-m_t}} \sum_{\substack{\nu\in\{0,1\}^{m'_t} \\ \mu\in\{0,1\}^{m_t}}} |l,\mu,\nu\rangle\langle k,\mu,\nu|_A \\
&\qquad \otimes|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}|_B\,(\mathbb{1}_A\otimes\Lambda_t^*)(U^*\otimes\mathbb{1}) \\
=\ & (\mathbb{1}_A\otimes\Lambda_t) \sum_{l,k\in\{0,1\}^{E-m_t}} \sum_{\substack{\nu\in\{0,1\}^{m'_t} \\ \mu\in\{0,1\}^{m_t}}} U|l,\mu,\nu\rangle\langle k,\mu,\nu|_A U^* \\
&\qquad \otimes|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}|_B\,(\mathbb{1}_A\otimes\Lambda_t^*) \\
=\ & (\mathbb{1}_A\otimes\Lambda_t) \sum_{l,k\in\{0,1\}^{E-m_t}} \sum_{\substack{\nu\in\{0,1\}^{m'_t} \\ \mu\in\{0,1\}^{m_t}}} |l,\mu,\nu\rangle\langle k,\mu,\nu| \\
&\qquad \otimes\tilde{U}|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}|_B\tilde{U}^*\,(\mathbb{1}_A\otimes\Lambda_t^*)\ ,
\end{aligned}$$

where U applies only on the l part of Alice's state, and $\tilde{U}$ is a unitary transformation on Bob's qubits as given in Lemma 3.1.2. Hence, after Alice performs her measurement and sends the measurement outcome to Bob, the joint state is

$$\begin{aligned}
&\sum_{\pi\in\{0,1\}^p} \sum_{l',k'\in\{0,1\}^{E-m_t-p}} \sum_{\substack{\nu\in\{0,1\}^{m'_t} \\ \mu\in\{0,1\}^{m_t}}} |l'\pi,\mu,\nu\rangle\langle k'\pi,\mu,\nu| \\
&\qquad \otimes|\pi\rangle\langle\pi|\otimes\Lambda_t\tilde{U}|\phi_{\mu,\nu,\pi l'}\rangle\langle\phi_{\mu,\nu,\pi k'}|_B\tilde{U}^*\Lambda_t^*\ .
\end{aligned}$$

Let

$$\Lambda_{t+1} \quad = \quad \mathbb{1}_{\mathcal{M}} \otimes \Lambda_t \text{ where } \mathcal{M} = \{0,1\}^p \ ,$$

and

$$|\phi_{\mu',\nu',l'}\rangle \quad = \quad |\pi\rangle \otimes \tilde{U}|\phi_{\mu,\nu,\pi l'}\rangle \ .$$

Then, the joint state can be written as

$$\sum_{l',k' \in \{0,1\}^{E-m_{t+1}}} \sum_{\substack{\nu' \in \{0,1\}^{m'_{t+1}} \\ \mu' \in \{0,1\}^{m_{t+1}}}} |l',\mu',\nu'\rangle\langle k',\mu',\nu'| \otimes \Lambda_{t+1}|\phi_{\mu',\nu',l'}\rangle\langle\phi_{\mu',\nu',k'}|\Lambda^*_{t+1} \ ,$$

where $m_{t+1} = m_t + p$ and $m'_{t+1} = m'_t$. Note that

$$\mathrm{Tr}(\Lambda_{t+1}\Lambda^*_{t+1}) \quad = \quad \mathrm{Tr}(\mathbb{1}_{\mathcal{M}} \otimes \Lambda_t\Lambda^*_t) \quad = \quad 2^p\,\mathrm{Tr}(\Lambda_t\Lambda^*_t) \quad = \quad 2^{m_{t+1}} \ ,$$

and by Lemma 3.1.2, the set $\{|\phi_{\mu',\nu',l'}\rangle\}$ is orthonormal.

Case (2): Bob applies a unitary transformation V and then performs the projection to the standard basis on his q leftmost qubits, and sends the outcome π of his measurement to Alice. The joint state after communication is

$$\sum_{\pi \in \{0,1\}^q} \sum_{l,k \in \{0,1\}^{E-m_t}} \sum_{\substack{\nu \in \{0,1\}^{m'_t} \\ \mu \in \{0,1\}^{m_t}}} |l,\mu,\nu,\pi\rangle\langle k,\mu,\nu,\pi| \otimes (|\pi\rangle\langle\pi| \otimes \mathbb{1})\,V\Lambda_t|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}|_B\Lambda^*_t V^*\,(|\pi\rangle\langle\pi| \otimes \mathbb{1}) \ .$$

Let

$$\Lambda_{t+1} \quad = \quad \sum_{b \in \{0,1\}^q} (|b\rangle\langle b| \otimes \mathbb{1})\,V\Lambda(\langle b| \otimes \mathbb{1}) \ ,$$

and

$$|\phi_{\mu',\nu',l'}\rangle \quad = \quad |\pi\rangle|\phi_{\mu,\nu,l}\rangle \ .$$

Then

$$\begin{aligned}
\mathrm{Tr}(\Lambda_{t+1}\Lambda^*_{t+1}) \quad &= \quad \mathrm{Tr}\left(\sum_{b \in \{0,1\}^q} (|b\rangle\langle b| \otimes \mathbb{1})\,V\Lambda_t\Lambda^*_t V^*\right) \\
&= \quad \mathrm{Tr}\left(V\Lambda_t\Lambda^*_t V^*\right) \\
&= \quad \mathrm{Tr}\left(\Lambda_t\Lambda^*_t\right) \\
&= \quad 2^{m_t} \quad = \quad 2^{m_{t+1}} \ ,
\end{aligned}$$

the set $\{|\phi_{\mu',\nu',l'}\rangle\}$ is orthonormal, and the joint state can be written as

$$\sum_{l',k'\in\{0,1\}^{E-m_{t+1}}} \sum_{\mu'\in\{0,1\}^{m_{t+1}},\nu'\in\{0,1\}^{m'_{t+1}}} |l',\mu',\nu'\rangle\langle k',\mu',\nu'| \otimes\Lambda_{t+1}|\phi_{\mu',\nu',l'}\rangle\langle\phi_{\mu',\nu',k'}|\Lambda^*_{t+1} \ ,$$

where $m_{t+1} = m_t$ and $m'_{t+1} = m'_t + q$, as required. So the inductive step is completed.

■

Theorem 3.3.2. *Suppose that Alice wants to convey n bits to Bob using an LOCC protocol, in which Alice and Bob share an arbitrary entangled state, the total number of classical bits exchanged by the two parties is m and the total number of classical bits Alice sends to Bob is m_A. Let X be the random variable (with uniform distribution) that Alice wants to convey and Y be the random variable denoting Bob's output in this protocol. Suppose that Bob guesses Alice's input correctly with probability $p \in (0,1]$, then m_A is at least $n - \log\frac{1}{p}$.*

Proof: We prove this theorem in a manner similar to Theorem 3.2.1 by bounding p from above. By Lemma 3.3.1, at the end of any general LOCC protocol, Bob's state is in a form similar to that in a one-way LOCC protocol, i.e., Bob's final state looks like

$$\sum_{l,k\in\{0,1\}^{E-m}} \sum_{\mu\in\{0,1\}^{m_A},\nu\in\{0,1\}^{m-m_A}} \Lambda|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,k}|\Lambda^* \ ,$$

for some linear transformation Λ with $\mathrm{Tr}(\Lambda\Lambda^*) = 2^{m_A}$ and orthonormal set $\{|\phi_{\mu,\nu,l}\rangle\}$. As before, after Bob performs his final projection to get Y, we have

$$\begin{aligned}
\Pr[X=Y] &= \sum_{x\in\{0,1\}^n} \frac{1}{2^n} \sum_{l\in\{0,1\}^{E-m_A}} \sum_{\mu\in\{0,1\}^{m_A},\nu\in\{0,1\}^{m-m_A}} \|P_x\Lambda|\phi_{\mu,\nu,l}\rangle\|^2 \\
&= \frac{1}{2^n}\sum_x \mathrm{Tr}(P_x\Lambda(\sum_{l,\mu,\nu}|\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,l}|)\Lambda^*) \\
&\le \frac{1}{2^n}\sum_x \mathrm{Tr}(P_x\Lambda\Lambda^*) \\
&= \frac{1}{2^n}\mathrm{Tr}(\Lambda\Lambda^*) \\
&= \frac{2^{m_A}}{2^n} \ ,
\end{aligned}$$

where the first inequality is true since the set $\{|\phi_{\mu,nu,l}\rangle\}$ is orthonormal and so

$$\sum_{l,\mu,\nu} |\phi_{\mu,\nu,l}\rangle\langle\phi_{\mu,\nu,l}| \leq \mathbb{1} \ ,$$

and the second last equality is derived using $\sum_x P_x = \mathbb{1}$. Therefore, we have $m_A \geq n - \log \frac{1}{p}$, as required. ■

Chapter 4

Approximate remote state preparation

Approximate remote state preparation is the process of preparing an approximation of a state in another place. The exact formulation of this problem is as follows.

Definition 4.0.1. *Let S be a finite set. Let $Q : S \to \mathsf{D}(\mathcal{H})$ be a function that "encodes" each $x \in S$ as some quantum state $Q(x)$ over the Hilbert space $\mathcal{H}$. Let $\epsilon \in [0, 1]$. Approximate remote state preparation, denoted as* $\mathrm{RSP}(S, Q, \epsilon)$*, is the following distributed task. Two physically separated parties, Alice and Bob, start with some shared entanglement. Both parties know the function Q. Alice is given an input $x \in S$, and the goal is for Bob to prepare an approximation σ_x of $Q(x)$. To accomplish this, they are allowed to run an LOCC protocol with a finite number of messages.*

In this chapter, we characterize the communication complexity of this problem for two different cases, average-case error and worst-case error. Note that we assume that Alice and Bob communicate within a perfect classical channel, and they have access to an arbitrarily large amount of entanglement and they have unlimited computational power. In section 4.1, we describe a protocol for approximate remote state preparation which was previously introduced by Jain, Radhakrishnan and Sen [17]. Then, in sections 4.2 and 4.3 we give lower bounds and upper bounds for the average-case error and worst-case error communication complexity of $\mathrm{RSP}(S, Q, \epsilon)$, respectively. Finally, in section 4.4, we compare our results with previous works and also compare the worst-case and the average-case.

4.1 A protocol for approximate remote state preparation

The Approximate Remote State Preparation (ARSP) can be performed by executing different kinds of protocols. A trivial protocol for this problem is when Alice sends her input, x, directly to Bob and so Bob can easily create the desired state $Q(x)$. In this protocol, Bob prepares $Q(x)$ with zero error ($\epsilon = 0$) using $\log n$ bits of classical communication, where $n = |S|$.

In [17], Jain *et al.* proposed another protocol using the inequalities derived from the substate theorem [16, 20]. Here, we explain that protocol for the case of having any such kind of inequalities.

Let $\mathcal{K}$ be a Hilbert space with $\dim(\mathcal{K}) \geq \dim(\mathcal{H})$ and $\{\sigma_x\}_{x\in S} \subseteq \mathsf{D}(\mathcal{H})$ be a set of quantum states such that for all $x \in S$, $\sigma_x \in \mathsf{B}^{\delta}(Q(x))$ for some $\delta \in [0,1]$. Suppose that for some $\lambda \in [0,\infty)$ and some $\sigma \in \mathsf{D}(\mathcal{H})$, we have

$$\sigma_x \quad \leq \quad 2^{\lambda}\sigma \qquad \text{for all} \quad x \in S \ . \tag{4.1.1}$$

This inequality can be written as

$$\sigma \quad = \quad 2^{-\lambda}\sigma_x + (1-2^{-\lambda})\xi_x \ ,$$

where $\xi_x \in \mathsf{D}(\mathcal{H})$ is a quantum state. Let $|v_x\rangle \in \mathcal{K}\otimes\mathcal{H}$ be a purification of σ_x in the Hilbert space $\mathcal{K}\otimes\mathcal{H}$, and $|u_x\rangle \in \mathcal{K}\otimes\mathcal{H}$ be a purification of ξ_x. Then

$$|w_x\rangle \quad = \quad \sqrt{2^{-\lambda}}\,|0\rangle|v_x\rangle \quad + \quad \sqrt{1-2^{-\lambda}}\,|1\rangle|u_x\rangle \ ,$$

is a purification of σ. Now, consider the following protocol.

Protocol: Initially, Alice and Bob share t copies of $|w\rangle$ (for a t to be specified later), an arbitrary but fixed purification of σ in $\mathbb{C}^2\otimes\mathcal{K}\otimes\mathcal{H}$, such that the purification part is with Alice and the σ part is with Bob. First, Alice performs a unitary operation U_x on her part which transforms $|w\rangle$ to $|w_x\rangle$. (By Theorem 2.2.1, such a unitary transformation exists.) Then, she measures the first qubit of these copies. If at least one of the measurement outcomes is equal to zero, then she sends the index of the corresponding copy, i.e. a number between 1 and t and Bob knows that his part of that copy is in fact σ_x. Otherwise, if the outcome of all measurements are equal to one, she sends $t+1$ to Bob and Bob prepares an arbitrary state, say the maximally mixed state.

After performing this protocol, Bob has $\frac{\mathbb{1}}{\dim(\mathcal{H})}$ with probability $(1-2^{-\lambda})^t$ and σ_x with probability $1-(1-2^{-\lambda})^t$. Hence, his final state is

$$\tilde{\sigma}_x \quad = \quad (1-(1-2^{-\lambda})^t)\sigma_x + (1-2^{-\lambda})^t \frac{\mathbb{1}}{\dim(\mathcal{H})} \quad .$$

By choosing δ small enough and t large enough, Bob's state $\tilde{\sigma}_x$ would be the desired approximation of $Q(x)$ in approximate remote state preparation. In the rest of this chapter, we exploit this protocol to find upper bounds on the worst-case error and average-case error communication complexity of $\mathrm{RSP}(S, Q, \epsilon)$.

4.2 Average-case error communication complexity

Let p be a probability distribution over S and $\mathsf{Q}_p^*(\mathrm{RSP}(S, Q, \epsilon))$ denote the average-case entanglement-assisted communication complexity of this problem with respect to p. We characterize this quantity by placing upper and lower bounds on it, in terms of the smooth max-information the encoding has about the input, i.e. $\mathrm{I}_{\max}^{\epsilon}(A:B)_{\rho(p)}$ which is the smooth max-information B has about A in the bipartite quantum state $\rho(p) = \sum_{x\in S} p_x |x\rangle\langle x|_A \otimes Q(x)_B$. Here, the subscripts A, B denote the parts to which the states correspond.

4.2.1 An upper bound

In this part, we show that to within error ϵ the average-case communication complexity of approximate remote state preparation problem is upper bounded by $\mathrm{I}_{\max}^{\delta}(A:B)_{\rho(p)} + \mathrm{O}(1)$, where $\delta = \frac{\epsilon}{\sqrt{1+\epsilon^2}}$, and the $\mathrm{O}(1)$ term depends only on ϵ. To do so, we use the protocol explained in Section 4.1.

Theorem 4.2.1. *For any finite set S, function $Q : S \to \mathsf{D}(\mathcal{H})$, and $\epsilon \in (0, 1]$, let p be a probability distribution over S and $\rho_{AB}(p) \in \mathsf{D}(\mathcal{H}' \otimes \mathcal{H})$ be the bipartite quantum state $\rho_{AB}(p) = \sum_{x\in S} p_x |x\rangle\langle x|_A \otimes Q(x)_B$. Then*

$$\mathsf{Q}_p^*(\mathrm{RSP}(S, Q, \epsilon)) \quad \leq \quad \mathrm{I}_{\max}^{\delta}(A:B)_{\rho(p)} + \log_2\left(\ln\left(\frac{4+3\epsilon^2}{2\epsilon^4}\right)\right) + 2 \quad ,$$

where $\delta = \frac{\epsilon}{2\sqrt{1+\epsilon^2}}$.

Proof: Fix some $\epsilon \in (0,1]$, and let λ be equal to $\mathrm{I}^{\delta}_{\max}(A:B)_{\rho(p)}$ with δ as in the statement of the theorem. By Theorem 2.2.7, there exist $\rho'_{AB} \in \mathsf{B}^{\delta}(\rho_{AB})$ and $\sigma_B \in \mathsf{D}(\mathcal{H})$ such that $\rho'_{AB} \leq 2^{\lambda}\rho'_A \otimes \sigma_B$,where $\rho'_{AB} = \sum_x q_x|x\rangle\langle x| \otimes \sigma^x_B$ with $\sum_x q_x = 1$ and $\sigma^x_B \in \mathsf{D}(\mathcal{H})$, and $\rho'_A = \sum_x q_x|x\rangle\langle x|$. Then

$$\sigma^x_B \quad \leq \quad 2^{\lambda}\sigma_B \ , \tag{4.2.1}$$

for all $x \in S$ with $q_x \neq 0$. Note that any σ^x_B with $p_x = 0$ is not important for us, and for each $x \in S$ with $q_x = 0$, we choose $\sigma^x_B = \sigma_B$. Inequality (4.2.1) is exactly in the form of inequality (4.1.1) and therefore we can execute the given protocol in Section 4.1 to perform approximate remote state preparation with $t = \lceil 2^{\lambda} \ln\left(\frac{4+3\epsilon^2}{2\epsilon^4}\right)\rceil$. First, Alice gets input x with probability p_x. She and Bob share t copies of entangled state $|w\rangle$, where $|w\rangle$ is a purification of σ_B. Now they perform the protocol for states σ^x_B and σ_B. The final joint state of Alice's input and Bob's output is

$$\tilde{\rho}_{AB} \quad = \quad \sum_{x\in S} p_x|x\rangle\langle x| \otimes \tilde{\sigma}^x_B \ ,$$

where $\tilde{\sigma}^x_B = (1-(1-2^{-\lambda})^t)\sigma^x_B + (1-2^{-\lambda})^t\frac{\mathbb{1}}{\dim(\mathcal{H})}$. Therefore,

$$\begin{aligned}
\mathrm{F}(\tilde{\rho}_{AB}, \rho'_{AB}) \quad &= \quad \mathrm{F}\left(\sum_{x\in S} p_x|x\rangle\langle x| \otimes \tilde{\sigma}^x_B, \sum_{x\in S} q_x|x\rangle\langle x| \otimes \sigma^x_B\right) \\
&\geq \quad \sqrt{1-(1-2^{-\lambda})^t}\ \mathrm{F}\left(\sum_{x\in S} p_x|x\rangle\langle x| \otimes \sigma^x_B, \sum_{x\in S} q_x|x\rangle\langle x| \otimes \sigma^x_B\right) \\
&= \quad \sqrt{1-(1-2^{-\lambda})^t} \sum_{x\in S} \sqrt{p_x q_x} \\
&\geq \quad \sqrt{1-(1-2^{-\lambda})^t}\left(\sqrt{1-\delta^2}\right) \ ,
\end{aligned}$$

where the first inequality is derived by Equation (2.2.2), and the last one is true since by monotonicity of fidelity we have

$$\begin{aligned}
\sum_{x\in S} \sqrt{p_x q_x} \quad &= \quad \mathrm{F}(\rho'_A, \rho_A) \\
&\geq \quad \mathrm{F}(\rho'_{AB}, \rho_{AB}) \ .
\end{aligned}$$

In addition, by Equation (2.2.3),

$$\begin{aligned}
\mathrm{F}(\tilde{\rho}_{AB}, \rho_{AB}) \quad &\geq \quad \mathrm{F}(\tilde{\rho}_{AB}, \rho'_{AB})^2 + \mathrm{F}(\rho_{AB}, \rho'_{AB})^2 - 1 \\
&\geq \quad (1-\delta^2) + \left(1-(1-2^{-\lambda})^t\right)(1-\delta^2) - 1 \\
&\geq \quad \sqrt{1-\epsilon^2} \ ,
\end{aligned}$$

where the last inequality is derived using inequalities $\ln(1-x) \leq -x$ and $1-\frac{x}{2} \geq \sqrt{1-x}$. Therefore, since $\mathrm{F}(\tilde{\rho}_{AB}, \rho_{AB}) = \sum_{x \in S} p_x \mathrm{F}(\tilde{\sigma}_x, Q(x))$, the protocol performs approximate remote state preparation with average-case error at most ϵ. Since the communication cost of this protocol is $\lceil \log(t+1) \rceil$, the communication complexity of approximate remote state preparation with average-case error ϵ is

$$\begin{aligned}
\mathsf{Q}^*_p(\mathrm{RSP}(S, Q, \epsilon)) &\leq \lceil \log(t+1) \rceil \\
&= \lceil \log(2^\lambda \ln(\frac{4+3\epsilon^2}{2\epsilon^4}) + 1) \rceil \\
&\leq \lambda + \log_2 \ln(\frac{4+3\epsilon^2}{2\epsilon^4}) + 2
\end{aligned}$$

as required. ■

4.2.2 A lower bound

We show that the average-case communication complexity in any protocol for approximate remote state preparation is bounded from below by $\mathrm{I}^\epsilon_{\max}(A:B)_{\rho(p)}$. In order to do this, first we prove the following lemma for smooth max-information.

Lemma 4.2.2. *Let $\epsilon \geq 0$ and $\rho_{MAB} \in \mathsf{D}(\mathcal{M} \otimes \mathcal{H}' \otimes \mathcal{H})$ be any tripartite quantum state that is classical on M. Then*

$$\mathrm{I}^\epsilon_{\max}(A:MB) \quad \leq \quad \mathrm{I}^\epsilon_{\max}(A:B) + \log|M| \quad ,$$

where M, A and B denote the three subsystems of ρ, respectively.

In [7], a similar lemma for any tripartite state is proved, where the upper bound for $\mathrm{I}^\epsilon_{\max}(A:MB)$ is replaced by $\mathrm{I}^\epsilon_{\max}(A:B) + 2\log|M|$.

Proof: Fix $\sigma_B \in \mathsf{D}(\mathcal{H})$ and $\tilde{\rho}_{AB} \in \mathsf{B}^\epsilon(\rho_{AB})$ such that $\mathrm{I}^\epsilon_{\max}(A:B) = \mathrm{D}_{\max}(\tilde{\rho}_{AB} \| \tilde{\rho}_A \otimes \sigma_B) = \lambda$. That is, λ is the minimum non-negative real number for which $\tilde{\rho}_{AB} \leq 2^\lambda \tilde{\rho}_A \otimes \sigma_B$. Then,

$$\frac{\mathbb{1}}{|M|} \otimes \tilde{\rho}_{AB} \quad \leq \quad 2^\lambda \frac{\mathbb{1}}{|M|} \otimes \tilde{\rho}_A \otimes \sigma_B \quad . \tag{4.2.2}$$

By Lemma 2.2.4, there exists some $\rho'_{MAB} \in \mathsf{B}^{\epsilon}(\rho_{MAB})$ such that $\mathrm{Tr}_M(\rho'_{MAB}) = \tilde{\rho}_{AB}$. Consider the quantum-to-classical channel $\Phi : \mathrm{L}(\mathcal{M}) \to \mathrm{L}(\mathcal{M})$ defined by

$$\Phi(X) \quad = \quad \sum_m \langle m|X|m\rangle |m\rangle\langle m|$$

for all $X \in \mathrm{L}(\mathcal{M})$, where $\{|m\rangle\}$ is the orthonormal basis for the Hilbert space $\mathcal{M}$ in which ρ_M is diagonal. Defining $\tilde{\rho}_{MAB} = (\Phi \otimes \mathbb{1})(\rho'_{MAB})$, we get a quantum state $\tilde{\rho}_{MAB}$ that is classical on M, $\mathrm{Tr}_M(\tilde{\rho}_{MAB}) = \tilde{\rho}_{AB}$. Also, since $\rho'_{MAB} \in \mathsf{B}^{\epsilon}(\rho_{MAB})$, by monotonicity of fidelity under quantum operations and the fact that ρ_{MAB} is classical on M, we get that $\tilde{\rho}_{MAB} \in \mathsf{B}^{\epsilon}(\rho_{MAB})$, and it can be written as

$$\tilde{\rho}_{MAB} \quad = \quad \sum_m \gamma_m |m\rangle\langle m| \otimes \sigma^m_{AB} \ ,$$

where all σ^m_{AB} are normalized and $\sum_m \gamma_m \leq 1$. We have $\tilde{\rho}_{MAB} \leq \mathbb{1}_M \otimes \tilde{\rho}_{AB}$. Combining this with Equation (4.2.2), we can conclude that

$$\tilde{\rho}_{MAB} \quad \leq \quad 2^{\lambda}|M| \left(\frac{\mathbb{1}_M}{|M|} \otimes \tilde{\rho}_A \otimes \sigma_B \right)$$

and consequently,

$$\mathrm{D}_{\max}\left(\tilde{\rho}_{MAB} \middle|\middle| \frac{\mathbb{1}_M}{|M|} \otimes \tilde{\rho}_A \otimes \sigma_B \right) \quad \leq \quad \lambda + \log|M| \ .$$

Considering the definition of smooth max-information, this implies that

$$\mathrm{I}^{\epsilon}_{\max}(A : MB) \quad \leq \quad \lambda + \log|M| \ ,$$

as required. ■

Using this lemma, we bound the average-case error communication complexity of $\mathrm{RSP}(S, Q, \epsilon)$ from below.

Theorem 4.2.3. *For any finite set S, function $Q : S \to \mathsf{D}(\mathcal{H})$, and $\epsilon \in [0, 1]$, let p be a probability distribution over S and $\rho(p)$ be the bipartite quantum state*

$$\rho(p) = \sum_{x \in S} p_x |x\rangle\langle x|_B \otimes Q(x)_A \ .$$

Then

$$\mathsf{Q}^*_p(\mathrm{RSP}(S, Q, \epsilon)) \quad \geq \quad \mathrm{I}^{\epsilon}_{\max}(A : B)_{\rho(p)} \ .$$

Proof: First, we prove this theorem for one-way protocols and then we extend it to two-way protocols.

One-way protocols

Consider a one-way LOCC protocol Π for $\mathrm{RSP}(S, Q, \epsilon)$ with average-case error ϵ for the distribution p . In this protocol, Bob does not have any input and Alice is the party who starts the protocol. Let X^A be Alice's input register, Y^A and Y^B be Alice's and Bob's registers holding their private qubits, initially. Let W_i^A and W_i^B be two classical-quantum registers held by Alice and Bob, respectively, after the i-th step of the protocol, where their classical parts are Z_i^A and Z_i^B, respectively, containing the transcript after i-th step, and their quantum parts are Y_i^A and Y_i^B, respectively, which are Y^A and Y^B after step i. Note that X^A does not change during the protocol.

Initially, X^A and Y^B are independent, and so

$$\mathrm{I}_{\max}(X^A : Y^B) = 0 \ .$$

As described in Section 2.2.2, in the first step, Alice performs a general measurement on her qubits Y^A controlled by X^A. So, W_1^A is $Z_1^A Y_1^A$, where Z_1^A contains the measurement outcome and Y_1^A may be different from Y^A, while W_1^B is Y^B. Therefore,

$$\mathrm{I}_{\max}(X^A : W_1^B) \quad = \quad \mathrm{I}_{\max}(X^A : Y^B) \quad = \quad 0 \ .$$

In step 2, Alice sends a copy of the measurement outcome M_i to Bob using m classical bits, and Bob adds the received message in the register Z_2^B. After step 2, Alice's register, W_2^A, is the same as W_1^A, however Bob's register has been changed to W_2^B which is in fact $Z_2^B Y_1^B$, where Y_2^B is Y_1^B. Hence,

$$\mathrm{I}_{\max}(X^A : W_2^B) \quad \leq \quad \mathrm{I}_{\max}(X^A : W_1^B) + m \quad = \quad m \ , \tag{4.2.3}$$

by Lemma 4.2.2.

In step 3, Bob performs a general measurement on his qubits Y_2^B controlled by Z_2^B. After this step, his register W_3^B is an extension of his output σ_x, where σ_x is an approximation of $Q(x)$. By Lemma 2.2.5, we conclude that

$$\begin{aligned} \mathrm{I}_{\max}(X^A : W_3^B) \quad &\leq \quad \mathrm{I}_{\max}(X^A : W_2^B) \\ &\leq \quad m \ , \end{aligned}$$

where the first inequality is derived using Theorem 2.2.5, and the second inequality is true by Equation 4.2.3. Therefore, using Theorem 2.2.5 implies that

$$\mathrm{I}_{\max}(A : B)_{\rho'(p)} \quad \leq \quad m \ ,$$

where A and B are Alice's input and Bob's output registers, respectively, and $\rho'(p) = \sum_x p_x|x\rangle\langle x| \otimes \sigma_x$ is the bipartite quantum state of Alice's input and Bob's output state. By definition of the protocol Π, the purified distance of $\rho(p)$ and $\rho'(p)$ is at most ϵ. As a consequence, $\mathrm{I}_{\max}(A : B)_{\rho'(p)}$ is greater than or equal to $\mathrm{I}^{\epsilon}_{\max}(A : B)_{\rho(p)}$. Therefore, we can conclude that the average-case entanglement-assisted communication complexity of approximate remote state preparation $\mathsf{Q}^*_p(\mathrm{RSP}(S, Q, \epsilon))$ is at least $\mathrm{I}^{\epsilon}_{\max}(A : B)_{\rho(p)}$.

Two-way protocols

Now consider a two-way LOCC protocol Π for $\mathrm{RSP}(S, Q, \epsilon)$ with average-case error ϵ. Similar to the one-way protocol, Bob has no input. Hence, we can assume that Alice starts the protocol. Let X^A be Alice's input register, and Y^A and Y^B be Alice's and Bob's registers holding their private qubits, initially. Let W^A_i and W^B_i be two classical-quantum registers hold by Alice and Bob, respectively, after the i-th round of the protocol, where their classical parts are Z^A_i and Z^B_i, respectively, containing the transcript after i-th round, and their quantum parts are Y^A_i and Y^B_i, respectively, which are Y^A and Y^B after round i. Similar to a one-way protocol, initially, X^A and Y^B are independent, and

$$\mathrm{I}_{\max}(X^A : Y^B) = 0 \ .$$

Now consider round i of a two-way LOCC protocol. As mentioned in Chapter 2.1, there are two possible cases for each round.

Case (1): Alice performs a measurement on Y^A_{i-1} controlled by Z^A_{i-1} and X^A, and adds the outcome of her measurement M_i to Z^A_{i-1}. Let Z^A_i be the registers Z^A_{i-1} and M_i together. Then, she sends a copy of M_i to Bob using m_i bits of communication, and Bob adds M_i to Z^B_{i-1}. Let Z^B_i be Z^B_{i-1} and M_i together. In this case,

$$\begin{aligned}
\mathrm{I}_{\max}(X^A : W^B_i) &= \mathrm{I}_{\max}(X^A : Z^B_i Y^B_i) \\
&\leq \mathrm{I}_{\max}(X^A : Z^B_{i-1} Y^B_{i-1}) + m_i \\
&= \mathrm{I}_{\max}(X^A : W^B_{i-1}) + m_i \ ,
\end{aligned}$$

where the inequality holds by Theorem 4.2.2. Note that Y^B_i is not different from Y^B_{i-1}.

Case (2): Bob performs a measurement on Y^B_{i-1} controlled by Z^B_{i-1}, and adds the outcome of his measurement M_i to Z^B_{i-1}. Let Z^B_i be the register Z^B_{i-1} together with M_i. Then he sends a copy of the outcome M_i to Alice using n_i bits of communication, and Alice adds the received message to Z^A_{i-1}. Let Z^A_i be M_i and Z^A_{i-1}, together. In this case,

$$\mathrm{I}_{\max}(X^A : W^B_i) \quad \leq \quad \mathrm{I}_{\max}(X^A : W^B_{i-1}) \ ,$$

since a controlled measurement can be considered as a quantum channel, and max-information is monotone under quantum channels (Theorem 2.2.5).

Therefore, in any N round two-way protocol,

$$\mathrm{I}_{\max}(X^A : W_N^B) \quad \leq \quad \mathrm{I}_{\max}(X^A : Y^B) + \sum_{i=1}^{N} m_i \ ,$$

assuming that $m_i = 0$ whenever Bob sends a message to Alice (Case(2)). Considering the fact that $\mathrm{I}_{\max}(X^A : Y^B) = 0$, for any two-way protocol with m_A bits of communication from Alice to Bob, we have

$$\mathrm{I}_{\max}(A : B)_{\rho'(p)} \quad \leq \quad m_A \ ,$$

where $\rho'(p)$ is the bipartite quantum state of Alice's input and Bob's output. In addition, by definition of the protocol Π, $\rho'(p)$ belongs to the set $\mathsf{B}^{\epsilon}(\rho(p))$. Therefore, $\mathsf{Q}_p^*(\mathrm{RSP}(S, Q, \epsilon))$ is at least $\mathrm{I}_{\max}^{\epsilon}(A : B)_{\rho(p)}$. ■

4.3 Worst-case error communication complexity

In this section, we give a lower bound and an upper bound for the worst-case error communication complexity of remote state preparation, denoted as $\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon))$, in terms of smooth max-relative entropy.

4.3.1 An upper bound

In this part, we show that for some fixed $\epsilon \in (0, 1]$, the worst-case communication complexity of the approximate remote state preparation problem is upper bounded by

$$\min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x \in S} \mathrm{D}_{\max}^{\delta}(Q(x)||\sigma) + \mathrm{O}(1) \ ,$$

where $\delta = \frac{\epsilon}{\sqrt{1+\epsilon^2}}$. Similar to the upper bound for the average-case, we utilize the protocol explained in Section 4.1.

Theorem 4.3.1. *Let S be a finite set, $Q : S \to \mathsf{D}(\mathcal{H})$ be a function from S to the set of density operators in the Hilbert space $\mathcal{H}$, and $\epsilon \in [0, 1]$. Then*

$$\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon)) \quad \leq \quad \min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x \in S} \mathrm{D}_{\max}^{\delta}(Q(x)||\sigma) + \log_2(1 + \epsilon^2) + \log_2 \ln \frac{1}{\epsilon^4} + 2 \ ,$$

where $\delta = \frac{\epsilon}{\sqrt{1+\epsilon^2}}$.

Proof: Let $\alpha = \min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x\in S} \mathrm{D}^{\delta}_{\max}(Q(x)||\sigma)$ and σ' be the quantum state for which the minimum is achieved, i.e. $\alpha = \max_{x\in S} \mathrm{D}^{\delta}_{\max}(Q(x)||\sigma')$. By definition, for all $x \in S$ there exists some $\sigma_x \in \mathsf{B}^{\delta}(Q(x))$ such that

$$\sigma' \quad \geq \quad 2^{-\alpha}\sigma_x \ .$$

Note that since $\mathrm{P}(\sigma_x, Q(x)) \leq \delta$, we have $\mathrm{F}(\sigma_x, Q(x))^2 \geq 1-\delta^2$. So, by Equation 2.2.1, $\mathrm{Tr}(\sigma_x) \geq 1-\delta^2 = \frac{1}{1+\epsilon^2}$ for all $x \in S$. Now for each $x \in S$, define $\rho_x := \frac{\sigma_x}{\mathrm{Tr}(\sigma_x)}$. Then, for all $x \in S$, ρ_x is a quantum state δ-close to $Q(x)$, i.e. $\rho_x \in \mathsf{B}^{\delta}(Q(x)) \cap \mathsf{D}(\mathcal{H})$, and

$$\begin{aligned} \sigma' &\geq 2^{-\alpha}\mathrm{Tr}(\sigma_x)\rho_x \\ &\geq \frac{2^{-\alpha}}{1+\epsilon^2}\rho_x \ . \end{aligned}$$

This inequality is precisely in the form of inequality (4.1.1). Similar to the proof of Theorem 4.2.1, the protocol in Section 4.1 can be utilized to perform approximate remote state preparation with $t = 2^{\alpha}(1+\epsilon^2)\ln\frac{1}{\epsilon^4}$. At the end of this protocol, Bob's state is

$$\tilde{\sigma}_x \quad = \quad \left[1-(1-2^{-\kappa})^t\right]\sigma_x + (1-2^{-\kappa})^t \frac{\mathbb{1}}{\dim(\mathcal{H})} \ ,$$

where $\kappa = \alpha + \log(1+\epsilon^2)$.

Hence

$$\begin{aligned} \mathrm{F}(Q(x), \tilde{\sigma}_x) &\geq \sqrt{1-(1-2^{-\kappa})^t}\, \mathrm{F}(Q(x), \sigma_x) \\ &\geq \sqrt{1-(1-2^{-\kappa})^t}\sqrt{1-\frac{\epsilon^2}{1+\epsilon^2}} \\ &= \sqrt{\frac{1-(1-2^{-\kappa})^t}{1+\epsilon^2}} \ , \end{aligned}$$

where the first inequality holds by Equation (2.2.2), and the second inequality holds because σ_x is $\frac{\epsilon}{\sqrt{1+\epsilon^2}}$-close to $Q(x)$. On the other hand, using the inequality $\ln(1-x) \leq -x$ and substituting the definition of t, we have

$$\begin{aligned} t\ln(1-2^{-\kappa}) &\leq -\frac{t}{2^{\kappa}} \\ &= \ln\epsilon^4 \ . \end{aligned}$$

Therefore,

$$\mathrm{F}(Q(x), \tilde{\sigma}_x) \quad \geq \quad \sqrt{1-\epsilon^2} \ ,$$

and the purified distance of $Q(x)$ and $\tilde{\sigma}_x$ is at most ϵ. So the protocol performs the remote state preparation with worst-case error ϵ. The communication cost of this protocol is $\lceil \log(t+1) \rceil$. Hence, we have

$$\begin{aligned} Q^*(\mathrm{RSP}(S, Q, \epsilon)) &\leq \lceil \log(t+1) \rceil \\ &= \lceil \log(2^\alpha (1+\epsilon^2) \ln(\frac{1}{\epsilon^4}) + 1) \rceil \\ &\leq \alpha + \log_2(1+\epsilon^2) + \log_2 \ln(\frac{1}{\epsilon^4}) + 2 \ . \end{aligned}$$

Therefore, the upper bound in the statement follows. ■

4.3.2 A lower bound

By definition, any protocol with worst-case error at most ϵ is also a protocol with average-case error at most ϵ. As a consequence, a lower bound for average-case communication complexity is also a lower bound for worst-case communication complexity. In particular, for each probability distribution p, $\mathrm{I}^\epsilon_{\max}(A : B)_{\rho(p)}$ is a lower bound for the worst-case communication complexity of remote state preparation by Theorem (4.2.3). Therefore,

$$\max_p \ \mathrm{I}^\epsilon_{\max}(A : B)_{\rho(p)} \quad \leq \quad \mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon)) \ , \tag{4.3.1}$$

where the maximum is over all probability distributions p on the inputs x.

In the following theorem, we give a lower bound for $\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon))$ in terms of max-relative entropy by exploiting Equation (4.3.1).

Theorem 4.3.2. *Let S be a finite set, $Q : S \to \mathsf{D}(\mathcal{H})$ be a function from S to the set of density operators in Hilbert space $\mathcal{H}$, $\epsilon \in (0, 1]$, and $0 < \delta < \epsilon$. Then*

$$\min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x \in S} \mathrm{D}^\gamma_{\max}(Q(x) || \sigma) - \log \frac{(1-\epsilon^2)(\epsilon^2 + \delta)}{\delta^3} - 3 \log 3 \quad \leq \quad \mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon)) \ ,$$

where $\gamma = \sqrt{2(\epsilon^2 + \delta)}$.

Proof: By definition of the smooth max-information, Equation 4.3.1 implies that

$$\max_{p} \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}^{\epsilon}_{\max}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma) \quad \leq \quad \mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon)) \ . \tag{4.3.2}$$

On the other hand, by Lemma 2.2.12, we have

$$\begin{aligned}
\max_{p} \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}^{\epsilon}_{\max}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma) \quad &\geq \quad \max_{p} \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}^{\lambda}_{\mathrm{h}}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma) - f(\epsilon, \delta) \\
&= \quad \max_{p} \min_{\sigma \in \mathsf{D}(\mathcal{H})} \left(-\log \beta^{\lambda}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma)\right) \\
&\quad + \log(1 - \lambda) - f(\epsilon, \delta) \\
&= \quad -\log\left(\min_{p} \max_{\sigma \in \mathsf{D}(\mathcal{H})} \beta^{\lambda}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma)\right) \\
&\quad + \log(1 - \lambda) - f(\epsilon, \delta) \ ,
\end{aligned}$$

where $\beta^{\lambda}(\rho||\sigma) = \inf\{\langle Q, \sigma\rangle | 0 \leq Q \leq 1 \wedge \langle Q, \rho\rangle \geq 1 - \lambda\}$, $\mathrm{D}^{\lambda}_{\mathrm{h}}(\rho||\sigma) = -\log \frac{\beta^{\lambda}(\rho||\sigma)}{1-\lambda}$, $f(\epsilon, \delta) = \log \frac{(1-\epsilon^2)(\epsilon^2+\delta)}{\delta^3} + 3\log 3$ and $\lambda = 1 - \epsilon^2 - \delta$.

Let A_1 be the set of all probability distributions p, and A_2 be the set of all quantum states $\sigma \in \mathsf{D}(\mathcal{H})$. Viewing σ as an element of the real vector space of Hermitian operators in $\mathsf{L}(\mathcal{H})$, A_1 and A_2 are non-empty, convex and compact subsets of $\mathbb{R}^n$ for some positive integer n. Moreover, by Lemma 2.2.10 and Lemma 2.2.11, $\beta^{\lambda}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma)$ is a continuous function which satisfies both conditions of the minimax theorem (Theorem 2.1.3), and therefore by applying the minimax theorem, we conclude that

$$\begin{aligned}
\max_{p} \min_{\sigma \in \mathsf{D}(\mathcal{H})} \mathrm{D}^{\epsilon}_{\max}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma) \quad &\geq \quad -\log\left(\max_{\sigma \in \mathsf{D}(\mathcal{H})} \min_{p} \beta^{\lambda}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma)\right) \\
&\quad + \log(1 - \lambda) - f(\epsilon, \delta) \\
&= \quad \min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{p} \mathrm{D}^{\lambda}_{\mathrm{h}}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma) - f(\epsilon, \delta) \\
&\geq \quad \min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{p} \mathrm{D}^{\gamma}_{\max}(\rho_{AB}(p)||\rho_A(p) \otimes \sigma) - f(\epsilon, \delta) \\
&\geq \quad \min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x \in S} \mathrm{D}^{\gamma}_{\max}(Q(x)||\sigma) - f(\epsilon, \delta) \ ,
\end{aligned} \tag{4.3.3}$$

where $\gamma = \sqrt{2(1 - \lambda)} = \sqrt{2(\epsilon^2 + \delta)}$ and $f(\epsilon, \delta) = \log \frac{(1-\epsilon^2)(\epsilon^2+\delta)}{\delta^3} + 3\log 3$. Note that the second inequality is derived using Lemma 2.2.12. Thus, combining Equations (4.3.3) and 4.3.2, we get our lower bound for the worst-case error communication complexity of ARSP. ■

4.4 Some observations

In the previous sections, we bounded the communication complexity of the approximate remote state preparation problem (ARSP) for both worst-case error and average-case error. We now discuss the results, especially in light of previous work.

4.4.1 A comparison with previous works

In Section 4.3, we derived upper and lower bounds for the worst-case error communication complexity of ARSP. Now, we study whether our bound is really different from previously known ones. As mentioned in the Introduction, Jain showed that the worst-case communication complexity of RSP is bounded from above by $\frac{\mathsf{T}(Q)}{\left(1-\sqrt{1-\epsilon^2}\right)^2} + \mathrm{O}(1)$ [18]. Here, we show that there exists a function Q for which there is a large separation between the bound in Theorem 4.3.1, and $\frac{\mathsf{T}(Q)}{\left(1-\sqrt{1-\epsilon^2}\right)^2} + \mathrm{O}(1)$. In other words, we show that our upper bound is asymptotically smaller than the bound due to Jain.

To achieve this goal, we use the following information-theoretic result which relates smooth max-entropy of two states to their observational divergence. This theorem is called *"substate theorem"* and the proof can be found in [20, 15].

Theorem 4.4.1. *Let $\mathcal{H}$ be a Hilbert space, and let $\rho, \sigma \in \mathsf{D}(\mathcal{H})$ be quantum states such that* $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$. *For any $\epsilon \in (0,1)$,*

$$\mathrm{D}^{\epsilon}_{\max}(\rho||\sigma) \quad \leq \quad \frac{\mathrm{D}(\rho||\sigma)}{\epsilon^2} + \log\frac{1}{1-\epsilon} \quad .$$

In addition, it has been shown that there exists an ensemble of quantum states for which there is a large separation between its Holevo and Divergence information [19]. (These two quantities have been defined in Section 2.2.4.)

Theorem 4.4.2. *Let N be a positive integer, and $\mathcal{H}$ be a Hilbert space of dimension N. For every positive real number $k \geq 1$ such that $N > 2^{36k^2}$, there is a set S and an ensemble $\mathcal{E} = \{(\lambda_x, \xi_x) : x \in S\}$ of quantum states $\xi_x \in \mathsf{D}(\mathcal{H})$ with $\xi = \sum_{x\in S}\lambda_x\xi_x = \frac{\mathbb{1}}{N}$, such that $\mathrm{D}(Q(x)||\xi) = \mathrm{D}(\mathcal{E}) = k$ for all $x \in S$ and $\chi(\mathcal{E}) \in \Theta(k\log\log N)$.*

It has been also shown that this is the best separation possible for an ensemble of quantum states with a completely mixed ensemble average [19].

In the following theorem, we state such a separation between our upper bound for the worst-case error and the upper bound derived in [19] by using above theorems.

Theorem 4.4.3. *Let S be a set and $\mathcal{H}$ be Hilbert space with dimension N. Then, for every positive real number $k \geq 1$ such that $N > 2^{36k^2}$, there exists a function $Q : S \to \mathsf{D}(\mathcal{H})$ such that $\mathsf{T}(Q) \in \Theta(k \log \log N)$ while*

$$\min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x \in S} \mathrm{D}^{\delta}_{\max}(Q(x) || \sigma) \quad \leq \quad \frac{k}{\delta^2} + \log \frac{1}{1-\delta^2} \ .$$

Proof: Let $\mathcal{E} = \{(\lambda_x, \xi_x) : x \in S\}$ be the ensemble for which Theorem 4.4.2 holds. Let $Q : S \to \mathsf{D}(\mathcal{H})$ be a function such that $Q(x) = \xi_x$ for all $x \in S$. Suppose that $\xi = \sum_{x \in S} \lambda_x \xi_x$ is the ensemble average. Then we have

$$\begin{aligned} \min_{\sigma \in \mathsf{D}(\mathcal{H})} \max_{x \in S} \mathrm{D}^{\delta}_{\max}(Q(x) || \sigma) \quad & \leq \quad \max_{x \in S} \mathrm{D}^{\delta}_{\max}(Q(x) || \xi) \\ & \leq \quad \frac{\max_x \mathrm{D}(Q(x) || \xi)}{\delta^2} + \log \frac{1}{1-\delta^2} \\ & = \quad \frac{\mathrm{D}(\mathcal{E})}{\delta^2} + \log \frac{1}{1-\delta^2} \\ & = \quad \frac{k}{\delta^2} + \log \frac{1}{1-\delta^2} \ , \end{aligned}$$

where the second inequality is derived using the substate theorem (Theorem 4.4.1), and first and second equality hold by Theorem 4.4.2. Moreover, by definition of $\mathsf{T}(Q)$ in Section 2.2.4, we have $\mathsf{T}(Q) \geq \chi(\mathcal{E})$. Therefore, Theorem 4.4.2 implies the existence of the required function Q. ■

In [18], Jain first gave a lower bound for exact remote state preparation. Then he considered approximate remote state preparation and bounded the worst-case error communication complexity of this problem from above. We also point out that considering approximate version decreases the communication cost significantly. He showed that $\frac{\mathsf{T}(Q)}{2}$ is a lower bound for communication complexity of perfect remote state preparation. By Theorem 4.4.3, we can also conclude that for some fixed $\epsilon \in (0, 1]$, there exists a function Q for which $\mathsf{Q}^*(\mathrm{RSP}(S, Q, 0)) \in \Theta(k \log \log N)$, while

$$\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon)) \quad \leq \quad \frac{k}{\delta^2} + \mathrm{O}(1) \ \text{ where } \ \delta = \frac{\epsilon}{2\sqrt{1+\epsilon^2}}.$$

4.4.2 Average-Case Error vs. Worst-Case Error

As we mentioned in Section 4.2, requiring bounded worst-case error is a stronger requirement, and is potentially a more expensive task, compared to the average-case. Here we quantify how much more expensive it could be. In order to answer this question, first we show that for every ϵ, there exists a set S, a function Q and a probability distribution p such that there is a large gap between $Q^*_p(\text{RSP}(S, Q, \epsilon))$ and $Q^*(\text{RSP}(S, Q, \epsilon))$. Then we consider a fixed function Q and a fixed probability distribution p over a set S and find the difference between $Q^*_p(\text{RSP}(S, Q, \epsilon))$ and $Q^*(\text{RSP}(S, Q, \epsilon))$ in terms of ϵ.

To do the first task, we show that for every $\epsilon \in [0, 1/\sqrt{2})$, there exists a set S, a Hilbert space $\mathcal{H}$ with $\dim(\mathcal{H}) = m$, a function $Q : S \to \mathsf{D}(\mathcal{H})$ and a probability distribution p over the set S such that $\mathsf{Q}^*_p(\text{RSP}(S, Q, \epsilon))$ is zero, while $\mathsf{Q}^*(\text{RSP}(S, Q, \epsilon))$ is at least $\log m$. Since any set of quantum states in Hilbert space $\mathcal{H}$ can be prepared with zero error with communication cost $\log m$ exploiting quantum teleportation, this separation is maximal.

Theorem 4.4.4. *Let $S = \{1, \ldots, 2^n\}$ be a set with cardinality 2^n, and $\mathcal{H}$ a Hilbert space with $\dim(\mathcal{H}) = m$ for some positive integer $m \geq 2^n$. There is a function $Q : S \to \mathsf{D}(\mathcal{H})$ such that for any $\epsilon \in [0, \frac{1}{\sqrt{2}})$*

$$\mathsf{Q}^*(\text{RSP}(S, Q, \epsilon)) \quad \geq \quad n \ . \tag{4.4.1}$$

Proof: Let $Q : S \to \mathsf{D}(\mathcal{H})$ be the following function:

$$Q(x) \quad = \quad |x\rangle\langle x| \qquad \text{for all } x \in S \ .$$

We show that this function satisfies Equation (4.4.1). Let X be the random variable corresponding to Alice's input with values in S and uniform distribution. Suppose that Alice is given $x \in S$, and Alice and Bob perform the following protocol.

1. They perform an arbitrary LOCC protocol to prepare a quantum state σ_x which is ϵ-close to $Q(x)$ on Bob's side. (Approximate remote state preparation)
2. Bob performs the projective measurement $\{P_x = |x\rangle\langle x| : \text{for all } x \in S\}$ to discriminate Alice's input.

These two steps together can be considered as an LOCC protocol to convey Alice's input to Bob with communication cost equal to the communication cost of the approximate remote state preparation step.

Let Y be the random variable corresponding to Bob's output. Then the success probability of the above protocol is

$$\begin{aligned}
\Pr[X=Y] &= \sum_{x\in S} \Pr[X=x]\Pr[Y=x|X=x] \\
&= \sum_{x} \frac{1}{2^n}\mathrm{Tr}\left(P_x\sigma_x\right) \\
&= \sum_{x} \frac{1}{2^n}\langle x|\sigma_x|x\rangle \\
&= \sum_{x} \frac{1}{2^n}\mathrm{F}(\sigma_x, Q(x))^2 \\
&\geq \sum_{x} \frac{1-\epsilon^2}{2^n} \\
&\geq 1-\epsilon^2
\end{aligned}$$

By Theorem 3.3.2, any LOCC protocol which conveys n bits of information from Alice to Bob with success probability p_w needs at least $n+\log p_w$ bits of classical communication. As a concequence, the communication cost of the above protocol is at least $n+\log(1-\epsilon^2)$. Note that since $\epsilon\in[0,\frac{1}{\sqrt{2}})$, we can ignore the term $\log(1-\epsilon^2)$ and conclude that

$$\mathsf{Q}^*(\mathrm{RSP}(S,Q,\epsilon)) \quad \geq \quad n\ .$$

■

Now, we choose $\mathcal{H}$ to be a Hilbert space of dimension $m=2^n$. Let p be the probability distribution defined by

$$p_x \quad = \quad \begin{cases} \sqrt{1-\epsilon^2} & x=x_0 \\ \frac{1-\sqrt{1-\epsilon^2}}{2^n-1} & x\neq x_0 \end{cases} \ \text{for some } x_0\in S\ \ , \tag{4.4.2}$$

and Q be the same function as in Proposition 4.4.4. Consider the following protocol.

Protocol: Whatever her input is, Alice does not send any message to Bob, and Bob always prepares the state $Q(x_0)=|x_0\rangle\langle x_0|$.

This is a protocol for approximate remote state preparation with final state

$$\rho'_{AB} \quad = \quad \sum_{x\in S} p_x|x\rangle\langle x|\otimes Q(x_0)$$

and communication cost equal to zero. Since in this protocol

$$\begin{aligned}\mathrm{F}(\rho_{AB}, \rho'_{AB}) &= \mathrm{F}(\sum_{x\in S} p_x |x\rangle\langle x| \otimes Q(x), \sum_{x\in S} p_x |x\rangle\langle x| \otimes Q(x_0)) \\ &\geq \sum_{x\in S} p_x \mathrm{F}(Q(x), Q(x_0)) \\ &= p_{x_0} \quad = \quad \sqrt{1-\epsilon^2} \ ,\end{aligned}$$

we conclude that

$$\mathsf{Q}^*_p(\mathrm{RSP}(S,Q,\epsilon)) \quad = \quad 0 \ .$$

However, by Theorem 4.4.4, we know that $\mathsf{Q}^*(\mathrm{RSP}(S,Q,\epsilon)) \geq \log m$. Hence for the above function Q and $\epsilon \in [0, 1/\sqrt{2})$, there is a gap of $\log m$ between $\mathsf{Q}^*_p(\mathrm{RSP}(S,Q,\epsilon))$ and $\mathsf{Q}^*(\mathrm{RSP}(S,Q,\epsilon))$.

Next we introduce a function Q and a probability distribution p over its domain and quantify the gap between the worst-case and average-case communication complexity of remote state preparation of Q in terms of ϵ.

Let $\mathcal{H}$ be a Hilbert space with $\dim(\mathcal{H}) = n$. Consider the function $Q : \{1,\ldots,n\} \to \mathsf{D}(\mathcal{H})$, such that $Q(x) = |x\rangle\langle x|$ for every $x \in \{1,\ldots,n\}$. Also, consider the geometrically decreasing probability p defined as

$$p_x \quad = \quad \begin{cases} \frac{1}{2^x} & x \in \{1,\ldots,n-1\} \\ \frac{1}{2^{n-1}} & x = n \end{cases} \quad .$$

Now consider the following protocol.

Protocol: If Alice's input x belongs to the set $\{1,\ldots,t\}$ with $t = \min\{\lceil \log \frac{2}{\epsilon^2} \rceil, n\}$, then she sends x to Bob. Otherwise, she sends a random number chosen from the set $\{1,\ldots,t\}$ to Bob. After receiving Alice's message μ, Bob prepares the state $\sigma_x = Q(\mu)$.

In this protocol, the final state of Alice and Bob is

$$\rho'_{AB} \quad = \quad \sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \sigma_x \ ,$$

and consequently

$$\begin{aligned}
\mathrm{F}(\rho_{AB}, \rho'_{AB}) &= \mathrm{F}\left(\sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes Q(x), \sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \sigma_x\right) \\
&= \sum_{x=1}^{n} p_x \mathrm{F}(Q(x), \sigma_x) \\
&= \sum_{x=1}^{t} p_x \\
&= 1 - \frac{1}{2^t} \\
&\geq 1 - \frac{\epsilon^2}{2} \\
&\geq \sqrt{1-\epsilon^2} \ ,
\end{aligned}$$

where the second equality is true since for every $x \in \{t+1, \ldots, n\}$, $\mathrm{F}(Q(x), \sigma_x) = 0$. Therefore, the above protocol is an LOCC protocol with average-case error at most ϵ using $\lceil \log t \rceil$ bits of communication. This implies that

$$\mathsf{Q}_p^*(\mathrm{RSP}(S, Q, \epsilon)) \quad \leq \quad \log_2\left(\min\{\log_2 \frac{2}{\epsilon^2}, \log_2 n\}\right) + 2 \ .$$

On the other hand, as stated in the proof of Theorem 4.4.4, for this function

$$\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon)) \quad \geq \quad \log_2 n + \log_2(1-\epsilon^2) \ .$$

Therefore, we can conclude for Q and p, defined as above, that the gap between $\mathsf{Q}_p^*(\mathrm{RSP}(S, Q, \epsilon))$ and $\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon))$ is at least $\log n + \log_2(1-\epsilon^2) - \log_2\left(\min\{\log_2 \frac{2}{\epsilon^2}, \log_2 n\}\right) - 2$.

According to our approach in finding the gap between $\mathsf{Q}_p^*(\mathrm{RSP}(S, Q, \epsilon))$ and $\mathsf{Q}^*(\mathrm{RSP}(S, Q, \epsilon))$, we can conclude that the more sharply the probability distribution over the domain of Q is decreasing, the bigger this gap can be, and the maximum possible gap happens when we choose the probability distribution as in Equation (4.4.2).

Chapter 5

Conclusion and outlook

In this thesis, we have studied the communication complexity of remote state preparation. Our main results can be summarized as follows:

- The communication complexity of remote state preparation with bounded average-case error ϵ can be characterized in terms of the smooth max-information Bob's output has about Alice's input.
- The communication complexity of remote state preparation with bounded worst-case error ϵ can be characterized in terms of the maximum of the smooth max-relative entropy of $Q(x)$, minimized over the quantum state σ and maximized over all $x \in S$.

We have also shown that our bounds for the worst-case error communication complexity are much tighter than previously known ones. In addition, we have shown that for some functions, the average-case communication complexity can be much smaller than the worst-case. We have also formalized the separation between the average-case and worst-case communication complexity in terms of ϵ.

We have considered the preparation of a quantum state, which can be a mixed state, and studied the communication complexity of this task. However, the desired quantum state may have quantum entanglement with some other systems, say the environment, and one can consider the problem of preparing an approximation of the quantum state such that its entanglement with other systems does not change significantly. This problem has been studied in asymptotic scenario in [3] and [5] asymptotically. In [6], Berta implicitly studied this problem in one-shot scenario by considering the *quantum state merging* problem, and showed that the minimal entanglement cost needed for this problem is equal to minus the ϵ-smooth conditional min-entropy of Alice's register conditioned on the environment, while classical communication is allowed for free. Note that the entanglement cost is defined as the difference between the number of bits of pure entanglement at the beginning and at the end of the process.

The question then arises as to if it is possible to characterize the minimum classical communication of the faithful ARSP in terms of non-asymptotic information theoretic quantities, as well.

References

[1] Charles H. Bennett, Gilles Brassard, Claude Crpeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[2] Charles H. Bennett, David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and William K. Wootters. Remote state preparation. *Physical Review Letters*, 87(7):077902, July 2001.

[3] Charles H. Bennett, Patrick Hayden, Debbie W. Leung, Peter W. Shor, and Andreas Winter. Remote preparation of quantum states. *IEEE Transactions on Information Theory*, 51(1):56–74, January 2005. arXiv:quant-ph/0307100.

[4] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical Review Letters*, 69(20):2881–2884, November 1992.

[5] Dominic W. Berry and Barry C. Sanders. Optimal remote state preparation. *Physical Review Letters*, 90(5), February 2003. arXiv:quant-ph/0209093.

[6] Mario Berta. *Single-shot Quantum State Merging.* Diploma thesis, ETH, Zurich, February 2008.

[7] Mario Berta, Matthias Christandl, and Renato Renner. The quantum reverse shannon theorem based on one-shot information theory. *Communications in Mathematical Physics*, 306(3):579–615, September 2011.

[8] Eric Chitambar, Debbie Leung, Laura Mancinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *arXiv:1210.4583 [quant-ph]*, October 2012.

[9] Nikola Ciganovi, Normand J. Beaudry, and Renato Renner. Smooth max-information as one-shot generalization for mutual information. *arXiv:1308.5884 [quant-ph]*, August 2013.

[10] N. Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, June 2009.

[11] Igor Devetak and Toby Berger. Low-entanglement remote state preparation. *Physical Review Letters*, 87(19), October 2001. arXiv:quant-ph/0102123.

[12] F. Dupuis, L. Kraemer, P. Faist, J. M. Renes, and R. Renner. Generalized entropies. *arXiv:1211.3141 [quant-ph]*, pages 134–153, November 2013. Proceedings of the XVIIth International Congress on Mathematical Physics, Aalborg, Denmark, 2012.

[13] A. Hayashi, T. Hashimoto, and M. Horibe. Remote state preparation without oblivious conditions. *Physical Review A*, 67(5), May 2003. arXiv:quant-ph/0205009.

[14] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problems Inform. Transmission*, 9(3):177—183, 1973.

[15] R. Jain and A. Nayak. Short proofs of the quantum substate theorem. *IEEE Transactions on Information Theory*, 58(6):3664–3669, June 2012.

[16] R. Jain, J. Radhakrishnan, and P. Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings*, pages 429–438, 2002.

[17] R. Jain, J. Radhakrishnan, and P. Sen. Prior entanglement, message compression and privacy in quantum communication. In *Twentieth Annual IEEE Conference on Computational Complexity, 2005. Proceedings*, pages 285–296, June 2005.

[18] Rahul Jain. Communication complexity of remote state preparation with entanglement. *Quantum Info. Comput.*, 6(4):461464, July 2006.

[19] Rahul Jain, Ashwin Nayak, and Yi Su. A separation between divergence and holevo information for ensembles. *Mathematical Structures in Computer Science*, 20(Special Issue 05):977–993, 2010.

[20] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A property of quantum relative entropy with an application to privacy in quantum communication. *J. ACM*, 56(6):33:133:32, September 2009.

[21] Richard Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[22] Eyal Kushilevitz and Noam Nisan. *Communication complexity.* Cambridge University Press, Cambridge, 2006.

[23] Debbie W. Leung and Peter W. Shor. Oblivious remote state preparation. *Physical Review Letters*, 90(12):127905, March 2003.

[24] Hoi-Kwong Lo. Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. *Physical Review A*, 62(1):012313, June 2000.

[25] William Matthews and Stephanie Wehner. Finite blocklength converse bounds for quantum channels. *arXiv:1210.4722 [quant-ph]*, October 2012.

[26] Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *J. ACM*, 53(1):184 206, January 2006.

[27] Ashwin Nayak and Peter Shor. On bit-commitment based quantum coin flipping. *Physical Review A*, 67(1), January 2003. arXiv:quant-ph/0206123.

[28] John von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer DE, 1996.

[29] Michael A Nielsen and Isaac L , Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge; New York, 2000.

[30] Martin J. Osborne and Ariel Rubinstein. *A Course in Game Theory.* MIT Press, 1994.

[31] Renato Renner. *Security of Quantum Key Distribution.* PHD thesis, ETH, Zurich, December 2005.

[32] Renato Renner and Stefan Wolf. Smooth renyi entropy and applications. In *IEEE International Symposium on Information Theory*, page 233, 2004.

[33] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56(9):4674–4681, September 2010. arXiv:0907.5238 [quant-ph].

[34] Marco Tomamichel and Masahito Hayashi. A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Transactions on Information Theory*, 59(11):7693–7710, November 2013. arXiv:1208.1478 [quant-ph].

[35] A. Uhlmann. The transition probability for states of star-algebras. *Annalen der Physik*, 497(4-6):524532, 1985.

[36] Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20), May 2012. arXiv:1007.5456 [quant-ph].

[37] Andrew Chi-Chih Yao. Quantum circuit complexity. In *, 34th Annual Symposium on Foundations of Computer Science, 1993. Proceedings*, pages 352–361, November 1993.