量子资源的量化及其应用

（申请清华大学理学博士学位论文）

培养单位：交叉信息研究院
学　　科：物理学
研 究 生：周游
指导教师：马雄峰副教授

二〇一九年七月

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业/传播，如果出现非法传播的情况，应该责任自负

邵钰莱2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Quantifying quantum resources and its application

Dissertation Submitted to
Tsinghua University
in partial fulfillment of the requirement
for the degree of
Doctor of Philosophy
in
Physics

by
You Zhou

Dissertation Supervisor : Associate Professor Xiongfeng Ma

July, 2019

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰菓2020311340承诺学位论文仅用作个人
学习，不转发不做商业传播，如果
出现非法传播的情况，应该责任自负

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：

清华大学拥有在著作权法规定范围内学位论文的使用权，其中包括：（1）已获学位的研究生必须按学校规定提交学位论文，学校可以采用影印、缩印或其他复制手段保存研究生上交的学位论文；（2）为教学和科研目的，学校可以将公开的学位论文作为资料在图书馆、资料室等场所供校内师生阅读，或在校园网上供校内师生浏览部分内容；（3）根据《中华人民共和国学位条例暂行实施办法》，向国家图书馆报送可以公开的学位论文。

本人保证遵守上述规定。

（保密的论文在解密后遵守此规定）

作者签名：________________ 导师签名：_______________

日　　期：________________ 日　　期：_______________

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业/传播，如果出现非法传播的情况，应该责任自负

邵钰菓2020311340承诺学位论文仅用作个人
学习，不转发不做商业传播，如果
出现非法传播的情况，应该责任自负

摘 要

量子信息科学与技术把量子力学规律应用在信息处理上，产生了例如量子计算，量子通信，量子度量学等子领域。量子信息在过去的四十多年时间里经历了显著的发展和进步。

量子资源，例如量子相干性与量子纠缠，是刻画量子系统有别经典系统的重要特性，在量子信息处理中发挥着举足轻重的作用。量子相干性描述了量子态在一组正交基上的叠加性质，它是很多量子信息与量子物理过程的必要元素，例如量子随机数生成，量子密钥分发，量子热力学以及量子输运。近期的一个重要工作使用量子资源理论严格地刻画了量子相干性。这项工作启发了后续一大批关于相干性的研究，从数学上的刻画与度量，到具体量子信息任务中的操作意义的诠释。量子纠缠，可以看作是量子相干性在两体/多体系统中的体现，它可以产生所谓的“鬼魅般的相互作用”。两体纠缠的研究可以追溯到量子信息领域的诞生之初。多体量子纠缠的研究是当今量子信息中的一个重要方向，它不光在许多量子信息任务，例如多边量子通信和基于测量的量子计算，中有重要的作用，而且为量子多体物理提供了很好的研究角度。由于希尔伯特空间维度随系统粒子数的指数增长，多体量子纠缠探测是一个相当有挑战性的问题。因此发展多体量子纠缠可行的探测方案十分有意义。

本论文主要研究量化量子相干性和量子纠缠，以及其在量子信息处理任务中的应用。首先，我们在量子资源理论的框架下，提出了多项式形式的量子相干性度量，并且系统地研究了该类度量的性质。其次，我们提出了一种评估实验上制备一般对称态保真度的测量方案，该方案可以进一步用来探测纠缠；此外，我们发展了一套系统的基于量子图态的纠缠结构探测方法，该方法的优点是适用于任何图态并且使用的测量数与系统尺寸无关。最后，我们探讨了量子资源在量子密钥分发和量子测量中的作用与意义。

关键词：量子相干性；量子纠缠；量子通信；量子测量；量子计算

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Abstract

Quantum information science and technology where quantum mechanics is utilized to boost information processing, such as computing, communication, and metrology, has being experiencing a rapid development in the past forty years.

Quantum resources, such as quantum coherence and entanglement, distinguish quantum systems from classical ones. Quantum coherence, the superposition of orthogonal quantum states, is indispensable in various quantum processes, such as quantum randomness generation, quantum key distribution, quantum thermodynamics and quantum transport. Quantum coherence was recently formalized under a rigourous framework of resource theory, which stimulated a rapidly growing research field ranging from its mathematical characterizations to its operational interpretations. Quantum entanglement, as a manifestation of coherence in bi/multipatite systems, enables the so-called "spooky actions". The study of bipartite entanglement can date back to the begining of quantum information. Multipartite entanglement draws a intense research these days, which is not only essential in many quantum information tasks, such as multipartite quantum cryptograph and measurement-based quantum computing, but also fundamental in understanding quantum many body physics. The detection of multipartite entanglement is generally challenging due to the exponentially increasing Hilbert space. Thus it is crucial to develop efficient methods to detect entanglement in multipartite systems.

This thesis mainly focuses on quantifying coherence and entanglement, and their applications in quantum information processing. First, we quantify coherence with polynomial-type measure and systemically investigate its properties in the resource theory framework. Then, we propose an efficient protocol to evaluate fidelity between an unknown state and any permutation-invariant state, which can be further applied to entanglement detection; We also develop a systematic method using very few measurements to detect multipartite entanglement structures based on graph states. Lastly, as applications, we study the operational interpretations of quantum resources in quantum key distribution and quantum measurement.

Key Words: Quantum coherence; Quantum multipartite entanglement; Quantum communication; Quantum measurement; Quantum computation

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Contents

Part I Preliminaries 1

Chapter 1 Background 2

Chapter 2 Basic concepts in quantum information 5

- 2.1 Quantum states 5
- 2.2 Qubit system 6
- 2.3 Bipartite and multipartite quantum systems 6
  - 2.3.1 Quantum observable and measurement 7
  - 2.3.2 Quantum gates 8
  - 2.3.3 Quantum channel 9
  - 2.3.4 Distance measures 9
- 2.4 Quantum entropies 10
- 2.5 Quantum coherence 10
  - 2.5.1 Resource theory framework 10
  - 2.5.2 Convex-roof coherence measures 11
  - 2.5.3 Quantum coherence and intrinsic randomness 12
- 2.6 Quantum entanglement 12
  - 2.6.1 Entanglement witness 13

Part II Resource theory of Coherence 15

Chapter 3 Quantifying Coherence: polynomial measure of coherence 16

- 3.1 Polynomial invariant and polynomial coherence measure 17
- 3.2 No-go result of polynomial measure 19
- 3.3 Necessary condition for polynomial coherence measure 21
- 3.4 Typical example: G-coherence measure 23
- 3.5 Discussion 28

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Part III Multipartite entanglement detection 30

Chapter 4 Decomposition of symmetric multipartite observable 31
4.1 Product-state basis for symmetric subspace 32
4.2 Symmetric observable decomposition and fidelity evaluation 34
4.3 Complexity upper bound of Dicke State 38
4.4 Lower bound on Measurement Complexity 42
4.5 Discussion 45

Chapter 5 Efficient detection of multipartite entanglement structure 46
5.1 Definition of multipartite entanglement structure 47
5.2 Graph state and stabilizer formalism 49
5.3 Entanglement structure witness 50
5.4 Robustness of entanglement structure witnesses 56
5.5 Several typical examples 57
5.6 Discussion 60

Part IV Applications in quantum information processing 61

Chapter 6 Operational interpretation of coherence in quantum key distribution 62
6.1 Security framework with coherence 64
6.2 Key rates of BB84 and six-state QKD 68
6.2.1 BB84 protocol 68
6.2.2 Six-state protocol 69
6.3 Improve the key rate with the framework 71
6.3.1 BB84 protocol 72
6.3.2 Six-state protocol 75
6.3.3 Numerical simulation 77
6.4 Practical issue: detection efficiency mismatch 77
6.4.1 Detector model 78
6.4.2 Derivation of the key rate 79
6.4.3 Analytical key rate formula under symmetric attack 82
6.5 Relation with entanglement 84
6.6 Discussion 86

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 7 Interaction-free measurement as quantum channel discrimination 88
7.1 Interaction-free measurement 89
7.1.1 Finite rounds and imperfect absorption 91
7.1.2 Related works 92
7.1.3 Main results 93
7.2 The general model 94
7.3 Simplify the quantum channel for pure state 99
7.4 Opaque object case 102
7.4.1 P_{loss} and P_{error} study with single photon input state 102
7.4.2 P_{loss} and P_{error} study with entangled photon input state 103
7.5 Semitransparent object case 104
7.5.1 Simplify the transforming matrix 105
7.5.2 P_{loss} study with single photon and entangled photon input state 107
7.5.3 P_{error} study with single photon and entangled photon input state 109
7.5.4 $N \to \infty$ behavior 111
7.6 Discussion 113
Bibliography 114
Acknowledgements 125
声　明 126
Appendix A Proofs of polynomial measure of coherence 127
A.1 Proof of Theorem 3.1 for $d = 3$ 127
A.2 Proof for $k = 0$ in Eq. (3-19) 128
A.3 Derivation of Eq. (3-28) 129
Appendix B Details of decomposition of symmetric multipartite observable 130
B.1 Proof of Theorem 4.1 130
B.2 Decomposition of PI state in the product-form basis 132
B.3 Proof of Theorem. 4.4 when $b_i = 0$ or $c_i = 0$ in Eq. (4-41) 134
B.4 Proof of Theorem 4.5 135
Appendix C Details of Efficient detection of multipartite entanglement structure 138
C.1 Witness entanglement structures of graph states 138
C.1.1 Entanglement entropy of graph state 138
C.1.2 Examples: 1-D and 2-D cluster states 139
C.1.3 Witnessing subsystem entanglement structures 141

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

C.1.4 Multi-color graph state 142
C.2 Proof of Corollary 5.1 144
C.3 Proof of Corollary 5.2 145
C.3.1 Proof of Corollary 5.2 of 1-D cluster state 145
C.3.2 Proof of Corollary 5.2 of 2-D cluster state 146
C.4 Proof of Corollary 5.3 147
C.5 Proof of Corollary 5.4 150
Appendix D Details of operational interpretation of coherence in QKD 154
D.1 Quantum bit error correction 154
D.2 Analytical solution to Problem 6.1 155
D.3 Derivation of the key rate K in Eq. (6-73) 157
D.4 Proof of Proposition 6.1 158
D.5 Comparison with the Devetak-Winter formula 158
Appendix E Details of IFM as quantum channel discrimination 160
E.1 Derivation of the quantum channel $\mathcal{E}_I$ of the generic semitransparent object 160
E.2 Non-increasing of the generalized trace distance under quantum operation .. 162
E.3 Proof of Lemma. 7.1 164
E.4 The effect of quantum correlation in IFM considering P_{error} and P_f 164
E.5 Derivation of Eq. (7-67) 165
个人简历、在学期间发表的学术论文与研究成果 167

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

List of denotation

IFM	Interaction-free measurement
GHZ	Greenberger-Horne-Zeilinger
LMS	local measurement setting
PI	permutation invariant
CPTP	complete positive and trace preserving
ICPTP	incoherent CPTP
LOCC	local operations and classical communication
SLOCC	stochastic LOCC
QKD	quantum key distribution
QRNG	quantum random number generator

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Part I

Preliminaries

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 1 Background

Superposition rule accompanied with measurement (or the collapse of wave function) distinguishes quantum mechanics from the classical one. This essential feature is denoted as wave-particle duality for quanta , and the famous gedanken experiment "Schrödinger's cat" demonstrates its peculiarity to the public . In the past four decades, quantum information science and technology where quantum mechanics is utilized to boost the information processing, such as computing, communication, and metrology, has experienced a rapid development.

In quantum computing, the famous Shor's algorithm [Shor (1997)] can factor large number exponentially faster than all the existing classical algorithms, which can threaten some classical encryption schemes, such as the widely-used RSA scheme. However, this kind of algorithm is still hard to realize in laboratory in large scale to surpass the classical supercomputer, since both the qubit number and the control on qubits are limited. Quantum supremacy protocols [Harrow et al. (2017)] such as Boson sampling [Aaronson et al. (2011)], running on the intermediate quantum processors, can achieve some tasks such as generation of some difficult probability distributions, which are believed to be intractable to any classical computers as the qubit number exceeds about 50 [Boixo et al. (2018)]. In addition, quantum simulation [Lloyd (1996)] enables to study many body quantum systems, which is beneficial to condensed matter physics, material design, chemical and biological applications, etc. Moreover, the interplay between quantum computing and artificial intelligence may give us more insight and accelerate the development in both fields [Das Sarma et al. (2019)].

In quantum communication, the first quantum key distribution (QKD) protocol was proposed by Charles Bennett and Gilles Brassard in 1984 (BB84) [Bennett et al. (1984)]. QKD allows two legitimate users to share secret and identical keys, under the eavesdropper who can attack the communication channels with arbitrary strategies allowed by the principles of quantum mechanics. Quantum teleportation [Bennett et al. (1993)] can transfer an unknown quantum state to a remote place based on the pre-shared entangled state with the help of classical communication. Nowadays, quantum communication, especially QKD, becomes more and more practical, such as metropolian QKD networks [Tang et al. (2016)] and satellite-based QKD [Liao et al. (2017); Yin et al. (2017)].

邵钰棐2020311340承诺学位论文仅作个人学习，不转发不做商业使用，如果出现非法传播的情况，应该责任自负

Quantum metrology can estimate the unknown parameter of the physical system more accurately than the classical method [Giovannetti et al. (2006); Wineland et al. (1992)]. Suppose the number of probes is N, the deviation of the result can scale as $1/N$ and reach the so-called Heisenberg limit with the help of quantum mechanics, which shows an enhancement compared with the classical scaling $1/\sqrt{N}$. In addition, quantum effect also benefits other detection processes and can lead to counterfactual detection in some scenario. For example, in the setting of quantum illumination [Lloyd (2008)], correlated photons can effectively decrease detection error. Moreover, quantum effects can lead to some counterfactual detection; in the setting of interaction-free measurement [Elitzur et al. (1993); Kwiat et al. (1995)], the incoming photon can detect the presence/absence of an object without without interacting with the object, which leads to applications in imaging biological substances.

It is no doubt that the improvements on these information tasks would disappear if the quantum phenomena are completely destroyed and the systems degenerate to the classical ones, which is always called decoherence. As a result, it is important to properly quantify the quantum resources (or quantumness) in these processes and identifies their operational meaning. The quantification of quantum resources has several advantages. First, we can calibrate and improve the existing quantum information protocols both in theoretic and experimental aspects, considering the corresponding quantumness; second, we can develop new protocols after thoroughly studying the essential properties of these quantumness; third, the investigation of quantumness can benefit us not only in quantum information but also in quantum physics, such as quantum thermal dynamics, equilibrium and thermalization in quantum many body system, quantum phase transition, exotic quantum orders, etc.

In this thesis, I focus on the quantification of quantum coherence and the detection of multipartite quantum entanglement. Coherence describes the superposition strength of orthogonal basis states. Even though the study of coherence can date back to the early development of quantum optics [Glauber (1963)], the mathematical rigorous treatment was put forward recently in a resource theory framework [Baumgratz et al. (2014); Winter et al. (2016)]. Several coherence measures are proposed and the roles of coherence in various tasks are identified along this line [Streltsov et al. (2017a)]. Entanglement can be viewed as a manifestation of coherence in bi/multipatite systems [Horodecki et al. (2009)]. For instance, the Bell state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ arises from the coherence between $|00\rangle$

邵钰菓2020311340承诺学位论文仅作个人
学习，不转发不做商业传播，如果
出现非法传播的情况，应该责任自负

and $|11\rangle$. The bipartite entanglement has been intensely studied and its importance in information processing has been uncovered in many scenarios, such as quantum teleportation [Bennett et al. (1993)], quantum cryptography [Bennett et al. (1984); Ekert (1991)], and non-locality test [Brunner et al. (2014)]. Multipartite entanglement is a resource for multipartite quantum communication and quantum computing. For example, in the setting of measurement-based quantum computation [Raussendorf et al. (2001, 2003)], one only needs to execute single qubit operations and classical feedback on the initial entangled state to realize universal quantum computing. In addition, multipartite entanglement is also a useful tool to study many body physics [Amico et al. (2008)]. As the particle number increases, the dimension of the Hilbert space grows exponentially with respective to the system size and the entanglement structures become more complex [Guhne et al. (2005); Huber et al. (2013)]. For example, even for a three-qubit system, there are two types of entanglement, i.e., GHZ-type and W-type [Acín et al. (2001); Dür et al. (2000)]. As a result, accurate quantification and efficient detection of multipartite entanglement are significant.

In the remaining of the thesis, we first give preliminaries in Chapter 2, which include basics in quantum information and a brief introduction to quantum coherence and entanglement. Chapter 3 is about quantifying coherence in the resource theory framework, whose content is based on the work polynomial measure of coherence [Zhou et al. (2017b)]. Multipartite entanglement detection is contained in Chapter 4 and 5, where we discuss fidelity evaluation of permutation-invariant states [Zhou et al. (2019b)] and entanglement structure detection based on graph states [Zhou et al. (2019c)], respectively. In Chapter 6 and 7, we show two applications in quantum information processing, one is about the operational interpretation of coherence in QKD [Ma et al. (2018)], the other is about interaction-free measurement [Zhou et al. (2017a)].

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 2 Basic concepts in quantum information

In this chapter, we review the basics of quantum information, which include the quantum state, quantum observable, quantum measurements, quantum gates, distance measures and quantum entropies. Here we only introduce the knowledge related to the contents of the thesis, for more complete review please Ref. [Nielsen et al. (2010); Watrous (2011); Wilde (2013)].

2.1 Quantum states

A (pure) quantum state denoted by $|\psi\rangle$, like the concepts such as the position and velocity in classical physics, is a description of the underlying physical object. For a finite dimensional Hilbert space $\mathcal{H}_d$, the state $|\psi\rangle$ can be written in a superposition form, i.e.,

$$|\psi\rangle = \sum_{i=1}^{d} \alpha_i |i\rangle, \tag{2-1}$$

where $\mathcal{I} = \{|i\rangle\}$ is a set of orthogonal pre-chosen basis, usually called computational basis; α_i is a complex number and $|\alpha_i|^2$ characterizes the probability of finding the state being $|i\rangle$ on account of Born's rule. With normalization, one has $\sum_i |\alpha_i|^2 = 1$. Actually, the state $|\psi\rangle$ can be expanded on any other basis, if the corresponding basis is complete, that is, can span the whole Hilbert space.

Besides the vector representation, a state can also be written in a matrix form, called density matrix, i.e.,

$$\rho = |\Psi\rangle \langle\Psi| . \tag{2-2}$$

From this point of view, the global phase of the state is unimportant. Moreover, normally the state in a real quantum system is not a pure state, since the interaction between the system and environment. A general mixed state can be view as a mixture of several pure states (not necessarily orthogonal),

$$\rho = \sum_j p_j |\Psi_j\rangle \langle\Psi_j| . \tag{2-3}$$

where p_j denotes the probability associated with the pure state $|\Psi_j\rangle$, and $\sum_j p_j = 1$. It is not hard to see that a mixed state can also be represented by a density matrix, with the

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

corresponding matrix being non-negative and the normalization $\mathrm{Tr}(\rho) = 1$

2.2 Qubit system

Qubit is in fact the combination of the words, quantum and bit. Bit is the tiniest quantity in computer science, similarly, qubit is the smallest quantum system with Hilbert space $\mathcal{H}_{d=2}$, which is always realized in the experiment by a two-level physical system. For a classical bit, one uses 0 and 1 to denote its current state, which is either 0 or 1. In contrast, a (pure) qubit state $|\psi\rangle$ can be written as the superposition,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \tag{2-4}$$

To clearly illustrate the concrete state of the state, one always parameterizes the state coefficients as follows,

$$|\psi\rangle_{\theta,\varphi} = \cos(\frac{\theta}{2})\,|0\rangle + e^{i\varphi}\sin(\frac{\theta}{2})\,|1\rangle\,. \tag{2-5}$$

and the state $|\psi\rangle_{\theta,\varphi}$ can be represented as a unit vector on a unit sphere, called Bloch sphere, as shown in Fig.

By introducing the following Pauli matrixes,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2-6}$$

the density matrix of $|\psi\rangle_{\theta,\varphi}$ can be written as,

$$\rho = \frac{\mathbb{I} + n_x\sigma_x + n_y\sigma_y + n_z\sigma_z}{2}, \tag{2-7}$$

where $n_x = \sin(\theta)\cos(\varphi)$, $n_y = \sin(\theta)\sin(\varphi)$ and $n_z = \cos(\theta)$. Note that the state is uniquely determined by the Bloch vector, $\vec{n} = \{n_x, n_y, n_z\}$. For general mixed states, they can also be represented on the Bloch sphere with $|\vec{n}| < 1$.

2.3 Bipartite and multipartite quantum systems

For multipartite systems, for example, the electrons in a real-world material or quantum computation on multi-qubit, the associated Hilbert space is the tensor product of the ones of individual components. For a N-partite system with local dimension being d, the total space is $\mathcal{H} = \mathcal{H}_d^{\otimes N}$. In general, the local dimension of each parties needs not to be the same. For simplicity, let us consider a two-qubit system with $\mathcal{H} = \mathcal{H}_2^{\otimes 2}$. The product state shows,

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle, \tag{2-8}$$

where $|\psi_1\rangle$ and $|\psi_2\rangle$ are the states on the qubit 1 and 2, respectively. In the rest of the thesis, we omit the tensor symbol when it is clear from the content. On the other hand, there are states that correlation between the two qubits, for instance, the Bell states, $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$

$$\begin{aligned} |\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, & |\Phi^-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ |\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, & |\Psi^-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \end{aligned} \tag{2-9}$$

2.3.1 Quantum observable and measurement

An observable is described by a Hermitian operator M, with $M = M^\dagger$, such as the Pauli operators, give in Eq. (2-6). Suppose M has the spectral decomposition,

$$M = \sum_m m P_m, \tag{2-10}$$

where P_m denotes the projector on the subspace with the eigenvalue m. A projective measurement can be described by these projectors. The probability to obtain a specific measurement outcome m is,

$$p(m) = \langle\Psi| P_m |\Psi\rangle, \tag{2-11}$$

and the corresponding state after the measurement is,

$$\frac{P_m |\Psi\rangle}{\sqrt{p(m)}}. \tag{2-12}$$

The expectation value of a observable M is thus given by,

$$\begin{aligned} \langle M\rangle &= \sum mp(m) \\ &= \sum_m m \langle\Psi| P_m |\Psi\rangle \\ &= \langle\Psi| \sum_m m P_m |\Psi\rangle \\ &= \langle\Psi| m |\Psi\rangle . \end{aligned} \tag{2-13}$$

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

2.3.2 Quantum gates

In quantum information an computation, the evolution of quantum state is described by quantum gates, which are realized by engineering the unitary dynamics driven by system Hamiltonian in experiments. Quantum gate is usally selected from a discrete gate set, which is an analog of basic gate, such as and,or,invert, in classical computation. In the following, we introduce several widely-used quantum gates. The Hadamard gate is a single qubit gate showing

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z). \tag{2-14}$$

It can transform between the Z and X basis, i.e.,

$$\begin{aligned} H\sigma_x H^\dagger &= \sigma_z, \\ H\sigma_z H^\dagger &= \sigma_x. \end{aligned} \tag{2-15}$$

Another type of single qubit gate is the rotation along Z basis, the $\frac{\pi}{4}$ gate (or phase) gate S and the $\frac{\pi}{8}$ (or magic) gate T are given by,

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}, \tag{2-16}$$

which can be realized by the rotation $e^{-i\frac{\theta}{2}\sigma_z}$, with $\theta = \frac{\pi}{4}, \frac{\pi}{8}$, respectively.

Besides the single qubit gates, one also needs two-qubit gates to generate correlations between different parties. The Controlled-NOT gate (CNOT) is defined as,

$$\begin{aligned} \text{C-NOT} &= |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_x \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \end{aligned} \tag{2-17}$$

We remark that the gate set $\{T, H, CNOT\}$ is universal for quantum computation in the sense that any multi-qubit unitary can be approximated by them to some accuracy, even though the number involved in the decomposition may be exponential large. On the other hand, the gate set $\{S, H, CNOT\}$ called the Clifford gate, can generate Clifford group on multi-qubit, which can be simulated by classical computer efficiently.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

2.3.3 Quantum channel

Quantum gates describe the perfect unitary evolution of the closed system. However, the underlying experiment system is indeed an open system, since one needs to add different forms of interactions to drive the system and in the same time unwanted noises arise due to unwanted couplings between the system and environment. In quantum information, open quantum system dynamics is described by quantum channels, which is in the following operator-sum form,

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{2-18}$$

where E_i is called Kraus operator, satisfying $\sum_i E_i^\dagger E_i \leq \mathrm{I}$. If there is post-selection, the output state of i-th output is,

$$\mathcal{E}(\rho) = E_i \rho E_i^\dagger / p_i, \quad p_i = \mathrm{Tr}(E_i \rho E_i^\dagger). \tag{2-19}$$

Actually, quantum channel can be realized by a joint unitary operation on the system and environment, followed by a partial trace operation on the environment as follows,

$$\mathcal{E}(\rho) = \sum_k \langle k| U[\rho \otimes |0\rangle \langle 0|] U^\dagger |k\rangle , \tag{2-20}$$

with $E_k = \langle k| U |0\rangle$.

2.3.4 Distance measures

The quantification of the distance between two given quantum states is important in quantum information. Here we introduce two widely-used quantifiers, trace distance and fidelity. The trace distance between two quantum states ρ and σ is given by,

$$D(\rho, \sigma) = \frac{1}{2} \mathrm{Tr}|\rho - \sigma| \tag{2-21}$$

where $|A| = \sqrt{A^\dagger A}$. And the fidelity is defnied as,

$$F(\rho, \sigma) = \mathrm{Tr}\sqrt{\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}}}. \tag{2-22}$$

For a pure state $|\Psi\rangle$ and a general mixed state ρ, the fidelity formula in Eq. (2-22) can be simplified to,

$$F(|\Psi\rangle , \rho) = \sqrt{\langle \Psi| \rho |\Psi\rangle}. \tag{2-23}$$

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

2.4 Quantum entropies

As a generalization of classical entropy to the quantum world, the Von Neumann entropy of the state ρ is defined as,

$$S(\rho) \equiv -\mathrm{Tr}[\rho \log \rho], \tag{2-24}$$

For a bipartite state ρ_{AB}, based on the quantum entropy formula, the mutual information $I(A, B)$ and the conditional entropy $S(A|B)$ show,

$$I(A, B) = S(\rho_A) + S(\rho_A) - S(\rho_{AB}), \tag{2-25}$$

$$S(A|B) = S(\rho_{AB}) - S(\rho_B). \tag{2-26}$$

The conditional entropy quantifies the ignorance of B on A. Interestingly, different from classical world, $H(A|B)$ can be negative for some quantum state, such as the Bell state $|\Psi^+\rangle$. This phenomenon is directly related to quantum entanglement.

2.5 Quantum coherence

With the development of the quantum information theory, a resource framework of coherence has been recently proposed [Baumgratz et al. (2014)], which is used to rigorously characterize, quantify and manipulate quantum coherence resource. In this section, we first review the resource theory of coherence, and show several widely-used coherence measures, with an emphasis on the convex-roof-based measure, finally we introduce a close connection between quantum coherence and intrinsic randomness.

2.5.1 Resource theory framework

In a d-dimensional Hilbert space $\mathcal{H}_d$, there is a set of pre-chosen reference (computational) basis $I = \{|i\rangle\}_{i=1,2,\ldots,d}$, which might be determined by the eigenstates of the system Hamiltonian. The incoherent state contains no coherence whose density matrix are diagonal in this reference basis, $\delta = \sum_{i=1}^{d} p_i |i\rangle\langle i| \in \mathcal{I}$. Denote the set of the incoherent states to be $\mathcal{I}$. The incoherent operation can be expressed as an Incoherent-CPTP (ICPTP) map $\Phi_{ICPTP}(\rho) = \sum_n K_n \rho K_n^\dagger$, in which each Kraus operator satisfies the condition $K_n \rho K_n^\dagger / Tr(K_n \rho K_n^\dagger) \in \mathcal{I}$ if $\rho \in \mathcal{I}$. That is to say, no coherence can be generated from any incoherent states via incoherent operations. Here, the probability to obtain the nth output is denoted by $p_n = \mathrm{Tr}(K_n \rho K_n^\dagger)$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播的情况，应该责任自负，如果出现非法传播

With the definitions of free states and free operations, one can define a coherence measure that quantifies the superposition of reference basis. Generally speaking, a coherence measure $C(\rho)$ maps a quantum state ρ to a non-negative number. There are three criteria for $C(\rho)$, as listed in Table. 2.1 [Baumgratz et al. (2014)]. Note that the criterion $(C1')$ is a stronger version than $(C1)$, and one can obtain $C(2a)$, by combing $C(2b)$ with the convexity $C(3)$.

Table 2.1 Criteria for a coherence measure

$(C1)$	$C(\delta) = 0$ if $\delta \in \mathcal{I}$; $(C1')$ $C(\delta) = 0$ iff $\delta \in \mathcal{I}$
$(C2a)$	Monotonicity: for any incoherent operation $\Phi_{\mathrm{ICPTP}}(\rho)$, $C(\rho) \geq C(\Phi_{\mathrm{ICPTP}}(\rho))$
$(C2b)$	Monotonicity with post-selection: for any incoherent operation $\Phi_{\mathrm{ICPTP}}(\rho) = \sum_n K_n \rho K_n^\dagger$, $C(\rho) \geq p_n C(\rho_n)$, where $\rho_n = K_n \rho K_n^\dagger / p_n$ and $p_n = \mathrm{Tr}(K_n \rho K_n^\dagger)$
$(C3)$	Convexity: $\sum_e p_e C(\rho_e) \geq C(\sum_e p_e \rho_e)$

Based on this coherence framework, several measures are proposed. One type of measure is based on distance measures, such as relative entropy of coherence,

$$C_r(\rho) = \min_{\sigma \in \mathcal{I}} S(\rho \| \sigma) \Delta(\rho^{\mathrm{diag}}) - S(\rho). \tag{2-27}$$

and l_1 norm of coherence [Baumgratz et al. (2014)],

$$C_{l_1}(\rho) = \min_{\sigma \in \mathcal{I}} \|\rho - \sigma\|_{l_1} = \sum_{i \neq j} |\rho_{ij}|. \tag{2-28}$$

2.5.2 Convex-roof coherence measures

Besides coherence measures from distance measures, the other kind is based on convex-roof construction [Winter et al. (2016); Yuan et al. (2015)]. For any coherence measure of pure states $C(|\psi\rangle)$, the convex-roof extension of a general mixed state ρ is defined as

$$C(\rho) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle), \tag{2-29}$$

where the minimization is over all the decompositions $\{p_i, |\psi_i\rangle\}$ of $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$. When $C(|\psi\rangle) = S(\Delta(|\psi\rangle\langle\psi|))$, where S is Von Neumann entropy and $\Delta(\rho) = \sum_i |i\rangle\langle i| \rho |i\rangle\langle i|$ is the dephasing channel on the reference basis I, the corresponding measure is the coherence of formation. When $C(|\psi\rangle) = \max_i |\langle i\rangle \psi|^2$, the corresponding

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

measure is the geometric coherence [Streltsov et al. (2015)]. ①.

2.5.3 Quantum coherence and intrinsic randomness

One important research direction of resource theory of coherence is to identify the operational application of coherence in various quantum information tasks. For instance, under the resource framework of coherence, it is recently observed that the coherence of a quantum state quantifies the extractable intrinsic randomness by measuring it in the reference basis [Yuan et al. (2015, 2016)].

Intrinsic randomness is unpredictable compared with the pseudo-randomness produced by deterministic algorithms. Quantum random number generator serves as an elegant solution to the intrinsic randomness generation, via measuring quantum state in well-designed methods [Herrero-Collantes et al. (2017); Ma et al. (2016b)]. To be more specific, let ρ_A denote the state of system A that is designed to generate random numbers. Consider a purification of ρ_A as $|\psi\rangle_{AE}$, i.e., $\mathrm{Tr}_E[|\psi\rangle_{AE}\langle\psi|_{AE}] = \rho_A$ with Tr_E as the partial trace over system E. In a randomness analysis, the purification system E is normally assumed to be held by Eve, who aims at predicting the measurement outcome of ρ_A by manipulating system E. Suppose a projective measurement on the I basis is performed on ρ_A, then the joint state $\rho_{AE} = |\psi\rangle_{AE}\langle\psi|_{AE}$ becomes $\rho'_{AE} = \sum_i |i\rangle_A\langle i| \otimes \langle i|_A\,\rho_{AE}\,|i\rangle_A$. Considering the independent and identically distributed (i.i.d.) scenario, the intrinsic randomness that is unpredictable to Eve, denoted by $R(\rho_A)$, is measured by the quantum conditional entropy $S(A|E)_{\rho'_{AE}}$. It is shown to be exactly characterized by the relative entropy of coherence $C_r(\rho_S)$ [Yuan et al. (2015, 2016)],

$$R(\rho_A) = S(A|E)_{\rho'_{AE}} = C_r(\rho_A). \tag{2-30}$$

Therefore, the resource theory of coherence provides a useful tool to quantify the intrinsic randomness in the reference basis.

2.6 Quantum entanglement

For a bipartite pure state $|\Psi_{AB}\rangle$, it is said separable if it is a product state,

$$|\Psi_{AB}\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle\,. \tag{2-31}$$

---

① Interestingly, geometric measure is also a distance-based measure, $C(\rho) = 1 - \max_{\sigma\in\mathcal{I}} F(\rho,\sigma)$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

For a mixed state, it is separable if it can be written as a mixture of pure separable states,

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i \tag{2-32}$$

A state ρ is entangled if it is not separable.

The concepts of separability and entanglement can be generalized to multipartite systems. For an N-partite system, a pure state is called m-separable, if it is in the tensor product form for a m-partition, i.e.,

$$|\Psi_m\rangle = \bigotimes_{i=1}^{m} |\Phi_{A_i}\rangle . \tag{2-33}$$

where $\bigcup_{i=1}^{m} A_i = \{N\}$ are m disjoint subsystems. A mixed state is m-separable, if it can be decomposed into a convex mixture of m-separable pure states,

$$\rho_m = \sum_i p_i |\Psi_m^i\rangle \langle\Psi_m^i| , \tag{2-34}$$

with $p_i \geq 0, \forall i$ and $\sum_i p_i = 1$. Note that the partition for each term $|\Psi_m^i\rangle$ in the summation needs not to be same. It is not hard to see that $S_{m+1} \subset S_m$. Define the *entanglement intactness* of a state ρ to be m, iff $\rho \notin S_{m+1}$ and $\rho \in S_m$. Thus, as $\rho \notin S_{m+1}$, the intactness is at most m, i.e., the non-separability can serve as an upper bound of the intactness. When the entanglement intactness is 1, the state possesses genuine multipartite entanglement; and when the intactness is N, the state is fully separable.

2.6.1 Entanglement witness

Entanglement is an essential resource for many quantum information tasks [Horodecki et al. (2009)], such as quantum teleportation [Bennett et al. (1993)], quantum cryptography [Bennett et al. (1984); Ekert (1991)], non-locality test [Brunner et al. (2014)], quantum computing [Nielsen et al. (2010)], quantum simulation [Lloyd (1996)] and quantum metrology [Giovannetti et al. (2006); Wineland et al. (1992)].

Detecting (genuine) entanglement of quantum multipartite state is generally a difficult task, since the the dimension of the Hilbert space increases exponentially with respect to the system size. Compared with the unfeasible quantum state tomography, entanglement witness is an useful tool to realize it. The witness is usually a Hermitian operator $\mathcal{W}$, and it satisfies that $\mathrm{Tr}(\mathcal{W}\sigma_s) \geq 0$ for all separable states $\sigma_s \in S_{sep}$, with S_{sep} denoting the separable state set; $\mathrm{Tr}(\mathcal{W}|\Psi\rangle\langle\Psi|) < 0$ for some entangled state, such as the GHZ state. Consequently, if W returns a negative value, one can confirm that the prepared

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

state is entangled; a non-negative value can not help us to determine whether the state is entangled or not, which is denoted as null result.

A straightforward way to construct a witness is based on the intuition that the prepared state ρ_{pre} is entangled if it is close to a certain target entangled state, say $|\Psi\rangle$. To be specific,

$$\mathcal{W} = \alpha\mathbb{I} - |\Psi\rangle\langle\Psi|, \tag{2-35}$$

where α is the maximal fidelity between $|\Psi\rangle$ and all separable states σ_s, i.e. $\alpha = sup\{\langle\Psi|\sigma_s|\Psi\rangle\,|\sigma_s \in S_{sep}\}$. On account of the convexity of S_{sep}, α can be determined by the maximal Schmit coefficient of $|\Psi\rangle$ optimized under all bipartitions. For instance, $\alpha = \frac{1}{2}$ for the GHZ state. The expectation value of $\mathcal{W}$ shows, $\mathrm{Tr}(\mathcal{W}\rho_{pre}) = \alpha - \mathrm{Tr}(|\Psi\rangle\langle\Psi|\rho_{pre})$, which is directly related to measuring fidelity. Normally, the multipartite projector $|\Psi\rangle\langle\Psi|$ is decomposed to a few of local measurement settings, for example $\sigma_x^{\otimes N}$, which can be realized in experiments. Even for one LMS, it needs thousands of times of the measurement to obtain the accurate expectation value. Thus the total number of LMSs characterize the efficiency of the witness. For the GHZ state, it needs $N + 1$ LMSs to evaluate the fidelity.

Comparing to evaluating the fidelity exactly, one can alternatively lower bound the fidelity with less number of local measurements and in the same time obtain a witness that is weaker than the original one. In general, there is a trade-off between the efficiency and the robustness of the witness, which characterize the detection ability of the underlying witness. We remark this kind of detection method for genuine multipartite entanglement can be generalized to multipartite entanglement structure.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Part II

Resource theory of Coherence

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰粟2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 3 Quantifying Coherence: polynomial measure of coherence

Coherence describes a unique feature of quantum mechanics — superposition of orthogonal states. The study of coherence can date back to the early development of quantum optics [Glauber (1963)], where interference phenomenon is demonstrated for the wave-particle duality of quantum mechanics. In quantum information, coherence acts as an indispensable ingredient in many tasks, such as quantum computing [Nielsen et al. (2010)], metrology [Braunstein et al. (1996)], and randomness generation [Ma et al. (2016b)]. Furthermore, coherence also plays an important role in quantum thermodynamics [Åberg (2014); Lostaglio et al. (2015a,b)], and quantum phase transition [Çakmak et al. (2015); Karpat et al. (2014)].

With the development of the quantum information theory, a resource framework of coherence has been recently proposed [Baumgratz et al. (2014)]. The free state and the free operation are two elementary ingredients in a quantum resource theory. In the resource theory of coherence, the set of free states is a collection of all quantum states whose density matrices are diagonal in a reference computational basis $I = \{|i\rangle\}$. The free operations are incoherent complete positive and trace preserving (ICPTP) operations, which cannot map any incoherent state to a coherent state. With the definitions of free states and free operations, one can define a coherence measure that quantifies the superposition of reference basis. Based on this coherence framework, several measures are proposed, such as relative entropy of coherence, l_1 norm of coherence [Baumgratz et al. (2014)], and coherence of formation [Winter et al. (2016); Yuan et al. (2015)]. Moreover, coherence in distributed systems [Chitambar et al. (2016c); Streltsov et al. (2017b)] and the connections between coherence and other quantum resources are also developed along this line [Chitambar et al. (2016a); Ma et al. (2016a); Streltsov et al. (2015)].

Inspired by the polynomial invariant in entanglement theory, we investigate polynomial measure of coherence in this section. First, in Sec. 3.1, we give the definition of polynomial coherence measure. Then, in Sec. 3.2, we show a no-go theorem for polynomial coherence measures. That is, if the coherence measure only vanishes on incoherent states, there is no such polynomial coherence measure when system dimension is larger than 2. Moreover, in Sec. 3.3, we permit some superposition states to take zero-coherence, and we find a necessary condition for polynomial coherence measures. In Sec. 3.4, we construct a polynomial coherence measure for pure states, which shows similar form with the G-concurrence in entanglement measure. In addition, we derive an analytical result for symmetric states and give a lower bound for general states. The content of this chapter is from the work [Zhou et al. (2017b)].

3.1 Polynomial invariant and polynomial coherence measure

One important class of coherence measures is based on the convex-roof construction [Yuan et al. (2015)]. For any coherence measure of pure states $C(|\psi\rangle)$, the convex-roof extension of a general mixed state ρ is defined as

$$C(\rho) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i C(|\psi_i\rangle), \tag{3-1}$$

where the minimization is over all the decompositions $\{p_i, |\psi_i\rangle\}$ of $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. In general, the minimization problem in Eq. (3-1) is extremely hard. In particular, analytical formula of the coherence of formation is only obtained for qubit states. The efficient calculation for this class of coherence measure is still an open problem.

This is very similar to quantifying another well-known quantum resource, entanglement, where free states are separable states and free operations are local operations and classical communication [Horodecki et al. (2009)]. In entanglement measures, convex-roof constructions have been widely studied [Bennett et al. (1996b); Uhlmann (1998)]. Similarly, the minimization problem is generally hard. Fortunately, there are two solvable cases, concurrence [Hill et al. (1997); Wootters (1998)] and three-tangle [Coffman et al. (2000)]. Both of them are related to a very useful class of functions, referred as *polynomial invariant* [Eltschka et al. (2014)]. A polynomial invariant is a homogenous polynomial function of the coefficients of a pure state, $P_h(|\psi\rangle)$, which is invariant under stochastic local operations and classical communication (SLOCC) [Dür et al. (2000)]. Denote h to be the degree of the polynomial function, for an N-qudit state $|\psi\rangle$,

$$P_h(\kappa L |\psi\rangle) = \kappa^h P_h(|\psi\rangle), \tag{3-2}$$

where κ is an arbitrary scalar and $L \in \mathcal{SL}(d, \mathbb{C})^{\otimes N}$ is a product of invertible linear operators representing SLOCC. For an entanglement measure of pure states, one can add a positive power m to the absolute value of the polynomial invariant,

$$E_h^m(|\psi\rangle) = |P_h(|\psi\rangle)|^m, \tag{3-3}$$

where the overall degree is hm. Polynomial invariants are used to classify and quantify various types of entanglement in multi-qubit [Djokovic et al. (2009); Osterloh et al. (2005)] and qudit systems [Gour et al. (2013)]. Specifically, the convex-roof of concurrence can be solved analytically in the two-qubit case [Wootters (1998)], and the three-tangle for three-qubit is analytically solvable for some special mixed states [Jung et al. (2009); Lohmayer et al. (2006); Siewert et al. (2012)]. Recently, a geometric approach [Regula et al. (2016)] is proposed to analyse the convex-roof extension of polynomial measures for the states of more qubits in some specific cases.

Inspired by the polynomial invariant in entanglement measure, we investigate polynomial measure of coherence as follows. Denote a homogenous polynomial function of degree-h, constructed by the coefficients of a pure state $|\psi\rangle = \sum_{i=1}^d a_i |i\rangle$ in the computational basis, as

$$P_h(|\psi\rangle) = \sum_{k_1,k_2,\ldots,k_d} \chi_{k_1k_2\cdots k_d} \prod_{i=1}^d a_i^{k_i}, \tag{3-4}$$

where k_i are the nonnegative integer power of a_i, $\sum k_i = h$, and $\chi_{k_1k_2\cdots k_d}$ are coefficients. Then after imposing a proper power $m > 0$ on the absolute value of a homogenous polynomial, one can construct a coherence measure as,

$$C_p(|\psi\rangle) = |P_h(|\psi\rangle)|^m, \tag{3-5}$$

where the overall degree is hm, and the subscript p is the abbreviation for polynomial.

A polynomial coherence measure for pure states $C_p(|\psi\rangle)$ can be extended to mixed states by utilizing the aforementioned convex-roof construction. Generally speaking, a coherence measure $C(\rho)$ maps a quantum state ρ to a non-negative number. There are three criteria for $C(\rho)$, as listed in Table. 2.1 [Baumgratz et al. (2014)]. In this chapter, we consider $C(2b)$, the monotonicity under ICPTP with post-selection, instead of the weaker version $C(2a)$, the monotonicity on average. We denote $C(2b)$ as $C(2)$ for simplicity without confusion. Note that if the pure-state measure Eq. (3-5) satisfies the coherence measure criteria listed in Table 2.1, the mixed-state measure via the convex-roof construction Eq. (3-1) would also satisfy these criteria [Yuan et al. (2015)].

邵钰棊2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

3.2 No-go result of polynomial measure

The simplest example of polynomial coherence measure is the l_1-norm for $d = 2$ on pure state. For a pure qubit state, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the l_1-norm coherence measure takes the sum of the absolute value of the off-diagonal terms in the density matrix,

$$C_{l_1}(|\psi\rangle) = |\alpha\beta^*| + |\alpha^*\beta| = 2|\alpha\beta|. \tag{3-6}$$

By the definition of Eq. (3-5), C_{l_1} is the absolute value of a degree-2 homogenous polynomial function with a power $m = 1$. Meanwhile, this coherence measure satisfies the criteria $(C1')$, $(C2)$, and $(C3)$ [Baumgratz et al. (2014)]. Then its convex-roof construction via Eq. (3-6) turns out to be a polynomial coherence measure satisfying these criteria. Note that when the function Eq. (3-6) is extended to $d > 2$, it cannot be expressed as the absolute value of a homogenous polynomial function. Thus, when $d > 2$, the l_1-norm coherence measure is not a polynomial coherence measure.

Surprisingly, for $d > 2$, there is no polynomial coherence measure that satisfies the criterion $(C1')$. In order to show this no-go theorem, we first prove the following Lemma.

Lemma 3.1: For any polynomial coherence measure $C_p(|\psi\rangle)$ and two orthogonal pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, there exists two complex numbers α and β such that

$$C_p(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) = 0 \tag{3-7}$$

where $|\alpha|^2 + |\beta|^2 = 1$. That is, there exists at least one zero-coherence state in the superposition of $|\psi_1\rangle$ and $|\psi_2\rangle$.

Proof. Since $m > 0$, the roots of $C_p(|\psi\rangle) = 0$ in Eq. (3-5) are the same with the ones of $|P_h(|\psi\rangle)| = 0$ in Eq. (3-4). That is, we only need to prove Lemma for the case of $m = 1$. Since $P_h(|\psi\rangle)$ is a homogenous polynomial function of the coefficients of $|\psi\rangle$, one can ignore its global phase. Thus, any pure state in the superposition of $|\psi_1\rangle$ and $|\psi_2\rangle$ can be represented by

$$|\psi\rangle = \frac{|\psi_1\rangle + \omega|\psi_2\rangle}{\sqrt{1+|\omega|^2}}, \tag{3-8}$$

where the global phase is ignored, ω is a complex number containing the relative phase, and $|\psi\rangle \to |\psi_2\rangle$, as $|\omega| \to \infty$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

First, if $C_p(|\psi_2\rangle) = 0$, the Lemma holds automatically. When $C_p(|\psi_2\rangle) > 0$, $C_p(|\psi\rangle)$ can be written as,

$$\begin{aligned} C_p(|\psi\rangle) &= \left| P_h\left(\frac{|\psi_1\rangle + \omega\,|\psi_2\rangle}{\sqrt{1+|\omega|^2}}\right)\right|, \\ &= (1+|\omega|^2)^{-h/2}|P_h(|\psi_1\rangle + \omega\,|\psi_2\rangle)|, \end{aligned} \tag{3-9}$$

since P_h a homogenous polynomial function of degree h. Note that the condition $C_p(|\psi_2\rangle) > 0$, i.e.,

$$\lim_{\omega\to\infty}(1+|\omega|^2)^{-h/2}|P_h(|\psi_1\rangle + w\,|\psi_2\rangle)| > 0, \tag{3-10}$$

guarantees that the coefficient of ω^h in $P_h(|\psi_1\rangle + \omega\,|\psi_2\rangle) = 0$ is nonzero. Then, there are h roots of the homogenous polynomial function of ω,

$$P_h(|\psi_1\rangle + \omega\,|\psi_2\rangle) = 0, \tag{3-11}$$

denoted by $\{z_1, z_2 \ldots, z_h\}$. Thus, $C_p(|\psi\rangle)$ can be expressed as

$$C_p(|\psi\rangle) = A(1+|\omega|^2)^{-h/2}\prod_{i=1}^{h}|\omega - z_i|, \tag{3-12}$$

where $A > 0$ is some constant. In summary, we find at least one ω, $\alpha = (1+|\omega|^2)^{-1/2}$ and $\beta = \omega(1+|\omega|^2)^{-1/2}$, such that $C_p(|\psi\rangle) = 0$

■

Theorem 3.1： There is no polynomial coherence measure in $\mathcal{H}_d$ with $d \geq 3$ that satisfies the criterion $(C1')$.

Proof. In the following proof, we focus on the case of $d \geq 4$ and leave $d = 3$ in Appendix A.1. With $d \geq 4$, we can decompose $\mathcal{H}_d$ into two orthogonal subspaces $\mathcal{H}_{d_1} \oplus \mathcal{H}_{d_2}$ in the computational basis, i.e., $\mathcal{H}_{d_1} = \{|i\rangle_{i=1,\cdots,d_1}\}$ and $\mathcal{H}_{d_2} = \{|i\rangle_{i=d_1+1,\cdots,d}\}$ with the corresponding dimensions d_1 and $d_2 = d - d_1$ both larger than 2.

Suppose there exist a polynomial coherence measure $C_p(|\psi\rangle)$ such that the criterion $(C1')$ listed in Table 2.1 can be satisfied. Then, there are exactly d zero-coherence pure states $|i\rangle$ $(i = 1,\cdots,d)$, which form the reference basis. One can pick up two coherent states, $|\psi_1\rangle \in \mathcal{H}_{d_1}$ and $|\psi_2\rangle \in \mathcal{H}_{d_2}$. That is, $C_p(|\psi_1\rangle) > 0$ and $C_p(|\psi_2\rangle) > 0$. Since two subspaces $\mathcal{H}_{d_1}$ and $\mathcal{H}_{d_2}$ are orthogonal, any superposition of these two states,

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

$\alpha |\psi_1\rangle + \beta |\psi_2\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, should not equal to any of the reference basis states, i.e., $\alpha |\psi_1\rangle + \beta |\psi_2\rangle \neq |i\rangle, \forall i = 1, \cdots, d$. Thus, due to the criterion $(C1')$, we have

$$C_p(\alpha |\psi_1\rangle + \beta |\psi_2\rangle) > 0. \tag{3-13}$$

On the other hand, for the polynomial coherence measure $C_p(|\psi\rangle)$, Lemma 3.1 states that provided any two orthogonal pure states $|\psi_1\rangle$, $|\psi_2\rangle$, there exists at least a pair of complex numbers, α and β, such that $\alpha |\psi_1\rangle + \beta |\psi_2\rangle$ is a zero-coherence state, i.e.,

$$C_p(\alpha |\psi_1\rangle + \beta |\psi_2\rangle) = 0. \tag{3-14}$$

Therefore, it leads to a contradiction. ■

3.3 Necessary condition for polynomial coherence measure

In Theorem 3.1, we have shown a no-go result of polynomial coherence measure for $d \geq 3$ when the criterion $(C1')$ in Table 2.1 is considered. In the following discussions, we study polynomial coherence measure with the criteria $(C1)$, $(C2)$, and $(C3)$. Then, there will be some coherent states whose coherence measure is zero. This situation also happens in entanglement measures, such as negativity, which remains zero for the bound entangled states [Horodecki (1997)]. Here, we focus on the pure-state case and employ the convex-roof construction for general mixed states. As presented in the following theorem, we find a very restrictive necessary condition for polynomial coherence measures that $C_p(|\psi\rangle) = 0$, for all $|\psi\rangle$ whose support does not span all the reference bases $\{i\}$.

Theorem 3.2: For any $|\psi\rangle \in \mathcal{H}_d$, the value of a polynomial coherence measure $C_p(|\psi\rangle)$ should vanish if the rank of the corresponding dephased state $\Delta(|\psi\rangle\langle\psi|)$ is less than d, i.e., $rank(\Delta(|\psi\rangle\langle\psi|)) < d$.

Proof. Suppose there exists $|\psi_1\rangle \in \mathcal{H}_d$ such that $C_p(|\psi_1\rangle) > 0$ and $rank(\Delta(|\psi_1\rangle\langle\psi_1|)) = d_1 < d$. Without loss of generality, $|\psi_1\rangle$ is assumed to be in the subspace $\mathcal{H}_{d_1} = spanned\{|1\rangle, |2\rangle, \cdots, |d_1\rangle\}$. Define the complementary subspace to be $\mathcal{H}_{d_2} = spanned\{|d_1+1\rangle, |d_1+2\rangle, \cdots, |d\rangle\}$, where $d_2 = d - d_1 > 0$. We prove this theorem by two steps.

Step 1: we show that if $d_1 \leq d/2$, then $C_p(|\psi_1\rangle) > 0$ leads to a contradiction to Lemma 3.1. Now that $d_1 \leq d/2 \leq d_2$, there exists a relabeling unitary U_t that transforms the bases

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

in $\mathcal{H}_{d_1}$ to parts of the bases in $\mathcal{H}_{d_2}$. For instance, $\mathcal{H}_{d_1} = spanned\{|1\rangle, |2\rangle\}$ and $\mathcal{H}_{d_2} = spanned\{|3\rangle, |4\rangle, |5\rangle\}$, then U_t can be chosen as $|1\rangle\langle 3| + |3\rangle\langle 1| + |2\rangle\langle 4| + |4\rangle\langle 2| + |5\rangle\langle 5|$. In fact, U_t and $U_t^\dagger$ are both incoherent operation, since they just exchange the index of the reference bases. Assume that U_t maps $|\psi_1\rangle$ to a new state $|\psi_2\rangle = U_t|\psi_1\rangle \in \mathcal{H}_{d_2}$, then we have $\langle\psi_1\rangle\,\psi_2 = 0$. Due to the criterion $(C2)$, it is not hard to show that an incoherent unitary transformation does not change the coherence,

$$C_p(|\psi_1\rangle) = C_p(|\psi_2\rangle). \tag{3-15}$$

Define another incoherent operation, composed by two operators $P_1 = \sum_{i=1}^{d_1} |i\rangle\langle i|$ and $P_2 = \sum_{i=d_1+1}^{d} |i\rangle\langle i|$ that project states to $\mathcal{H}_{d_1}$ and $\mathcal{H}_{d_2}$, respectively,

$$\Phi_{ICPTP}(\rho) = \sum_{i=1,2} P_i \rho P_i^\dagger, \tag{3-16}$$

which represents a dephasing operation between the two subspaces. Then, for any superposition state, $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, its coherence measure should not increase under the ICPTP operation with post-selection, as required by $(C2)$ in Table. 2.1,

$$\begin{aligned} C_p(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) &= |\alpha|^2 C_p(|\psi_1\rangle) + |\beta|^2 C_p(|\psi_2\rangle) \\ &= C_p(|\psi_1\rangle) > 0. \end{aligned} \tag{3-17}$$

where the last equality comes from Eq. (3-15). Therefore, $C_p(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) > 0$ for any α and β. This leads to a contradiction to Lemma 3.1.

Step 2: we show that if $d/2 < d_1 < d$, then $C_p(|\psi_1\rangle) > 0$ also leads to a contradiction. Now that $0 < d_2 < d/2 < d_1 < d$, for any $|\psi_2\rangle \in \mathcal{H}_{d_2}$, we have $C_p(|\psi_2\rangle) = 0$ due to the above proof in Step 1.

Similar to the proof of Lemma 3.1, we only need to consider the case of $m = 1$ and we can get the coherence measure for the superposition state of $|\psi_1\rangle \in \mathcal{H}_{d_1}$ and $|\psi_2\rangle \in \mathcal{H}_{d_2}$ as $(1 + |\omega|^2)^{-h/2}|P_h(|\psi_1\rangle + \omega|\psi_2\rangle)|$. Since

$$C_p(|\psi_2\rangle) = \lim_{\omega\to\infty}(1 + |\omega|^2)^{-h/2}|P_h(|\psi_1\rangle + w|\psi_2\rangle)| = 0, \tag{3-18}$$

the largest degree of ω in the polynomial $P_h(|\psi_1\rangle + \omega|\psi_2\rangle)$, denoted by μ, is smaller than the degree h.

When $\mu = 0$, i.e., the polynomial is a constant, we denote its absolute value by k. Then the coherence measure becomes,

$$C_p(|\psi\rangle) = k(1 + |\omega|^2)^{-h/2}. \tag{3-19}$$

邵钰棐2020311340承诺学位论文仅作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

We show that the constant $k = 0$ in Appendix A.2. As a result, $C_p(|\psi_1\rangle) = 0$. This leads to a contradiction to our assumption that $C_p(|\psi_1\rangle) > 0$.

When $0 < \mu < d$, i.e., $P_h(|\psi_1\rangle + \omega |\psi_2\rangle)$ is a non-constant polynomial of ω, there exists at least one root $|z| < \infty$, such that $P_h(|\psi_1\rangle + z |\psi_2\rangle) = 0$. Then, we can find that the coherence measure of the state $|\psi_r\rangle = (|\psi_1\rangle + z |\psi_2\rangle)/\sqrt{1 + |z|^2}$ is $C_p(|\psi_r\rangle) = 0$. Next, we apply the ICPTP operation described in Eq. (3-16) on $|\psi_r\rangle$ and obtain,

$$\begin{aligned} C_p(|\psi_r\rangle) &\geq \frac{1}{1+|z|^2} C_p(|\psi_1\rangle) + \frac{|z|^2}{1+|z|^2} C_p(|\psi_2\rangle) \\ &= \frac{1}{1+|z|^2} C_p(|\psi_1\rangle), \end{aligned} \tag{3-20}$$

where we use $C_p(|\psi_2\rangle) = 0$ in the equality. Combing the fact that $C_p(|\psi_r\rangle) = 0$, we can reach the conclusion that $C_p(|\psi_1\rangle) = 0$. This leads to a contradiction to our assumption that $C_p(|\psi_1\rangle) > 0$. ■

3.4 Typical example: G-coherence measure

From Theorem 3.2, we can see that only the states with a full support on the computational basis could have positive values of a polynomial coherence measure. Here, we give an example of polynomial coherence measure satisfying this condition, which takes the geometric mean of the coefficients, for $|\psi\rangle = \sum_{i=1}^{d} a_i |i\rangle$,

$$C_G(|\psi\rangle) = d|a_1 a_2 \cdots a_d|^{2/d}. \tag{3-21}$$

Note that it is a degree-d homogenous polynomial function modulated by a power $m = 2/d$. This definition is an analogue to the G-concurrence in entanglement measure, which is related to the geometric mean of the Schmidt coefficients of a bipartite pure state [Gour (2005)]. Hence we call the coherence measure defined in Eq. (3-21) *G-coherence measure*. Since the geometric mean function is a concave function [Boyd et al. (2004)], following Theorem 1 in Ref. [Du et al. (2015b)], we can quickly show that the G-coherence measure satisfies the criteria $(C1)$, $(C2)$ and $(C3)$.

When $d = 2$, the G-coherence measure becomes the l_1-norm measure on pure state. When $d > 2$, according to Theorem 3.2, there is a significant amount of coherent states whose G-coherence is zero. For instance, in the case of $d = 3$, the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ has zero G-coherence and this state cannot be transformed to a coherent state $|\psi\rangle$, where $rank(\Delta(|\psi\rangle\langle\psi|)) = 3$, via a probabilistic incoherent operation [Winter et al. (2016)].

$C_p(\frac{|0\rangle+|2\rangle}{\sqrt{2}}) = 0\, \mathcal{H}_3 = spanned\{|0\rangle, |1\rangle, |2\rangle\}$ Now we move onto the mixed states with the convex-roof construction. In fact, searching for the optimal decomposition in Eq. (3-1) is generally hard. However, like the entanglement measures, there exist analytical solutions for the states with symmetries [Terhal et al. (2000); Vollbrecht et al. (2001)]. Here, we study the states related to the permutation group G_s on the reference basis. A element $g \in G_s$ is defined as

$$g = \begin{pmatrix} 1 & 2 & \dots & d \\ i_1 & i_2 & \dots & i_d \end{pmatrix} \tag{3-22}$$

and the order (the number of the elements) of G_s is $d!$. The corresponding unitary of g is denoted as $U_g = \sum_k |i_k\rangle \langle k|$. Then we have the following definition.

Definition 3.1： A state ρ is a symmetric state if it is invariant under all the permutation unitary operations, i.e., $\forall g \in G_s$, $U_g \rho U_g^\dagger = \rho$.

Denote the symmetric state as ρ^s and the symmetric state set as S. Given the maximally coherent state $|\Psi_d\rangle = \frac{1}{\sqrt{d}} \sum_i |i\rangle$, it is not hard to show the explicit form of symmetric states,

$$\rho^s = p\,|\Psi_d\rangle \langle \Psi_d| + (1-p)\frac{\mathbb{I}}{d}, \tag{3-23}$$

which is only determined by a single parameter, the mixing probability $p \in [0,1]$. Apparently, the symmetric state ρ^s is a mixture of the maximally coherent state $|\Psi_d\rangle$ and the maximally mixed state $\mathbb{I}/d$. The state $|\Psi_d\rangle$ is the only pure state in set S. Borrowing the techniques used in quantifying entanglement of symmetric states [Sentís et al. (2016); Vollbrecht et al. (2001)], we obtain an analytical result $C_G(\rho^s)$ in Theorem 3.3, following Lemma 3.2 and Lemma 3.3.

First, we consider a map

$$\Lambda(\rho) = \frac{1}{|G_s|} \sum_g U_g \rho U_g^\dagger. \tag{3-24}$$

It uniformly mixes all the permutation unitary U_g on a state ρ, which is an incoherent operation by definition.

Lemma 3.2： The map $\Lambda(\rho)$ defined in Eq. (3-24) satisfies two properties, $\forall \rho$,

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Proof. For any $U_{g'}$ with $g' \in G_s$,

$$
\begin{aligned}
U_{g'}\Lambda(\rho)U_{g'}^{\dagger} &= \frac{1}{|G_s|}\sum_{g}(U_{g'}U_g)\rho(U_{g'}U_g)^{\dagger} \\
&= \frac{1}{|G_s|}\sum_{g} U_{g'g}\rho U_{g'g}^{\dagger} \\
&= \Lambda(\rho).
\end{aligned}
\tag{3-25}
$$

The last equality is due to the fact that by going through all permutations g, the joint permutation $g'g$ also traverses all the permutations in the group G_s. By Definition 3.1, we prove that $\Lambda(\rho) \in S$.

The overlap between the output state $\Lambda(\rho)$ and the maximally coherent state $|\Psi_d\rangle$ is given by,

$$
\begin{aligned}
\langle\Psi_d|\,\Lambda(\rho)\,|\Psi_d\rangle &= \langle\Psi_d|\,\frac{1}{|G_s|}\sum_{g} U_g\rho U_g^{\dagger}\,|\Psi_d\rangle \\
&= \frac{1}{|G_s|}\sum_{g}\langle\Psi_d|\,U_{g^{-1}}^{\dagger}\rho U_{g^{-1}}\,|\Psi_d\rangle \\
&= \langle\Psi_d|\,\rho\,|\Psi_d\rangle .
\end{aligned}
\tag{3-26}
$$

where in the second line we use the relation $U_g^{\dagger} = U_{g^{-1}}$ and the last line is due to the fact that $|\Psi_d\rangle \in S$ and $U_{g^{-1}}|\Psi_d\rangle = |\Psi_d\rangle$. ■

Then, we define the following function for a symmetric state ρ^s,

$$
\bar{C}_G(\rho^s) = \min_{|\psi\rangle}\{C_G(|\psi\rangle)|\Lambda(|\psi\rangle\langle\psi|) = \rho^s\}.
\tag{3-27}
$$

Since the state ρ^s in Eq. (3-23) only has one parameter p, it can be uniquely determined by its overlap with the maximally coherent state $K = \langle\Psi_d|\,\rho^s\,|\Psi_d\rangle = p\frac{d-1}{d} + \frac{1}{d}$. Thus, ρ^s linearly depends on K. According to Lemma 3.2, $\Lambda(|\psi\rangle\langle\psi|)$ is a symmetric state and the overlap does not change under the map Λ. Hence, the constraint $\Lambda(|\psi\rangle\langle\psi|) = \rho^s$ in Eq. (3-27) is equivalent to $|\langle\Psi_d|\psi\rangle|^2 = \langle\Psi_d|\,\rho^s\,|\Psi_d\rangle$. Following the derivations of the G-concurrence [Sentís et al. (2016)], we solve the minimization problem and obtain an explicit form of $\bar{C}_G(\rho^s)$,

$$
\bar{C}_G(K) = \begin{cases} 0 & 0 \le K \le \dfrac{d-1}{d} \\ d(ab^{d-1})^{(2/d)} & \dfrac{d-1}{d} \le K \le 1 \end{cases}
\tag{3-28}
$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

where

$$a = \frac{1}{\sqrt{d}}(\sqrt{K} - \sqrt{d-1}\sqrt{1-K}),$$
$$b = \frac{1}{\sqrt{d}}(\sqrt{K} + \frac{\sqrt{1-K}}{\sqrt{d-1}}).$$

Details can be found in Appendix A.3. Here, we substitute $\bar{C}_G(K)$ for $\bar{C}_G(\rho^s)$ without ambiguity. When $\frac{d-1}{d} \le K \le 1$, $\bar{C}_G(K)$ is a concave function [Sentís et al. (2016)]. We show $\bar{C}_G(K)$ in the case of $d = 4$ in Fig. 3.1. Moreover, following the results of Ref. [Vollbrecht et al. (2001)], we have the following lemma.

Lemma 3.3: The convex-roof of the G-coherence measure C_G for a symmetric state ρ^s is given by,

$$\begin{aligned} C_G(\rho^s) &= \min_{\{p_i,|\psi_i\rangle\}} \sum_i p_i C_G(|\psi_i\rangle) \\ &= \min_{\{q_j,\rho_j^s\}} \sum_j q_j \bar{C}_G(\rho_j^s), \end{aligned} \tag{3-29}$$

where $\sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho^s$, $\sum_j q_j \rho_j^s = \rho^s$, and $\rho_j^s \in S$.

Proof. Denote $Z_1 = \min_{\{p_i,|\psi_i\rangle\}} \sum_i p_i C_G(|\psi_i\rangle)$ and $Z_2 = \min_{\{q_j,\rho_j^s\}} \sum_j q_j \bar{C}_G(\rho_j^s)$. Now we prove the lemma by showing that both of them equal to,

$$Z_3 = \min_{\{p_i,|\psi_i\rangle\}} \left\{ \sum_i p_i C_G(|\psi_i\rangle) \middle| \sum_i p_i \Lambda(|\psi_i\rangle\langle\psi_i|) = \rho^s \right\}. \tag{3-30}$$

$Z_1 = Z_3$: For a decomposition, $\rho^s = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, after applying the map Λ on both sides, we have

$$\sum_i p_i \Lambda(|\psi_i\rangle\langle\psi_i|) = \Lambda(\rho^s) = \rho^s. \tag{3-31}$$

Here, we use the fact that ρ^s is a symmetric state, which is invariant under the map Λ. That is, any decomposition satisfies the constraint $\sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho^s$ as required for Z_1 also satisfies the constraint $\sum_i p_i \Lambda(|\psi_i\rangle\langle\psi_i|) = \rho^s$ as required for Z_3. Thus, we have $Z_3 \le Z_1$. On the other hand, the constraint $\sum_i p_i \Lambda(|\psi_i\rangle\langle\psi_i|) = \rho^s$ in Eq. (3-30) is also a pure-state decomposition of the state ρ^s, since every component in $\Lambda(|\psi_i\rangle\langle\psi_i|)$ is a pure state $U_g|\psi_i\rangle$ with probability $p_i/|G_s|$. Thus we also have $Z1 \le Z3$. Consequently, $Z1 = Z3$.

$Z_2 = Z_3$: In fact, the constraint in Eq. (3-30) is on $\Lambda(|\psi_i\rangle\langle\psi_i|) \in S$, thus we can solve the minimization problem of Eq. (3-30) in two steps. First, given $\Lambda(|\psi_i\rangle\langle\psi_i|) \in S$, we

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

minimize $C_G(|\psi_i\rangle)$, which turns out to be the same as the definition of $\bar{C}_G(\Lambda(|\psi_i\rangle\langle\psi_i|))$ in Eq. (3-27). Next, we optimize the decomposition of ρ^s in the symmetric state set S, which turns out to be the same as the definition of Z_2. Thus we have $Z_2 = Z_3$. ■

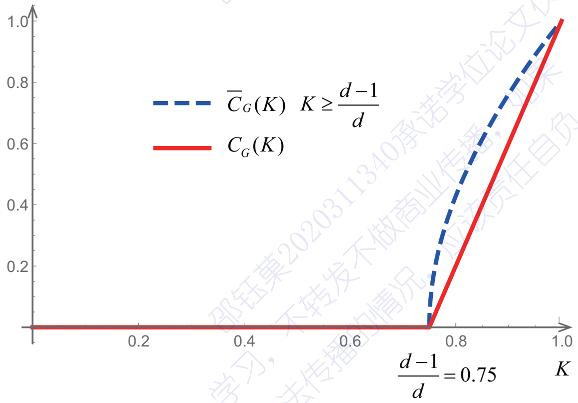


Figure 3.1 Illustration for the two functions $\bar{C}_G(K)$ and $C_G(K)$ in $d = 4$ case. When $0 \leq K \leq \frac{d-1}{d} = 0.75$, $\bar{C}_G(K) = 0$; when $\frac{d-1}{d} = 0.75 \leq K \leq 1$, $\bar{C}_G(K)$ is a concave function following the form in Eq. (3-28), represented by the dashed blue line. Thus the minimization result via Eq. (3-33), $C_G(K)$ is the linear function $1 - 4(1 - K)$, when $\frac{d-1}{d} = 0.75 \leq K \leq 1$, described by the red line.

Theorem 3.3: For a symmetric state $\rho^s \in S$ in $\mathcal{H}_d$, the G-coherence measure is given by

$$C_G(\rho^s) = \max\{1 - d(1 - K), 0\}, \tag{3-32}$$

where $K = \langle\Psi_d|\,\rho^s\,|\Psi_d\rangle$ is the overlap between ρ_s and the maximally coherent state $|\Psi_d\rangle$.

Proof. According to Lemma 3.3, the G-coherence measure for a symmetric state is given by $C_G(\rho^s) = \min_{\{q_j,\rho_j^s\}} \sum_j q_j \bar{C}_G(\rho_j^s)$ with $\sum_j q_j \rho_j^s = \rho^s$. Since the symmetric state linearly depends on the overlap K, this minimization is equivalent to,

$$C_G(K) = \min_{\{q_j,K_j\}} \left\{ \sum_j q_j \bar{C}_G(K_j) \middle| \sum_j q_j K_j = K \right\} \tag{3-33}$$

Then, according to the explicit expression of $\bar{C}_G(K)$ in Eq. (3-28): When $0 \leq K \leq \frac{d-1}{d}$, $\bar{C}_G(K) = 0$. Thus, $C_G(K) \leq \bar{C}_G(K) = 0$. When $\frac{d-1}{d} \leq K \leq 1$, fortunately, $\bar{C}_G(K)$ is a concave function. It is not hard to find that the optimization result is a straight line connecting the point $\{\frac{d-1}{d}, 0\}$ and $\{1, 1\}$ on the $\{K, C_G(K)\}$ plane. Consequently, $C_G(\rho^s)$ shows the form in Eq. (3-32). ■

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

The dependence of $\bar{C}_G(K)$ and $C_G(K)$ on K in the case of $d = 4$ are plotted in Fig. 3.1. Furthermore, we can give a lower bound of the G-coherence measure C_G for any general mixed state ρ, with the analytical solution for ρ^s in Theorem 3.3.

Corollary 3.1: For a mixed state ρ,

$$C_G(\rho) \geq \max[1 - d(1 - K), 0] \tag{3-34}$$

where $K = \langle \Psi_d | \rho | \Psi_d \rangle$.

Proof. Since Λ is an incoherent operation, we have,

$$C_G(\rho) \geq C_G(\Lambda(\rho)). \tag{3-35}$$

From Lemma 3.2, we know that the overlap $K = \langle \Psi_d | \rho | \Psi_d \rangle = \langle \Psi_d | \Lambda(\rho) | \Psi_d \rangle$ and $\Lambda(\rho) \in S$. Following Theorem 3.3, the corollary holds. ■

In fact, the tightness of the bound depends on the overlap. Thus, we can enhance the bound by pre-treating the state by a certain ICPTP χ that can increase the overlap, i.e.,

$$C_G(\rho) \geq C_G(\chi(\rho)) \geq C_G(\Lambda(\chi(\rho))) \geq \max[1 - d(1 - K'), 0], \tag{3-36}$$

where $K' = \langle \Psi_d | \chi(\rho) | \Psi_d \rangle > K = \langle \Psi_d | \rho | \Psi_d \rangle$.

3.5 Discussion

We conjecture that there are not too many polynomial coherence measures, due to the restrictive condition given by Theorem 3.2; and we suspect that all the polynomial measures would share similar structure as the G-coherence, proposed in Sec. 3.4. In addition, we should remark that the symmetry consideration in our paper is also helpful to understand and bound other coherence measures, especially the ones built by the convex-roof method.

In entanglement quantification, the polynomial invariant is an entanglement monotone if and only if its degree $\eta \leq 4$ in the multi-qubit system [Eltschka et al. (2012); Verstraete et al. (2003)]. Here, the quantification theory of coherence shows many similarities to the one for entanglement. Following the similar approaches in our paper, some results can be extended to the entanglement case. For example, one can obtain some necessary conditions where a polynomial invariant serves as an entanglement monotone, in more general multi-partite system $\mathcal{H} = {\mathcal{H}_{d_l}}^{\otimes N}$, whose local dimension $d_l > 2$ [Gour et al. (2013)].

Moreover, polynomial coherence measure (especially G-coherence) defined here may serve as an important quantifier when studying the relation and conversion between the two important quantum resources, coherence and entanglement.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Part III

Multipartite entanglement detection

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 4 Decomposition of symmetric multipartite observable

Quantum states with genuine multipartite entanglement, such as the GHZ state [Greenberger et al. (1989)], the Dicke state (including the W state) [Dicke (1954); Dür et al. (2000)], and the general graph (stabilizer) state [Gottesman (1997); Hein et al. (2004)], are essential ingredients for many quantum information processing tasks, such as multipartite quantum key distribution [Chen et al. (2007)], quantum secret sharing [Cleve et al. (1999); Hillery et al. (1999)], quantum error correction [Gottesman (1997); Nielsen et al. (2010)], measurement-based quantum computing [Raussendorf et al. (2001, 2003)], and quantum metrology [Giovannetti et al. (2004); Wineland et al. (1994)]. In practice, due to the noise caused by the uncontrolled interaction between the system and environment, the prepared state unavoidably deviates from the target one. Hence, it is necessary to quantify such deviation, which acts as calibration for the experiment system and provide the basis of further information processing.

A straightforward method to benchmark the system is quantum state tomography [Paris et al. (2004); Vogel et al. (1989)]. In reality, due to the tensor product structure of the Hilbert space, the required resources scale exponentially with the number of system parties (say, qubits) in tomography. In the last decade, the qubit number under manipulation increases significantly in various experiment systems, such as ion-trap [Monz et al. (2011)], superconducting [Song et al. (2017)], and linear optics based ones [Wang et al. (2016)]. Thus, it is impractical to directly conduct tomography for state-of-art multipartite quantum systems. Fortunately, the required resources can be dramatically reduced, if one possesses some pre-knowledge about the prepared state and takes advantage of symmetries. In this spirit, several efficient tomography methods were put forward for various types of quantum states, such as the low rank state [Flammia et al. (2012); Gross et al. (2010)], the matrix product state [Baumgratz et al. (2013); Cramer et al. (2010); Lanyon et al. (2017)], and the permutation invariant (PI) state [Moroder et al. (2012); Tóth et al. (2010)]. The insight under this simplification is that one only needs the parameters of the ansatz states there, such as the tensor network state and the PI state, whose number only increases polynomially with the number of qubits N.

In practical quantum information tasks, instead of gaining all the information about the density matrix, one only needs to guarantee that the prepared state holds sufficiently high fidelity with the target state. If focusing on fidelity evaluation instead of a full tomography, one can further reduce the measurement efforts. Sometime, one only needs to detect or witness entanglement for multipartite systems. As shown in Preliminaries 2.6.1, entanglement witness is directly related to fidelity evalution. Since quantum states with high symmetries are widely used in information processing, such as the GHZ, the W and the Dicek states. These tasks generally involve symmetric observables, which are invariant under permutations of parties. In addition, multipartite measurement is normally very challenging in practice. Instead, it is often broken down to local measurements [Bourennane et al. (2004); Terhal (2002)]. Take an N-qubit system for example, to measure the fidelity between a prepared state ρ and the GHZ state, $\mathrm{Tr}(\rho\,|GHZ\rangle\,\langle GHZ|)$, one cannot measure it directly with $|GHZ\rangle\,\langle GHZ|$. Instead, $\langle|GHZ\rangle\,\langle GHZ|\rangle$ is broken down to a set of local measurements $\{A^{\otimes N}\}$, whose number determines the complexity of fidelity evaluation. Note that from a local measurement setting (LMS) $A^{\otimes N}$, not only the expectation value $\langle A^{\otimes N}\rangle$ can be obtained, but also the full statistics. For instance, one can get the probability of any specific measurement result, say an N-bit string, from the Pauli-Z measurement, $\sigma_Z^{\otimes N}$.

In this chapter, we focus on evaluating the fidelity between an unknown prepared state with any PI states. This chapter is organized as follows. In Sec. 4.1, we constructs a set of product-state basis for the symmetric subspace. In Sec. 4.2, we propose a method which based on the previous theorem, with $(N+1)(N+2)/2$ LMSs, to evaluate the fidelity between an unknown state and any target PI state. In Sec. 4.4, we further reduce the number of LMSs in fidelity evaluation for some special PI states, GHZ, W, and Dicke. Further discussions are contained in Sec. 4.5 . The content of this chapter is from the work [Zhou et al. (2019b)].

4.1 Product-state basis for symmetric subspace

In this section, we construct a set of linearly independent vectors (states) in the product form, which can span the symmetric subspace. This construction will help us to find LMSs for decomposition of symmetric operators and fidelity evaluation of PI state in the following sections.

First, let us briefly review the symmetric subspace of an N-qudit Hilbert space $\mathcal{H}_d^{\otimes N}$, denoted by $\mathrm{Sym}_N(\mathcal{H}_d)$. Given an element π in the symmetric group S_N with N letters,

邵钰棠2020311340承诺学位论文仅作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

the corresponding permutation operator defined on $\mathcal{H}_d^{\otimes N}$ is,

$$P_d(\pi) = \sum_{i_1,\cdots,i_N \in [d]} |i_{\pi^{-1}(1)}, \cdots, i_{\pi^{-1}(N)}\rangle \langle i_1, \cdots, i_N|, \tag{4-1}$$

where $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ is the local basis for each qudit and $[d] = \{0, 1, \cdots, d-1\}$. The symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d) \subseteq \mathcal{H}_d^{\otimes N}$ contains all the pure states which are invariant under permutation,

$$\mathrm{Sym}_N(\mathcal{H}_d) = \{|\Psi\rangle \in \mathcal{H}_d^{\otimes N} : P_d(\pi)|\Psi\rangle = |\Psi\rangle, \ \forall \pi \in S_N\}. \tag{4-2}$$

In the qubit case with $d = 2$, we denote the permutation operator as $P(\pi)$ for simplicity.

It is known that the dimension of $\mathrm{Sym}_N(\mathcal{H}_d)$ is given by [Harrow (2013)]

$$D_S = \binom{N+d-1}{N} = \frac{(N+d-1)!}{N!(d-1)!}, \tag{4-3}$$

and there is a set of orthogonal (unnormalized) basis of $\mathrm{Sym}_N(\mathcal{H}_d)$,

$$\left\{ |\Psi_{\vec{i}}\rangle = \sum_{\pi} |0\rangle^{\otimes i_0} |1\rangle^{\otimes i_1} \cdots |d-1\rangle^{\otimes i_{d-1}} \middle| i_k \in \mathbb{Z}^+, \ \sum_{k=0}^{d-1} i_k = N \right\}, \tag{4-4}$$

where $\mathbb{Z}^+$ denotes the nonnegative integer set and $\vec{i} = (i_0, i_1, \cdots, i_{d-1})$ is a d-dimensional vector. Here, $\sum_\pi$ represents the summation over all permutations of N qudits that yield different expressions. We keep this notation throughout this chapter.

Meanwhile, the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$ can be spanned by the symmetric product states,

$$\mathrm{Sym}_N(\mathcal{H}_d) = \mathrm{span}\{|\phi\rangle^{\otimes N} : |\phi\rangle \in \mathcal{H}_d\}. \tag{4-5}$$

For a finite N, it is not hard to see that the symmetric product states, $|\phi\rangle^{\otimes N}$, are linearly dependent. In the following, we construct a product-state basis for the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$, by selecting $\binom{N+d-1}{N}$ linearly independent product states, as shown in Theorem 4.1.

Define a $d \times (N+1)$ matrix with complex elements $a_{k,j}$ satisfying

$$\begin{aligned} a_{0,j} &= 1, \\ a_{k,j} &\neq a_{k,j'}, \forall 1 \leq k \leq d-1, \end{aligned} \tag{4-6}$$

for all $0 \leq j \neq j' \leq N$. That is, all the elements in the 0-th row are 1; and for the other rows, the elements are different for different columns.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Theorem 4.1： The following state set $\mathcal{B}$ contains $\binom{N+d-1}{N}$ linearly independent vectors which are (unnormalized) symmetric product states, and they can span the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$,

$$\mathcal{B} = \left\{ |\Phi_{\vec{j}}\rangle = \left(a_{0,j_0}|0\rangle + a_{1,j_1}|1\rangle + \cdots + a_{d-1,j_{d-1}}|d-1\rangle\right)^{\otimes N} \middle| j_k \in \mathbb{Z}^+, \ \sum_{k=0}^{d-1} j_k = N \right\}, \tag{4-7}$$

where the coefficients a_{k,j_k} are selected from any matrix satisfying Eq. (4-6).

In the following, we call the vectors in $\mathcal{B}$ a set of basis of $\mathrm{Sym}_N(\mathcal{H}_d)$, even though they might not be orthogonal with each other. The complete proof of Theorem 4.1 is shown in Appendix B.1, which is based on induction. Here, we present the qubit case of Theorem 4.1 in Corollary 4.1 and provide a simple proof.

Corollary 4.1： The following state set $\mathcal{B}$ contains $N+1$ linearly independent vectors which are (unnormalized) symmetric product states, and they can span the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_2)$,

$$\mathcal{B} = \left\{ |\Phi_j\rangle = (|0\rangle + a_j|1\rangle)^{\otimes N} | 0 \le j \le N \right\}, \tag{4-8}$$

where a_i are complex numbers and $a_j \neq a_{j'}$ for $j \neq j'$.

Proof. The state set $\mathcal{B}$ only contains symmetric product states in $\mathrm{Sym}_N(\mathcal{H}_2)$. From Eq. (4-3), the dimension of $\mathrm{Sym}_N(\mathbb{C}^2)$ is $N+1$, which equals to the cardinality of $\mathcal{B}$. Therefore, we only need to prove that the states in $\mathcal{B}$ are linearly independent.

In this qubit case, the orthogonal basis, given in Eq. (4-4),

$$\left\{ |\Psi_i\rangle = \sum_{\pi} |0\rangle^{\otimes N-i} |1\rangle^{\otimes i}, 0 \le i \le N \right\}, \tag{4-9}$$

contains all the Dicke states. If one expands $|\Phi_j\rangle$ of Eq. (4-8) in this $\{|\Psi_i\rangle\}$ basis, the coefficients are $(1, a_j, a_j^2 \cdots, a_j^N)^T$. The matrix formed by the coefficients $(|\Phi_0\rangle, |\Phi_1\rangle, \cdots, |\Phi_N\rangle)$ is a Vandermonde matrix which is nonsingular. Consequently, $|\Phi_k\rangle$ are linearly independent and form a basis of $\mathrm{Sym}_N(\mathcal{H}_2)$. ■

4.2 Symmetric observable decomposition and fidelity evaluation

In this section, we propose a method to decompose a symmetric observable and apply it to evaluate the fidelity between a prepared state ρ and any target PI state using $(N+1)(N+2)/2$ LMSs.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

The PI state set $\mathcal{S}_{PI}$ contains all the states which are invariant under any subsystem permutation,

$$\rho^{PI} = P(\pi)\rho^{PI}P(\pi),\ \forall\pi \tag{4-10}$$

where $P(\pi)$ is permutation operation of the element π in the symmetry group S_N. It is worth to mention another related state set, symmetric state set $\mathcal{S}_S$, which contains all the pure states satisfying,

$$|\psi_s\rangle = P(\pi)\,|\psi_s\rangle,\ \forall\pi \tag{4-11}$$

and their convex combination. It is not hard to see that $\mathcal{S}_S \subset \mathcal{S}_{PI}$ ①.

Here, we only focus on the N-qubit scenario, but the method can be generalized to the N-qudit case. As shown in Eq. (4-10), a PI state is defined on the density matrix level. That is, ρ^{PI} is invariant under any permutation operation among qubits. Due to this permutation invariant property, we only need to consider the case where the local operators in LMS are the same for all qubits [Tóth et al. (2010)], that is, in the form of $A^{\otimes N}$, where A is a qubit Hermitian operator. Generally, one needs a set of LMSs $\{A_i^{\otimes N}\}$ to evaluate the fidelity. Also, the target state is normally pure. We have the following theorem.

Theorem 4.2： For any N-qubit target PI state $|\Psi^{PI}\rangle$, the fidelity between a prepared state ρ and $|\Psi^{PI}\rangle$,

$$F = \langle\Psi^{PI}|\,\rho\,|\Psi^{PI}\rangle = \mathrm{Tr}(\rho\,|\Psi^{PI}\rangle\langle\Psi^{PI}|), \tag{4-12}$$

can be evaluated with $(N+1)(N+2)/2$ LMSs.

Denote the projector formed by the PI state, $|\Psi^{PI}\rangle\langle\Psi^{PI}|$, to be Ψ^{PI}. In order to measure the fidelity F in Eq. (4-12), one should decompose the projector Ψ^{PI} into local measurements. In the following, we introduce the symmetric subspace of N-qubit Hermitian operators where Ψ^{PI} locates in. Then, by constructing a set of tensor-product basis of this symmetric subspace, we can accordingly decompose Ψ^{PI}.

---

① For example, the Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ has eigenvalue -1 of the permutation operation between the two qubits, i.e., $P(2,1)\,|\Psi^-\rangle = -\,|\Psi^-\rangle$. Hence $|\Psi^-\rangle \notin S_S$ but $|\Psi^-\rangle \in S_{PI}$. Symmetric states possess many interesting properties. For example, there is a dichotomy for entanglement depth of pure symmetric state [Ichikawa et al. (2008); Wei (2010)], i.e., they are either product states or fully entangled.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Proof. Let us first define the symmetric subspace of N-qubit Hermitian operators. Denote the N-qubit Pauli group to be G_N, whose element, called N-qubit Pauli operator, is a tensor product of single qubit Pauli operators and identity $G_1 = \{\mathbb{I}, \sigma_X, \sigma_Y, \sigma_Z\}$. An N-qubit Hermitian operator M can be written as the linear combination of the Pauli operators in G_N. Since the operators we consider here are Hermitian, their coefficients must be real. Thus, the operator space F_{G_N} is isomorphic to $F_{G_N} \simeq (\mathbb{R}^4)^{\otimes N}$, with $\mathbb{R}$ denoting real domain. Then, the corresponding symmetric subspace, $\mathrm{Sym}_N(G_1)$, is defined as,

$$\mathrm{Sym}_N(G_1) = \left\{M \in F_{G_N} : P(\pi)MP(\pi) = M, \forall \pi \in S_N\right\}. \tag{4-13}$$

By the definition in Eq. (4-10), any PI state, $\rho^{PI} \in \mathrm{Sym}_N(G_1)$.

Since $\mathrm{Sym}_N(G_1)$ is isomorphic to $\mathrm{Sym}_N(\mathbb{R}^4)$, the dimension of $\mathrm{Sym}_N(G_1)$ is $\binom{N+3}{3}$ according to Eq. (4-3). Meanwhile, the results shown in Sec. 4.1 can be directly applied to the operator space here.

- Similar to the orthogonal basis shown in Eq. (4-4), the following Hermitian operators form an orthogonal basis (in the sense of Hilbert-Schmidt inner product) of $\mathrm{Sym}_N(G_1)$,

  $$M_{i,j,k} = \sum_{\pi} \mathbb{I}^{\otimes i} \otimes \sigma_X^{\otimes j} \otimes \sigma_Y^{\otimes k} \otimes \sigma_Z^{\otimes(N-i-j-k)}, \tag{4-14}$$

  where $\sigma_X^{\otimes j}$ denotes that there are totally j qubits with σ_X on them, similar for $\mathbb{I}^{\otimes i}, \sigma_Y^{\otimes k}, \sigma_Z^{\otimes(N-i-j-k)}$.
- Similar to Eq. (4-5), product operators can also span the symmetric subspace,

  $$\mathrm{Sym}_N(G_1) = \mathrm{span}\{A^{\otimes N} : A = a\mathbb{I} + b\sigma_X + c\sigma_Y + d\sigma_Z\}, \tag{4-15}$$

  where $a, b, c, d \in \mathbb{R}$.
- Similar to the proof of Theorem 4.1, with previous two steps, we only need to select $\binom{N+3}{3}$ linearly independent operators $\{A^{\otimes N}\}$ to act as the product-form basis of $\mathrm{Sym}_N(G_1)$. According to Theorem 4.1, we can construct a set of basis for $\mathrm{Sym}_N(G_1)$ with product operators, where the local basis are $\{\mathbb{I}, \sigma_X, \sigma_Y, \sigma_Z\}$. To be specific,

  $$\mathcal{B}_o = \left\{(a_{1,j_1}\mathbb{I} + a_{2,j_2}\sigma_X + a_{3,j_3}\sigma_Y + a_{0,j_0}\sigma_Z)^{\otimes N} \middle| \sum_{k=0}^{3} j_k = N\right\}, \tag{4-16}$$

  where the subscript "o" denotes an operator set, and the coefficients a_{k,j_k} with $0 \leq k \leq 3$ and $0 \leq j_k \leq N$ are real numbers satisfying Eq. (4-6).

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

After step 3, we further reduce the number $\binom{N+3}{3} \Rightarrow \binom{N+2}{2}$ due to the fact that some of the product operators can be measured by the same LMS. Since $a_{0,j_0} = 1$ for any j_0, the operator set in Eq. (4-16) can be also written as,

$$\mathcal{B}_o = \left\{ (a_i\mathbb{I} + b_j\sigma_X + c_k\sigma_Y + \sigma_Z)^{\otimes N} \middle| 0 \le i, j, k \le N,\ i + j + k \le N \right\}, \tag{4-17}$$

where for the simplicity of notation, let $a_i = a_{1,i}$, $b_j = a_{2,j}$ and $c_k = a_{3,k}$.

On account of Proposition 4.1 shown below, product operators in $\mathcal{B}_o$ with different a_i but same b_j and c_k can be obtained via the same LMS $(b_j\sigma_X + c_k\sigma_Y + \sigma_Z)^{\otimes N}$. Therefore, the total number of LMSs required is the number of different parameter set (b_j, c_k), which equals to the number of solutions for $j + k \le N$, i.e., $\binom{N+2}{2} = (N + 1)(N + 2)/2$.

Consequently, one can utilize $(N+1)(N+2)/2$ LMSs to obtain the expectation values of all the basis operators in $\mathcal{B}_o$ of symmetric subspace $\mathrm{Sym}_N(G_1)$. Since any PI state $\Psi^{PI} \in \mathrm{Sym}_N(G_1)$, we can decompose any Ψ^{PI} in this basis and finally obtain the fidelity in Eq. (4-12). ■

Proposition 4.1: The expectation value of the product operator $(a\mathbb{I}+b\sigma_X+c\sigma_Y+d\sigma_Z)^{\otimes N}$ can be obtained via the LMS $(a\mathbb{I} + b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N} \Rightarrow (b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N}$.

Proof.

$$\begin{aligned} &(a\mathbb{I} + b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N} \\ =&\sum_{i=0}^{N} a^i \sum_{\pi} \mathbb{I}^{\otimes i} \otimes (b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N-i}. \end{aligned} \tag{4-18}$$

Note that each term in Eq. (4-18) can be directly obtained from the LMS $(b\sigma_X + c\sigma_Y + d\sigma_Z)^{\otimes N}$. ■

Some remarks and discussions of Theorem 4.2 are listed as follows.

- We show how to efficiently decompose a general PI state in a set of product-form basis in Appendix B.2, which is useful in practical implementation. And we remark that this decomposition is suitable for general symmetric operators, which may be useful for other related problems. In fact, on account of Theorem 4.1, there are possibility to choose other set of product-form basis. Thus, we also discuss how to choose basis which is more robust to noise there.
- Theorem 4.2 can be directly extended to the qudit case, by considering the generalized local Pauli basis for qudit.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

- Our method can evaluate the fidelity between an unknown prepared state with any PI state with the same $\binom{N+2}{2}$ LMSs, by only post-processing the measurement results.
- Finally, from the above proof of Theorem 4.2, it shows that the expectation values of all the basis operators in $\mathcal{B}_o$ can be measured with $\binom{N+2}{2}$ LMSs. As a result, not only the fidelity in Eq. (4-12) can be evaluated, but also the information of general PI state ρ^{PI}, which is related to permutation invariant tomography [Tóth et al. (2010)]. However, our basis constructed in Eq. (4-16) for $\mathrm{Sym}_N(G_1)$ is more explicit and different compared with theirs.

We will show in the following that our decomposition method can further help to reduce the number of LMSs for some special PI states. To be specific, it is known that for the GHZ state and the W state, one only needs $N+1$ and $2N-1$ LMSs to decompose them respectively [Gühne et al. (2007)], compared with $\binom{N+2}{2}$ for general PI state. In the following sections, we define a quantity called *measurement complexity* which quantifies the minimal number of LMSs to decompose a state, and systemically study the measurement complexities for the GHZ state, the W state and the Dicke state.

4.3 Complexity upper bound of Dicke State

In the previous section, we have already obtained a method to decompose any PI state, and in the following we focus on reducing the number of LMSs for some specific PI states. Certain PI states are typical for quantum information processing and have been extensively studied, including the GHZ state, the W state and the Dicke state. In this section and the next section, the number of LMSs required for these states are discussed.

First, let us give the definition of *measurement complexity* of PI states, strictly speaking, symmetric-measurement complexity, since the LMSs utilized here are in the symmetric form. For simplicity, we use the term measurement complexity without confusion.

Definition 4.1： For an N-qubit PI state ρ, measurement complexity $C_S(\rho)$ is the minimal number of LMSs to decompose it,

$$\begin{aligned} &C_S(\rho) = \min n_A, \\ &s.t., \rho = \sum_{i=1}^{n_A} \sum_{j=1}^{N} \alpha_{ij} \sum_{\pi} \mathbb{I}^{\otimes j} A_i^{\otimes N-j}, \end{aligned} \tag{4-19}$$

where $A_i = b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z$ and $\alpha_{ij}, b_i, c_i, d_i \in \mathbb{R}$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Here we allow $\sum_\pi \mathbb{I}^{\otimes j} A_i^{\otimes N-j}$ to appear in the summation in Eq. (4-19), since its expectation value can be inferred from the LMS $A_i^{\otimes N}$. Note that we do not need to introduce $\mathbb{I}$ into A_i, like $(a_i\mathbb{I} + b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z)^{\otimes N}$, since any operator $\sum_\pi \mathbb{I}^{\otimes j}(a_i\mathbb{I} + A_i)^{\otimes N-j}$ can be written as a combination of $\sum_\pi \mathbb{I}^{\otimes j} A_i^{\otimes N-j}$.

A summary of the results are listed in Table 4.1. It is worth mentioning that the measurement complexities for these states all grows linearly with the number of qubits, $\Theta(N)$, whereas the measurement complexity of a general PI state grows quadratically with N, as stated in Theorem 4.2.

Table 4.1 Measurement complexity of some typical PI states. For these states, the measurement complexity is linear, $\Theta(N)$. Here $*$ denotes previous results given in [Gühne et al. (2007)]

State	Upper bound	Lower bound
W	$2N - 1$ [*]	$N - 1$
Dicke	$m(2m+3)N + 1$	$N - 2m + 1$
GHZ	$N + 1$ [*]	$\lceil \frac{N+1}{2} \rceil$

In this section, we focus on finding upper bound of measurement complexity. To find a upper bound, one needs to give a specific decomposition of the state. Note that one can use $N + 1$ and $2N - 1$ LMSs to decompose the GHZ and the W state respectively, which are listed as the upper bounds shown in Table 4.1.

In the following, we give an explicit decomposition of Dicke state $|D_{N,m}\rangle$ of N qubits with m excitations [Dicke (1954)],

$$|D_{N,m}\rangle = \frac{1}{\sqrt{\binom{N}{m}}} \sum_\pi |0\rangle^{\otimes N-m} |1\rangle^{\otimes m}. \tag{4-20}$$

using $m(2m + 3)N + 1$ LMSs. Note that as $m = 1$, it is W state [Dür et al. (2000)],

$$|W_N\rangle = \frac{1}{\sqrt{N}} \left(|10\cdots01\rangle + |01\cdots0\rangle + \cdots + |00\cdots1\rangle\right). \tag{4-21}$$

To do so, we characterize a subspace of the symmetric subspace that contains the state, then construct a set of basis for that subspace with some LMSs. Consequently, one obtains an upper bound of the measurement complexity of $|D_{N,m}\rangle$, which is summarized in the following theorem.

Theorem 4.3： The measurement complexity of the Dicke state $|D_{N,m}\rangle$ is upper bounded

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

by

$$C_S(D_{N,m}) \leq m(2m+3)N+1. \tag{4-22}$$

Proof. The density matrix of $|D_{N,m}\rangle$ can be explicitly written down as,

$$\begin{aligned} D_{N,m} &= \frac{1}{\binom{N}{m}} \sum_{t=0}^{m} \Theta_t, \\ \Theta_t &\equiv \sum_{\pi} (|1\rangle\langle 1|)^{\otimes m-t} \otimes (|0\rangle\langle 1|)^{\otimes t} \otimes (|1\rangle\langle 0|)^{\otimes t} \otimes (|0\rangle\langle 0|)^{\otimes N-m-t}, \end{aligned} \tag{4-23}$$

where we denote each term in the summation as Θ_t, and Θ_0 is the diagonal term. It is clear that Θ_0 can be obtained by the Z-basis measurement $\sigma_Z^{\otimes N}$. Thus in the following we focus on Θ_t with $1 \leq t \leq m$, which are the off-diagonal terms.

With the relations $|1\rangle\langle 1| = (\mathbb{I}-\sigma_Z)/2$, $|0\rangle\langle 0| = (\mathbb{I}+\sigma_Z)/2$, $|0\rangle\langle 1| = (\sigma_X + i\sigma_Y)/2$ and $|1\rangle\langle 0| = (\sigma_X - i\sigma_Y)/2$, Θ_t can be written into the following form,

$$\Theta_t = \sum_{\pi} (\frac{\mathbb{I}-\sigma_Z}{2})^{\otimes m-t} \otimes \chi_t \otimes (\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes N-m-t}, \tag{4-24}$$

where χ_t is given by

$$\begin{aligned} \chi_t &= \sum_{\pi} (|0\rangle\langle 1|)^{\otimes t} \otimes (|1\rangle\langle 0|)^{\otimes t} \\ &= \sum_{\pi} (\frac{\sigma_X + i\sigma_Y}{2})^{\otimes t} \otimes (\frac{\sigma_X - i\sigma_Y}{2})^{\otimes t} \\ &= \sum_{l=0}^{2t} \sum_{\pi} \alpha_{t,l} \sigma_X^{\otimes l} \sigma_Y^{\otimes(2t-l)}, \end{aligned} \tag{4-25}$$

where $\alpha_{t,l}$ are the corresponding coefficients, whose values do not affect the following analysis.

Based on the single qubit operators appearing in Θ_t, we utilize a new orthogonal one-qubit basis $G_1' = \{\frac{\mathbb{I}-\sigma_Z}{2}, \sigma_X, \sigma_Y, \frac{\mathbb{I}+\sigma_Z}{2}\}$ to act as the local basis, and clearly one has $\mathrm{Sym}_N(G_1') = \mathrm{Sym}_N(G_1)$. Similar as Eq. (4-14), the corresponding new orthogonal basis of the symmetric subspace is

$$M'_{i,j,k} = \sum_{\pi} (\frac{\mathbb{I}-\sigma_Z}{2})^{\otimes i} \otimes \sigma_X^{\otimes j} \otimes \sigma_Y^{\otimes k} \otimes (\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes(N-i-j-k)}. \tag{4-26}$$

As a result, Θ_t lies in the subspace

$$V_t = \mathrm{span}\{M'_{i,j,k} | i+j+k = m+t\}. \tag{4-27}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

In fact, V_t is isomorphic to $\mathrm{Sym}_{(m+t)}(\mathbb{R}^3)$, in the sense that

$$\sum_{\pi}\left(a(\frac{\mathbb{I}-\sigma_Z}{2})+b\sigma_X+c\sigma_Y\right)^{\otimes(m+t)}\otimes(\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes(N-m-t)}=\sum_{i+j+k=m+t}a^ib^jc^kM'_{i,j,k}. \quad (4\text{-}28)$$

Thus, according to Theorem 4.1, for any two real number sets $\{b_0, b_1\cdots, b_{m+t}\}$ and $\{c_0, c_1, \cdots, c_{m+t}\}$,

$$\left\{A^{(t)}_{j,k}=\sum_{\pi}(\frac{\mathbb{I}-\sigma_Z}{2}+b_j\sigma_X+c_k\sigma_Y)^{\otimes(m+t)}\otimes(\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes(N-m-t)}\middle| j+k\le m+t\right\} \quad (4\text{-}29)$$

is a set of basis of V_t.

Consequently, by constructing $A^{(t)}_{j,k}$ for all j, k, each Θ_t in the V_t subspace can be decomposed. Then after decomposing all Θ_t, the decomposition of $D_{N,m}$ can be obtained. In the following, we show how to construct $A^{(t)}_{j,k}$ with LMSs.

Since $1 \le t \le m$, the parameter b_j, c_k which determine the basis operator $A^{(t)}_{j,k}$ of each subspace V_t in Eq. (4-29) are extended to $\{b_0, b_1\cdots, b_{2m}\}$ and $\{c_0, c_1, \cdots, c_{2m}\}$. That is, we construct $A^{(t)}_{j,k}$ of different t by using the same sets of b_j and c_k, which can help us save the number of LMSs.

Deonote $T_{j,k}=\frac{\mathbb{I}-\sigma_Z}{2}+b_j\sigma_X+c_k\sigma_Y$ for simplicity, and the basis operator $A^{(t)}_{j,k}$ of V_t space in Eq. (4-29) shows,

$$A^{(t)}_{j,k}=\sum_{\pi}T^{\otimes(m+t)}_{j,k}(\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes(N-m-t)}. \quad (4\text{-}30)$$

$A^{(t)}_{j,k}$ is a symmetric operator, generated by the single-qubit operators $T_{j,k}$ and $(\mathbb{I}+\sigma_Z)/2$. Thus, according to Theorem 4.1, for specific j, k, one can construct $A^{(t)}_{j,k}$ by the following $N+1$ product basis for any t,

$$\left\{\left(\tan\theta_k T_{i,j}+\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes N}\right\}, \quad (4\text{-}31)$$

where $0 \le k \le N$, $0 \le \theta_k < \pi$, and $\theta_k \ne \theta_{k'}$ with $k \ne k'$. For example, $\theta_k = \frac{k\pi}{N+1}$. As a result, after constructing $A^{(t)}_{j,k}$, we can decompose Θ_t, as well as $D_{N,m}$.

Finally, let us count the total number of LMSs. For each $T_{j,k}$, we need $N+1$ LMSs. And there are $\binom{2m+2}{2}=(m+1)(2m+1)$ of different $T_{j,k}$. Thus totally $(m+1)(2m+1)(N+1)$ LMSs. In fact, one can reduce the number of the LMSs with more careful analysis. There is one setting $(\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes N}$ with $\theta_k=0$ shared by all $T_{j,k}$, which is equavilent to the $\sigma_Z^{\otimes N}$ setting. In addition, if we choose $b_0=c_0=0$, $T_{0,0}$ only needs the same setting $\sigma_Z^{\otimes N}$. As a

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

result, the final number of LMSs is,

$$((m+1)(2m+1)-1)N+1 = m(2m+3)N+1. \tag{4-32}$$

■

Some remarks are as follows. First, our construction is general and suitable for any Dicke state $|D_{N,m}\rangle$. We expect that the number of LMSs could be reduced further with more elaborate analysis. Specifically, one may find a smaller subspace compared with V_t that contains Θ_t. Second, as $m = 1$, our upper bound is $5N + 1$, which is larger than the previous result $2N - 1$ for the W state. Thus, it is also expected that for certain Dicke state, such as $|D_{N,2}\rangle$, the number of LMSs can also be reduced. And we leave them for further work.

4.4 Lower bound on Measurement Complexity

In this section, we bound measurement complexity of the GHZ state, the W state and the Dicke state from below. The corresponding results are listed in the second column of Table 4.1.

Before formally discuss the lower bound of measurement complexity for specific state, here we explain the high level idea of how to bound it from below. On the one hand, we find a subspace on which the projection of the state has certain form; on the other hand, on account of the product form of LMS, we show that the projection result can only be reconstructed with enough number of LMSs.

First, let us study the measurement complexity of the N-qubit GHZ state [Greenberger et al. (1989)],

$$|GHZ_N\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \tag{4-33}$$

In Ref. [Gühne et al. (2007)], the authors decompose $|GHZ_N\rangle$ into $N + 1$ LMSs. In the following theorem, we provide a lower bound for the measurement complexity of GHZ state which also grows linearly. It means that one should make use of $\Theta(N)$ LMSs to evaluate the fidelity with GHZ state.

Theorem 4.4: The measurement complexity of the N-qubit GHZ state $|GHZ_N\rangle$ is lower bounded by

$$C_S(|GHZ_N\rangle) \geq \lceil \frac{N+1}{2} \rceil. \tag{4-34}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Proof. The density matrix of GHZ state can be written in the following form [Gühne et al. (2007)],

$$GHZ_N = \frac{1}{2}\left(\frac{\mathbb{I}+\sigma_Z}{2}\right)^{\otimes N} + \frac{1}{2}\left(\frac{\mathbb{I}-\sigma_Z}{2}\right)^{\otimes N} + \frac{1}{2^N}\sum_{\text{even } k=0}^{N}(-1)^{k/2}\sum_{\pi}\sigma_Y^{\otimes k}\sigma_X^{\otimes(N-k)}, \quad (4\text{-}35)$$

where the first two terms account for the diagonal elements and the last one for the off-diagonal elements.

Denote the set of LMSs used to decompose GHZ state as

$$\mathcal{A} = \{A_i^{\otimes N} = (b_i\sigma_X + c_i\sigma_Y + d_i\sigma_Z)^{\otimes N} | i = 1, 2, \cdots, n_A\}, \quad (4\text{-}36)$$

and the final operator constructed from $\mathcal{A}$ shown in Eq. (4-19) as O,

$$O = \sum_{i=1}^{n_A}\sum_{j=1}^{N}\alpha_{ij}\sum_{\pi}\mathbb{I}^{\otimes j}A_i^{\otimes N-j}. \quad (4\text{-}37)$$

It is assumed that $O = GHZ_N$.

Then, consider the projection onto the following subspace,

$$\text{span}\{M_{0,N-k,k} | 0 \leq k \leq N, \text{even } k\}, \quad (4\text{-}38)$$

where $M_{i,j,k}$ is the orthogonal basis defined in (4-14).

For GHZ state, we write the projection results on all the basis operators $M_{0,N-k,k}$ in Eq. (4-38) in the vector form as

$$v_{GHZ} = \frac{1}{2^N}(1, -1, 1, \cdots, (-1)^{\lfloor N/2 \rfloor}). \quad (4\text{-}39)$$

For O, it is not hard to see that only the following terms in the summation of Eq. (4-37) have non-zero projection on this subspace,

$$\sum_{i=1}^{n_A}\alpha_{i0}A_i^{\otimes N}, \quad (4\text{-}40)$$

and the projection result shows

$$v_O = \sum_{i=1}^{n_A}\alpha_{i0}(b_i^N, b_i^{N-2}c_i^2, \cdots, b_i^{N-2\lfloor N/2 \rfloor}c_i^{2\lfloor N/2 \rfloor}). \quad (4\text{-}41)$$

Since $O = GHZ_N$, the projection results should also be equal, i.e., $v_{GHZ} = v_O$. In the following, we show that if $v_G = v_O$, the number of LMSs $n_A \geq \lceil \frac{N+1}{2} \rceil$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Here we focus on the case where $b_i \neq 0$ and $c_i \neq 0$, and leave the proof of the general case in Appendix B.3. Define $\beta_i = (c_i/b_i)^2$ and it is clear that $\beta_i > 0$, then v_O shows

$$v_O = \sum_{i=1}^{n_A} \alpha_i (1, \beta_i \cdots, \beta_i^{\lfloor N/2 \rfloor}), \tag{4-42}$$

where $\alpha_i = \alpha_{i0} b_i^N$.

We construct the following function

$$g(x) = \sum_{i=1}^{n_A} \alpha_i \beta_i^x, \tag{4-43}$$

which is the linear combination of n_A exponential functions. Since $v_O = v_G$, we have

$$g(0) = \frac{1}{2^N},\ g(1) = -\frac{1}{2^N},\ \ g(2) = \frac{1}{2^N},\ \cdots,\ g(\lfloor N/2 \rfloor) = (-1)^{\lfloor N/2 \rfloor} \frac{1}{2^N}. \tag{4-44}$$

and it is clear $g(x)$ changes its sign with respect to adjacent points. On account of the continuity of $g(x)$, there are at least one root of $g(x) = 0$ in each of the intervals $(0, 1)$, $(1, 2)$, $\cdots$, $(\lfloor N/2 \rfloor - 1, \lfloor N/2 \rfloor)$. Totally, there are at least $\lfloor N/2 \rfloor$ roots.

On the other hand, it is known that $g(x)$ at most has $n_A - 1$ roots [Tossavainen (2006)], as shown in Lemma 4.1 below. Consequently, one has $n_A - 1 \geq \lfloor N/2 \rfloor$, i.e. $n_A \geq \lceil \frac{N+1}{2} \rceil$.
■

Lemma 4.1: [Tossavainen (2006)] For real numbers $\{\alpha_i\}_1^n$ and $\{\beta_i\}_1^n$ with $\alpha_i \neq 0, \beta_i > 0$, and $\beta_i \neq \beta_j$ for $i \neq j$, the function

$$g(x) = \sum_{i=1}^{n} \alpha_i \beta_i^x \tag{4-45}$$

has at most $n - 1$ roots.

The proof of Lemma 4.1 can be found in [Tossavainen (2006)].

Then, we give the measurement complexity lower bounds of Dicke state as well as W state.

Theorem 4.5: The measurement complexity of the Dicke state $|D_{N,m}\rangle$ is lower bounded by

$$C_S(|D_{N,m}\rangle) \geq N - 2m + 1. \tag{4-46}$$

As a result of Theorem 4.5, we also have the lower bound for W state.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Corollary 4.2： The measurement complexity of the N-qubit W state $|W_N\rangle$ is lower bounded by

$$C_S(|W_N\rangle) \geq N - 1. \tag{4-47}$$

There is a known decomposition of $|W_N\rangle$ using $2N-1$ LMSs [Gühne et al. (2007)], which is consistent with our lower bound. It means that one should make use of $\Theta(N)$ LMSs to evaluate the fidelity with the W state.

The proof of Theorem 4.5 is similar with the one of Theorem 4.4 for GHZ state. We find a specific subspace where the state $D_{N,m}$ has zero projection. On the other hand, we show that there should be at least $N-2m+1$ LMSs in the decomposition of $D_{N,m}$, in order to make the projection to be also zero. The detailed proof is left in Appendix B.4.

4.5 Discussion

In this chapter, by introducing a set of product basis for the symmetric subspace, we show that a set of $(N+1)(N+2)/2$ LMSs can be used to decompose a symmetric observable and apply it to evaluate the fidelity between the prepared state with any PI state. For some typical PI states, such as the GHZ state, the W state, and the Dicke state with constant number excitations, we can further reduce the measurement complexity down to the linear regime.

There are a few prospective questions can be explored in the future. First, it is interesting to show whether the measurement complexity of Dicke states with $\Theta(N)$ excitations, such as $|D_{N,\frac{N}{2}}\rangle$, is still $\Theta(N)$. Second, besides the GHZ state, the W state, and the Dicke state, one might also reduce the measurement complexity for the tasks related to other specific PI states using similar decomposition techniques. Third, our decomposition technique focuses on the party permutation symmetry but it might also be extended to other types of symmetry, such as permutation symmetry of eigenstates in high dimensional system. In addition, the observable decomposition method can be directly applied to entanglement detection, by constructing the corresponding fidelity-based entanglement witnesses [Gühne et al. (2009); Terhal (2002)], where further reduction of LMSs is expected [Gühne et al. (2007); Zhao et al. (2019)]. In fact, we find that this kind of construction can yield much better witness considering entanglement detection under coherent noise [Zhou et al. (2019a)].

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 5 Efficient detection of multipartite entanglement structure

Entanglement is an essential resource for many quantum information tasks [Horodecki et al. (2009)], such as quantum teleportation [Bennett et al. (1993)], quantum cryptography [Bennett et al. (1984); Ekert (1991)], non-locality test [Brunner et al. (2014)], quantum computing [Nielsen et al. (2010)], quantum simulation [Lloyd (1996)] and quantum metrology [Giovannetti et al. (2006); Wineland et al. (1992)]. Tremendous efforts have been devoted to the realization of multipartite entanglement in various systems [Britton et al. (2012); Chen et al. (2017); Lücke et al. (2014); Luo et al. (2017); Monz et al. (2011); Schmied et al. (2016); Song et al. (2017); Takei et al. (2016); Wang et al. (2016); Zhong et al. (2018)], which provide the foundation for small- and medium-scale quantum information processing in near future and will eventually pave the way to universal quantum computing. In order to build up a quantum computing device, it is crucial to first witness multipartite entanglement. So far, genuine multipartite entanglement has been demonstrated and witnessed in experiment with more than 10 qubits in different realizations, such as 14-ion-trap-qubit [Monz et al. (2011)], 10-superconducting-qubit [Song et al. (2017)], 12-photon-qubit systems [Zhong et al. (2018)].

When the system size becomes large, see for instance, Google's a 72-qubit chip ① and IonQ's a 79-qubit system ②, it is an experimental challenge to create genuine multipartite entanglement. Nonetheless, even without global genuine entanglement as the target state possesses, the experimental prepared state might still have fewer-body entanglement within a subsystem and/or among distinct subsystems [Acín et al. (2001); Dür et al. (2000); Guhne et al. (2005)]. The study of lower-order entanglement, which can be characterized by the detailed entanglement structures [Huber et al. (2013); Lu et al. (2018); Shahandeh et al. (2014)], is important for quantum hardware development, because it might reveal the information on unwanted couplings to the environment and acts as an benchmark of the underlying system. Moreover, the certified lower-order entanglement among several subsystems could be still useful for some quantum information tasks.

Considering an N-partite quantum system and its partition into m subsystems ($m \leq N$), the entanglement structure indicates how the subsystems are entangled with each other.

---

① https://www.sciencenews.org/article/google-moves-toward-quantum-supremacy-72-qubit-computer

② https://physicsworld.com/a/ion-based-commercial-quantum-computer-is-a-first/

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Each subsystem corresponds to a subset of the whole quantum system. For instance, we can choose each subsystem to be each party (i.e., $m = N$), and then the entanglement structure indicates the entanglement between the N parties. In some specific systems, such as distributed quantum computing [Cirac et al. (1999)], quantum networks [Kimble (2008)] or atoms in a lattice, the geometric configuration can naturally determine the system partition (see Fig. 5.1 for an illustration). In other cases, one might not need to specify the partition in the beginning. By going through all possible partitions, one can investigate higher level entanglement structures, such as entanglement intactness (non-separability) [Guhne et al. (2005); Lu et al. (2018)], which quantifies how many pieces in the N-partite state are separated.

In this chapter, we propose a systematic method to witness the entanglement structure based on graph states. Our detection method for entanglement structures of generic graph states is presented in Theorem 5.1 and 5.2. The entanglement structure detection method only involves k local measurements. Here, k is the chromatic number of the corresponding graph, which is typically a small constant and independent of the number of qubits. In order to obtain the fidelity bounds, one needs to solve optimization problems, which grow exponentially with the system size. In general, the optimization is a challenge when the system size is large. For several common graph states, 1-D and 2-D cluster states and the GHZ state, we construct witnesses with only $k = 2$ local measurement settings, and derive analytical solutions to the optimization problem. These results are shown in Corollaries 5.1 to 5.4. All the proofs of corollaries are presented in Appendix C. The content of this chapter is from the work [Zhou et al. (2019c)].

5.1 Definition of multipartite entanglement structure

Considering an N-qubit quantum system in a Hilbert space $\mathcal{H} = \mathcal{H}_2^{\otimes N}$, one can partition the whole system into m nonempty disjoint subsystems A_i, i.e., $\{N\} \equiv \{1, 2, \ldots, N\} = \bigcup_{i=1}^m A_i$ with $\mathcal{H} = \bigotimes_{i=1}^m \mathcal{H}_{A_i}$. Denote this partition to be $\mathcal{P}_m = \{A_i\}$ and omit the index m when it is clear from the context. Similar to definitions of regular separable states, here, we define fully- and bi-separable states with respect to a specific partition $\mathcal{P}_m$ as follows.

Definition 5.1: An N-qubit pure state, $|\Psi_f\rangle \in \mathcal{H}$, is $\mathcal{P}$-fully separable, iff it can be written as,

$$|\Psi_f\rangle = \bigotimes_{i=1}^{m} |\Phi_{A_i}\rangle . \tag{5-1}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

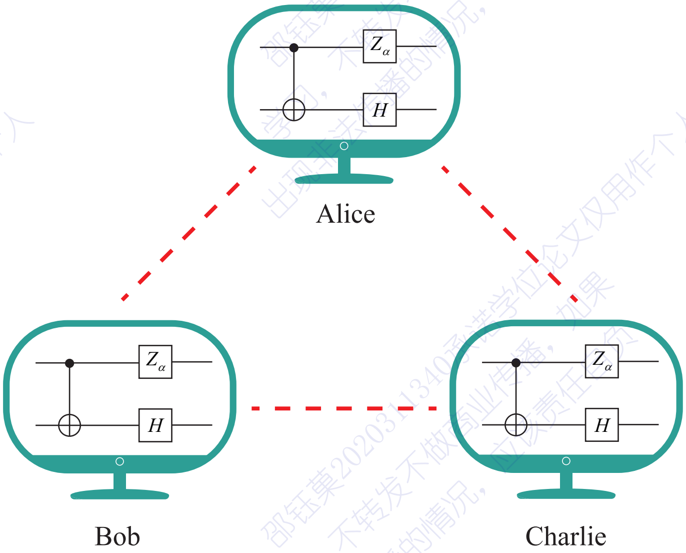


Figure 5.1 A distributed quantum computing scenario. Three remote (small) quantum processors, owned by Alice, Bob and Charlie, are connected by quantum links. Each of them possesses a few of qubits and performs quantum operations. In this case, the partition of the whole quantum system is determined by the locations of these processors. In order to perform global quantum operations involving multiple processors, entanglement among the processors are generally required. Thus, it is essential to benchmark the entanglement structure on this network.

An N-qubit mixed state ρ_f is $\mathcal{P}$-fully separable, iff it can be decomposed into a convex mixture of $\mathcal{P}$-fully separable pure states,

$$\rho_f = \sum_i p_i \left|\Psi_f^i\right\rangle \left\langle\Psi_f^i\right|, \tag{5-2}$$

with $p_i \geq 0, \forall i$ and $\sum_i p_i = 1$.

Denote the set of $\mathcal{P}$-fully separable states to be $S_f^{\mathcal{P}}$. Thus, if one can confirm that a state $\rho \notin S_f^{\mathcal{P}}$, the state ρ should possess entanglement between the subsystems $\{A_i\}$. Such kind of entanglement could be weak though, since it only requires at least two subsystems to be entangled. For instance, the state $|\Psi\rangle = |\Psi_{A_1A_2}\rangle \otimes \prod_{i=3}^m |\Psi_{A_i}\rangle$ is called entangled nevertheless only with entanglement between A_1 and A_2. It is interesting to study the states where all the subsystems are genuinely entangled with each other. Below, we define this genuine entangled state via $\mathcal{P}$-bi-separable states.

Definition 5.2： An N-qubit pure state, $|\Psi_s\rangle \in \mathcal{H}$, is $\mathcal{P}$-bi-separable, iff there exists a subsystem bipartition $\{A, \bar{A}\}$, where $A = \bigcup_i A_i$, $\bar{A} = \{N\}/A \neq \emptyset$, the state can be written as,

$$|\Psi_b\rangle = |\Phi_A\rangle \otimes |\Phi_{\bar{A}}\rangle . \tag{5-3}$$

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

An N-qubit mixed state ρ_b is $\mathcal{P}$-bi-separable, iff it can be decomposed into a convex mixture of $\mathcal{P}$-bi-separable pure states,

$$\rho_b = \sum_i p_i \left|\Psi_b^i\right\rangle \left\langle\Psi_b^i\right|, \tag{5-4}$$

with $\sum_i p_i = 1$ and $p_i \geq 0, \forall i$, and each state $|\Psi_b^i\rangle$ can have different bipartitions.

Denote the set of bi-separable states to be $S_b^{\mathcal{P}}$. It is not hard to see that $S_f^{\mathcal{P}} \subseteq S_b^{\mathcal{P}}$.

Definition 5.3: A state ρ is $\mathcal{P}$-genuine entangled iff $\rho \notin S_b^{\mathcal{P}}$.

The three entanglement-structure definitions of $\mathcal{P}$-fully separable, $\mathcal{P}$-bi-separable, and $\mathcal{P}$-genuinely entangled states can be viewed as generalized versions of regular fully separable, bi-separable, and genuinely entangled states, respectively. In fact, when $m = N$, these pairs of definitions are the same.

By definitions, one can see that if a state is $\mathcal{P}_m$-fully separable, it must be m-separable defined in Eq. (5-2). Of course, an m-separable state might not be $\mathcal{P}_m$-fully separable, for example, if the partition is not properly chosen. Interestingly, there exist some m-separable states that are not $\mathcal{P}_m$-fully separable for any m-partition. In experiment, it is important to identify the partition under which the system is fully separated. With the partition information, one can quickly identify the links where entanglement is broken. Moreover, for some systems, such as distributed quantum computing, multiple quantum processor, and quantum network, natural partition exists due to the system geometric configuration. Therefore, it is practically interesting to study entanglement structure under partitions.

5.2 Graph state and stabilizer formalism

Graph state [Briegel et al. (2001); Hein et al. (2006)] is one of the most important classes of multipartite states for quantum information processing, such as measurement-based quantum computing [Raussendorf et al. (2001, 2003)], quantum routing and quantum networks [Perseguers et al. (2013)], quantum error correction [Schlingemann et al. (2001)], and Bell nonlocality test [Gühne et al. (2005); Scarani et al. (2005)]. It is also related to the symmetry-protected topological order in condensed matter physics Zeng et al. (2015). Typical graph states include cluster states, GHZ state, and the states involved in the encoding process of the 5-qubit Steane code and the concatenated [7, 1, 3]-CSS-code [Hein et al. (2006)].

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Let us recap the basics of graph states and the stabilizer formalism. In a graph, denoted by $G = (V, E)$, there are a vertex set $V = \{N\}$ and a edge set $E \subset [V]^2$. Two vertexes i, j are called neighbors if there is an edge (i, j) connecting them. The set of neighbors of the vertex i is denoted as N_i. A graph state is defined on a graph G, where the vertexes represent the qubits initialized in the state of $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and the edges represent a Controlled-Z (C-Z) operation, $\mathrm{CZ}^{\{i,j\}} = |0\rangle_i \langle 0| \otimes \mathbb{I}_j + |1\rangle_i \langle 1| \otimes Z_j$, between the two neighbor qubits. Then the graph state can be written as,

$$|G\rangle = \prod_{(i,j)\in E} \mathrm{CZ}^{\{i,j\}} |+\rangle^{\otimes N}. \tag{5-5}$$

Denote the Pauli operators on qubit i to be X_i, Y_i, Z_i. A N-partite graph state can also be uniquely determined by independent N stabilizers,

$$S_i = X_i \bigotimes_{j\in N_i} Z_j, \tag{5-6}$$

where N_i denotes the neighbor set of the vertex i. S_i commutes with each other and satisfies $S_i |G\rangle = |G\rangle$, $\forall i$. That is, the graph state is the unique eigenstate with eigenvalue of $+1$ for all the N stabilizers. Here, S_i contains identity operators for all the qubits that do not appear in Eq. (5-6). As a result, a graph state can be written as a product of stabilizer projectors,

$$|G\rangle \langle G| = \prod_{i=1}^{N} \frac{S_i + \mathbb{I}}{2}. \tag{5-7}$$

The fidelity between ρ and a graph state $|G\rangle$ can be obtained from measuring all possible products of stabilizers. However, as there are exponential terms in Eq. (5-7), this process is generally inefficient for large systems.

5.3 Entanglement structure witness

In this section, we propose a systematic method to detect entanglement structures of graph states. The main idea of our entanglement structure detection method runs as follows. First, with the close connection between the maximal Schmidt coefficient and quantum entropy, we upper-bound the fidelity of fully- and bi-separable states. These bounds are directly related to the entanglement entropy of the underlying graph states with respect to certain bipartition. Then, inspired by the genuine entanglement detection method [Tóth et al. (2005)], we lower-bound the fidelity between the unknown prepared state and the target graph state, with local measurements corresponding to the stabilizer operators of the graph state. Finally, by comparing theses fidelity bounds, we can witness the entanglement structures, such as the (genuine multipartite) entanglement between any subsystem partitions, and hence the entanglement intactness.

First, we give fidelity bounds between separable states and graph states as the following proposition.

Proposition 5.1： Given a graph state $|G\rangle$ and a partition $\mathcal{P} = \{A_i\}$, the fidelity between $|G\rangle$ and any $\mathcal{P}$-fully separable state is upper bounded by

$$\mathrm{Tr}\left(|G\rangle\langle G|\,\rho_f\right) \leq \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}; \tag{5-8}$$

and the fidelity between $|G\rangle$ and any $\mathcal{P}$-bi-separable state is upper bounded by

$$\mathrm{Tr}(|G\rangle\langle G|\,\rho_b) \leq \max_{\{A,\bar{A}\}} 2^{-S(\rho_A)}, \tag{5-9}$$

where $\{A, \bar{A}\}$ is a bipatition of $\{A_i\}$, and $S(\rho_A) = -\mathrm{Tr}[\rho_A \log_2 \rho_A]$ is the von Neumann entropy of the reduced density matrix $\rho_A = \mathrm{Tr}_{\bar{A}}(|G\rangle\langle G|)$.

Proof. First, let us prove the $\mathcal{P}$-bi-separable state case in Eq. (5-9). Since the $\mathcal{P}$-bi-separable state set $S_b^{\mathcal{P}}$ is convex, one only needs to consider the fidelity $|\langle\Psi_b|G\rangle|^2$ of the pure state $|\Psi_b\rangle$ define Eq. (5-3),

$$|\Psi_b\rangle = |\Phi_A\rangle \otimes |\Phi_{\bar{A}}\rangle\,. \tag{5-10}$$

It is known that the maximal value of the fidelity equals to the largest Schmidt coefficient of $|G\rangle$ with regard to the bipartition $\{A, \bar{A}\}$ [Bourennane et al. (2004)], i.e.,

$$\max_{|\Psi_b\rangle} |\langle\Psi_b|G\rangle|^2 = \lambda_1, \tag{5-11}$$

with the Schmidt decomposition $|G\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\,|\Phi_i\rangle_A\,|\Phi_i'\rangle_{\bar{A}}$ and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d$. For general graph state $|G\rangle$, the spectrum of any reduced density matrix ρ_A is flat, i.e., $\lambda_1 = \lambda_2 = \cdots \lambda_d$, with d being the rank of ρ_A [Hein et al. (2004)]. As a result, one has

$$S(\rho_A) = \log_2 d, \quad \lambda_i = \frac{1}{d} = 2^{-S(\rho_A)}. \tag{5-12}$$

To get an upper bound, one should maximize $2^{-S(\rho_A)}$ on all possible subsystem bipartitions and then obtain Eq. (5-9).

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Second, we prove the $\mathcal{P}$-fully separable state case in Eq. (5-8). Similarly, we only need to upper bound the fidelity of the pure state $|\Psi_f\rangle$ defined in Eq. (5-1),

$$|\Psi_f\rangle = \bigotimes_{i=1}^{m} |\Phi_{A_i}\rangle, \tag{5-13}$$

due to the convexity property of the $\mathcal{P}$-fully separable state set $S_f^{\mathcal{P}}$. From the proof of Eq. (5-9) above, we know that the fidelity of the $\mathcal{P}$-bi-separable state satisfies the bound $|\langle\Psi_b|G\rangle|^2 \leq 2^{-S(\rho_A)}$, given a subsystem bipartition $\{A, \bar{A}\}$. It is not hard to see that these bounds all hold for $|\Psi_f\rangle$, since $S_f^{\mathcal{P}} \subseteq S_b^{\mathcal{P}}$. Thus, one can obtain the finest bound via minimizing over all possible bipartitions and finally get Eq. (5-8). ■

The bound in Eq. (5-9) is tight, i.e., there always exists a $\mathcal{P}$-bi-separable state to saturate it. The bound in Eq. (5-8) may not be tight for some partition $\mathcal{P} = \{A_i\}$ and some graph state $|G\rangle$. In addition, we remark that to extend Theorem 5.1 from graph state to general state $|\Psi\rangle$, one should substitute the entropy in the bounds of Eqs. (5-8) and (5-9) with min-entropy $S_\infty(\rho_A)$ and $\rho_A = \mathrm{Tr}_{\bar{A}}(|\Psi\rangle\langle\Psi|)$.

The entanglement entropy $S(\rho_A)$ relates to the rank of the adjacency matrix, which can be efficiently calculated. Details are discussed in Appendix C.1.1. While the optimization problems can be computationally hard due to the exponential number of possible bipartitions, one can solve it properly as the number of the subsystems m is not too large. In addition, we can always have an upper bound on the minimisation by only considering specific partitions. Analytical calculation of the optimization is possible for graph states with certain symmetries, such as the 1-D and 2-D cluster states and the GHZ state, as we will discuss later in Corollaries.

Next, we propose an efficient method to lower bound the fidelity between an unknown prepared state and the target graph state. A graph is k-colorable if one can divide the vertex set into k disjoint subsets $\bigcup V_l = V$ such that any two vertexes in the same subset are not connected. The smallest number k is called the chromatic number of the graph ①. We define the stabilizer projector of each subset V_l as

$$P_l = \prod_{i\in V_l} \frac{S_i + \mathbb{I}}{2}, \tag{5-14}$$

where S_i is the stabilizer of $|G\rangle$ in subset V_i. The expectation value of each P_l can be obtained by one local measurement setting $\bigotimes_{i\in V_l} X_i \bigotimes_{j\in V/V_l} Z_j$. Then, we can propose a

---

① Note that the colorability is a property of the graph (not the state), one may reduce the number of measurement settings by local Clifford operations [Hein et al. (2006)].

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

fidelity evaluation scheme with k local measurement settings, as the following proposition.

Proposition 5.2: For a graph state $|G\rangle\langle G|$ and the projectors P_l defined in Eq. (5-14), the following inequality holds,

$$|G\rangle\langle G| \geq \sum_{l=1}^{k} P_l - (k-1)\mathbb{I}, \tag{5-15}$$

where $A \geq B$ indicates that $A - B$ is positive-semidefinite.

Proof. A graph state $|G\rangle$ can be written in the following form

$$|G\rangle\langle G| = \prod_{i=1}^{N} \frac{S_i + \mathbb{I}}{2} = \prod_{l=1}^{k} P_l. \tag{5-16}$$

Accordingly, Eq. (5-15) in Proposition 5.2 becomes,

$$\left[\prod_{l=1}^{k} P_l + (k-1)\mathbb{I}\right] - \sum_{l=1}^{k} P_l \geq 0. \tag{5-17}$$

The projectors P_l commute with each other, thus we can prove (5-17) for all subspaces which are determined by the eigenvalues of all P_l. For the subspace where the eigenvalues of all P_l are 1, the inequality $(1 + k - 1) - k \geq 0$ holds. For the subspace where only one of P_l takes value of 0, the inequality $(0 + k - 1) - (k - 1) \geq 0$ holds. Moreover, for the subspace in which there are more than one P_l taking 0, the inequality also holds. As a result, we finish the proof. ■

Note that Proposition 5.2 with $k = 2$ case has also been studied in literature [Tóth et al. (2005)]. Combining Propositions 5.1 and 5.2, we propose an entanglement structure witness with k local measurement settings, as presented in the following theorem.

Theorem 5.1: Given a partition $\mathcal{P} = \{A_i\}$, the operator $W_f^{\mathcal{P}}$ can witness non-$\mathcal{P}$-fully separability (entanglement),

$$W_f^{\mathcal{P}} = \left(k - 1 + \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}\right)\mathbb{I} - \sum_{l=1}^{k} P_l, \tag{5-18}$$

with $\langle W_f^{\mathcal{P}}\rangle \geq 0$ for all $\mathcal{P}$-fully-separable states; and the operator $W_b^{\mathcal{P}}$ can witness $\mathcal{P}$-genuine entanglement,

$$W_b^{\mathcal{P}} = \left(k - 1 + \max_{\{A,\bar{A}\}} 2^{-S(\rho_A)}\right)\mathbb{I} - \sum_{l=1}^{k} P_l, \tag{5-19}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

with $\langle W_b^{\mathcal{P}} \rangle \geq 0$ for all $\mathcal{P}$-bi-separable states, where $\{A, \bar{A}\}$ is a bipartition of $\{A_i\}$, $\rho_A = \mathrm{Tr}_{\bar{A}}(|G\rangle\langle G|)$, and the projectors P_l is defined in Eq. (5-14).

Proof. The proof is to combine Proposition 5.1 and 5.2. Here we only show the proof of Eq. (5-18), and Eq. (5-19) can be proved in the same way. To be specific, one needs to show that any $\mathcal{P}$-fully separable state satisfies the $\langle W_f^{\mathcal{P}} \rangle \geq 0$, that is,

$$\begin{aligned} \mathrm{Tr}\left\{\sum_{l=1}^{k} P_l \rho_f\right\} &\leq \mathrm{Tr}\left\{[(k-1)\mathbb{I} + |G\rangle\langle G|]\,\rho_f\right\} \\ &\leq (k-1) + \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}. \end{aligned} \tag{5-20}$$

where the first and the second inequalities are on account of Proposition 5.2 and 5.1, respectively. ■

The proposed entanglement structure witnesses have several favourable features. First, given an underlying graph state, the implementation of the witnesses is the same for different partitions. This feature allows us to study different entanglement structures in one experiment. Note that the witness operators in Eqs. (5-18) and (5-19) can be divided into two parts: The measurement results of P_l obtained from the experiment rely on the prepared unknown state and are independent of the partition; The bounds, $1 + \min(\max)_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$, on the other hand, rely on the partition and are independent of the experiment. Hence, in the data postprocessing of the measurement results of P_l, we can study various entanglement structures for different partitions by calculating the corresponding bounds analytically or numerically.

Second, besides investigating the entanglement structure among all the subsystems, one can also employ the same experimental setting to study that of a subset of the subsystems, by performing different data post-processing. For example, suppose the graph G is partitioned into 3 parts, say A_1, A_2 and A_3, and only the entanglement between subsystems A_1 and A_2 is of interest. One can construct new witness operators with projectors P_l', by replacing all the Pauli operators on the qubits in A_3 in Eq. (5-14) to identities. Such measurement results can be obtained by processing the measurement results of the original P_l. Then the entanglement between A_1 and A_2 can be detected via Theorem 5.1 with projectors P_l' and the corresponding bounds of the graph state $|G_{A_1A_2}\rangle$. Details are discussed in Appendix C.1.3.

Third, when each subsystem A_i contains only one qubit, that is, $m = N$, the witnesses in Theorem 5.1 become the conventional ones. It turns out that Eq. (5-19) is the same for

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

all the graph states under the N-partition $\mathcal{P}_N$, as shown in the following corollary. Note that, a special case of the corollary, the genuine entanglement witness for the GHZ and 1-D cluster states, has been studied in literature [Tóth et al. (2005)].

Corollary 5.1： The operator $W_b^{\mathcal{P}_N}$ can witness genuine multipartite entanglement,

$$W_b^{\mathcal{P}_N} = \left(k - \frac{1}{2}\right)\mathbb{I} - \sum_{l=1}^{k} P_l, \tag{5-21}$$

with $\langle W_b^{\mathcal{P}_N}\rangle \geq 0$ for all bi-separable states, where P_l is defined in Eq. (5-14) for any graph state.

Fourth, the witness in Eq. (5-18) can be naturally extended to identify non-m-separability, by investigating all possible partitions $\mathcal{P}_m$ with fixed m. In fact, according to the definition of m-separable states and Eq. (5-8), the fidelity between any m-separable state ρ_m and the graph state $|G\rangle$ can be upper bounded by $\max_{\mathcal{P}_m} \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$, where the maximization is over all possible partitions with m subsystems. As a result, we have the following theorem on the non-m-separability.

Theorem 5.2： The operator W_m can witness non-m-separability,

$$W_m = \left(k - 1 + \max_{\mathcal{P}_m} \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}\right)\mathbb{I} - \sum_{l=1}^{k} P_l, \tag{5-22}$$

with $\langle W_m\rangle \geq 0$ for all m-separable states, where the maximization takes over all possible partitions $\mathcal{P}_m$ with m subsystems, the minimization takes over all bipartition of $\mathcal{P}_m$, $\rho_A = \mathrm{Tr}_{\bar{A}}(|G\rangle\langle G|)$, and the projector P_l is defined in Eq. (5-14).

Proof. With Eq. (5-8) one can bound the fidelity from any $\mathcal{P}$-fully separable state to a graph state $|G\rangle$. The m-separable state set S_m contains all the state ρ_m which can be written the convex mixture of pure m-separable state, $\rho_m = \sum_i p_i |\Psi_m^i\rangle\langle\Psi_m^i|$, where the partition for each constitute $|\Psi_m^i\rangle$ needs not to be the same. Hence one can bound the fidelity from ρ_m to a graph state $|G\rangle$ by investigating all possible partitions, i.e.,

$$\mathrm{Tr}(|G\rangle\langle G|\rho_m) \leq \max_{\mathcal{P}_m} \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}, \tag{5-23}$$

where the maximization takes over all possible partitions $\mathcal{P}_m$ with m subsystems, the minimization takes over all bipartition of $\mathcal{P}_m$. Then like in Eq. (5-20), by combing Eqs. (5-15) and (5-23) we finish the proof. ■

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

The optimization problem in Theorem 5.2 over the partitions is generally hard, since there are about $m^N/m!$ possible ways to partition N qubits into m subsystems. For example, when N is large (say, in the order of 70 qubits), the number of different partitions is exponentially large even with a small separability number m. Similarly, as discussed below Proposition 5.1, the optimization problem in Theorem 5.1 is also generally hard. Surprisingly, for several widely-used types of graph states, such as 1-D, 2-D cluster states, and the GHZ state, we find the analytical solutions to the optimization problem, as shown in the following Corollaries.

5.4 Robustness of entanglement structure witnesses

In this section, we discuss the robustness of the proposed witnesses in Theorem 5.1 and Theorem 5.2. In practical experiment, the prepared state ρ deviates from the target graph state $|G\rangle$ due to nonnegligible noise. Here we utilize the following white noise model to quantify the robustness of the witnesses,

$$\rho = (1 - p_{noise}) |G\rangle \langle G| + p_{noise}\frac{\mathbb{I}}{2^N}, \tag{5-24}$$

which is a mixture of the original state $|G\rangle$ and maximally mixed state and with coefficient p_{noise}. We will find the largest p_{limit}, such that the witness can detect the corresponding entanglement structure when $p_{noise} < p_{limit}$. Thus p_{limit} reflects the robustness of the witness.

Let us first consider the entanglement witness $W_f^{\mathcal{P}}$ in Eq. (5-18) of Theorem 5.1. For clearness, we denote $C_{min} = \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$. Insert the state of Eq. (5-24) into the witness, one gets,

$$\begin{aligned}
\mathrm{Tr}(W_f^{\mathcal{P}}\rho) &= \mathrm{Tr}\left\{\left[(k-1+C_{min})\mathbb{I} - \sum_{l=1}^{k} P_l\right]\left[p_{noise}\frac{\mathbb{I}}{2^N} + (1-p_{noise})|G\rangle\langle G|\right]\right\}, \\
&= p_{noise}\left(k-1+C_{min} - 2^{-N}\sum_{l=1}^{k} 2^{N-n_l}\right) + (1-p_{noise})(k-1+C_{min}-k), \\
&= p_{noise}\left(-\sum_{l=1}^{k} 2^{-n_l} + k\right) + (C_{min}-1),
\end{aligned} \tag{5-25}$$

where $n_l = |V_l|$ is the qubit number in each vertex set with different color, and in the second line we employ the facts that $\mathrm{Tr}(P_l) = 2^{N-n_l}$ and $\mathrm{Tr}(P_l |G\rangle\langle G|) = 1$. Let the above

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

expectation value less than zero, one has

$$p_{noise} < \frac{1 - C_{min}}{k - \sum_{l=1}^{k} 2^{-n_l}}. \tag{5-26}$$

Similarly, for the $\mathcal{P}$-genuine entanglement witness and non-m-separability witness in Eqs. (5-19) and (5-22), we have,

$$\begin{aligned} p_{noise} &< \frac{1 - C_{max}}{k - \sum_{l=1}^{k} 2^{-n_l}}, \\ p_{noise} &< \frac{1 - C_{m}}{k - \sum_{l=1}^{k} 2^{-n_l}}, \end{aligned} \tag{5-27}$$

where we denote the optimizations $\max_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$ and $\max_{\mathcal{P}_m} \min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$ as C_{max} and C_m respectively.

Moreover, it is not hard to see that all the coefficients C_{min}, C_{max} and C_m are less than 0.5. Thus, for any entanglement structure witness, one has

$$p_{limit} \geq \frac{0.5}{k - \sum_{l=1}^{k} 2^{-n_l}} \geq \frac{1}{2k}. \tag{5-28}$$

As a result, our entanglement structure witness is quite robust to noise, since the largest noise parameter p_{limit} is just related to the chromatic number of the graph.

5.5 Several typical examples

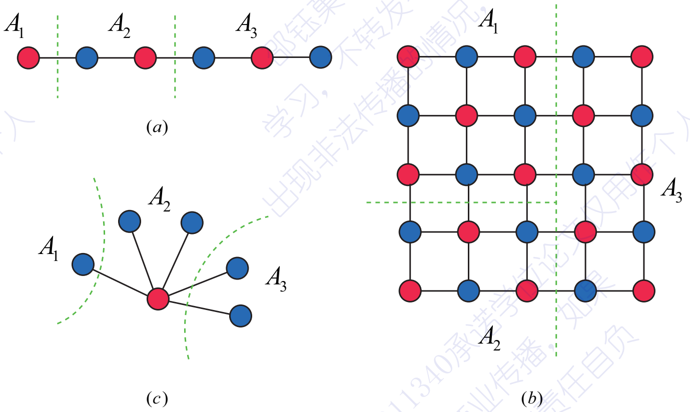
For several widely-used graph states, 1-D, 2-D cluster states, and the GHZ state, the corresponding graphs are all 2-colorable. Thus, we can realize the witnesses with only two local measurement settings. For clearness, the vertexes in the subsets V_1 and V_2 are associated with red and blue colors respectively, as shown in Fig. C.1. We write the stabilizer projectors defined in Eq. (5-14) for the two subsets as,

$$P_1 = \prod_{red\ i} \frac{S_i + \mathbb{I}}{2}, \; P_2 = \prod_{blue\ i} \frac{S_i + \mathbb{I}}{2}. \tag{5-29}$$

The more general case with k-chromatic graph states is presented in Appendix C.1.4.

We start with a 1-D cluster state $|C_1\rangle$ with stabilizer projectors in the form of Eq. (5-29). Consider an example of tripartition $\{A_1, A_2, A_3\}$, as shown in Fig. C.1(a), there are three ways to divide the three subsystems into two sets, i.e., $\{A, \bar{A}\} = \{A_1, A_2A_3\}$, $\{A_2, A_1A_3\}$, $\{A_3, A_1A_2\}$. It is not hard to see that the corresponding entanglement entropies are $S(\rho_{A_1}) = S(\rho_{A_3}) = 1$ and $S(\rho_{A_2}) = 2$. Note that in the calculation, each broken edge

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负



(a) (c) (b)

Figure 5.2 Graphs of the (a) 1-D cluster state $|C_1\rangle$, (b) 2-D cluster state $|C_2\rangle$, and (c) GHZ state $|GHZ\rangle$. Note that the graph state form of the GHZ state is equivalent to its canonical form, $(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$, up to local unitary operations.

will contribute 1 to the entropy, which is a manifest of the area law of entanglement entropy [Eisert et al. (2010)]. According to Theorem 5.1, the operators to witness $\mathcal{P}_3$-entanglement structure are given by,

$$
\begin{aligned}
W_{f,C_1}^{\mathcal{P}_3} &= \frac{5}{4}\mathbb{I} - (P_1 + P_2),\\
W_{b,C_1}^{\mathcal{P}_3} &= \frac{3}{2}\mathbb{I} - (P_1 + P_2),
\end{aligned}
\tag{5-30}
$$

where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the graph of Fig. C.1(a).

Next, we take an example of 2-D cluster state $|C_2\rangle$ defined in a 5×5 lattice and consider a tripartition, as shown in Fig. C.1(b). Similar to the 1-D cluster state case with the area law, the corresponding entanglement entropies are $S(\rho_{A_1}) = S(\rho_{A_3}) = 5$ and $S(\rho_{A_2}) = 4$. According to Theorem 5.1, the operators to witness $\mathcal{P}_3$-entanglement structure are given by,

$$
\begin{aligned}
W_{f,C_2}^{\mathcal{P}_3} &= \frac{33}{32}\mathbb{I} - (P_1 + P_2),\\
W_{b,C_2}^{\mathcal{P}_3} &= \frac{17}{16}\mathbb{I} - (P_1 + P_2),
\end{aligned}
\tag{5-31}
$$

where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the graph of Fig. C.1(b). Similar analysis works for other partitions and other graph states.

Now, we consider the case where each subsystem A_i contains exactly one qubit, $\mathcal{P}_N$. Then, witnesses in Eq. (5-18) become the conventional ones, as shown in the following Corollary.

邵钰茱2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Corollary 5.2： The operator $W_{f,C}^{\mathcal{P}_N}$ can witness can witness non-fully separability (entanglement),

$$W_{f,C}^{\mathcal{P}_N} = (1 + 2^{-\lfloor \frac{N}{2} \rfloor})\mathbb{I} - (P_1 + P_2), \tag{5-32}$$

with $\langle W_{f,C}^{\mathcal{P}_N} \rangle \geq 0$ for all fully separable states, where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the stabilizers of any 1-D or 2-D cluster state.

Here, we only show the cases of 1-D and 2-D cluster states. We conjecture that the witness holds for any (such as 3-D) cluster states. For a general graph state, on the other hand, the corollary does not hold. In fact, we have a counter example of the GHZ state. It is not hard to show that for any GHZ state, the entanglement entropy is given by,

$$S(\rho_A^{GHZ}) = 1, \quad \forall \{A, \bar{A}\}. \tag{5-33}$$

Then, Eqs. (5-18) and (5-19) yield the same witnesses. That is, the witness constructed by Theorem 5.1 for the GHZ state can only tell genuine entanglement or not.

Following Theorem 5.2, one can fix the number of the subsystems m and investigate all possible partitions to detect the non-m-separability. The optimization problem can be solved analytically for the 1-D and 2-D cluster states, as shown in Corollary 5.3 and 5.4, respectively.

Corollary 5.3： The operator W_{m,C_1} can witness non-m-separability,

$$W_{m,C_1} = (1 + 2^{-\lfloor \frac{m}{2} \rfloor})\mathbb{I} - (P_1 + P_2), \tag{5-34}$$

with $\langle W_{m,C_1} \rangle \geq 0$ for all m-separable states, where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the stabilizers of a 1-D cluster state.

In particular, when $m = 2$ and $m = N$, W_{m,C_1} becomes the entanglement witnesses in Eqs. (5-21) and (5-32), respectively. Comparing to the 1-D cluster state case, the partition of the 2-D cluster state is much richer and its separability witness is shown in the following corollary.

Corollary 5.4： The operator W_{m,C_2} can witness non-m-separability for $N \geq m(m-1)/2$,

$$W_{m,C_2} = \left(1 + 2^{-\left\lceil \frac{-1+\sqrt{1+8(m-1)}}{2} \right\rceil}\right)\mathbb{I} - (P_1 + P_2), \tag{5-35}$$

with $\langle W_{m,C_2} \rangle \geq 0$ for all m-separable states, where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the stabilizers of a 2-D cluster state.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

We remark that the witnesses constructed in Corollaries 5.1, 5.2, and 5.3 are tight. Take the witness W_{m,C_1} in Corollary 5.3 as an example. There exists an m-separable state ρ_m that saturates $\mathrm{Tr}(\rho_m W_{m,C_1}) = 0$. In addition, as $m \leq 5$, the witness W_{m,C_2} in Corollary 5.4 is also tight. Detailed discussions are presented in Appendix C.1.2.

5.6 Discussion

The proposed witnesses can be directly generalized to stabilizer states [Gottesman (1997); Nielsen et al. (2010)], which are equivalent to graph states up to local Clifford operations [Hein et al. (2006)]. It is also interesting to extend the method to more general multipartite quantum states, such as hyper-graph states [Rossi et al. (2013)], tensor network states [Orùs (2014)]. In addition, the generalization to neural network state [Carleo et al. (2017)] is also intriguing, since this kind of ansatz is able to represent broader quantum states with a volume law of entanglement entropy [Deng et al. (2017)], and is a fundamental block for potential artificial intelligence applications.

In addition, one may utilize the proposed witness method to detect other multipartite entanglement properties, such as entanglement depth and width [Sørensen et al. (2001); Wölk et al. (2016)], as m-separability in this work. Further more, one can also consider the self-testing scenario, such as (measurement)-device-indepedent settings [Branciard et al. (2013); Liang et al. (2015)], which can help to manifest the entanglement structures with less assumptions on the devices.

Finally, considering the case of GHZ state, all the entanglement witnesses are reduced to one operator, which hinders us from investigating more detailed entanglement structures. Thus, it is also necessary to develop other methods to resolve this situation, such as the witnesses proposed in Ref. [Lu et al. (2018)] for GHZ-like states.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Part IV

Applications in quantum information processing

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 6 Operational interpretation of coherence in quantum key distribution

As the notion that captures the quantum superposition between differentiable physical states, quantum coherence represents one of the fundamental features that distinguish quantum mechanics from its classical counterpart [Born (1926); Schrödinger (1935)]. Despite of the early recognition of its importance, quantum coherence was only recently formalized under a rigourous framework of resource theory [Baumgratz et al. (2014)], which stimulated a rapidly growing research field on quantum coherence, ranging from its mathematical characterizations to its operational interpretations [Streltsov et al. (2017a)].

The motivation on studying the operational interpretation of quantum coherence is two-folded. First, by linking coherence to the operational advantage of quantum information processing protocols, one can improve existing protocols and derive new ones by exploiting similar mechanisms. Second, the observable phenomenon bestowed by quantum coherence allows one to better understand the boundary between quantum and classical realms, one of the fundamental problems in theoretical physics.

The operational significance of quantum coherence has been recognized in many areas, including quantum metrology [Braunstein et al. (1996)], quantum computing [Nielsen et al. (2010)], quantum thermodynamics [Åberg (2014); Lostaglio et al. (2015a)] and quantum biology [Huelga et al. (2013)]. With the newly developed resource theory of coherence, more operational significance of coherence was discovered and quantified [Bagan et al. (2016); Hillery (2016); Lostaglio et al. (2015b); Marvian et al. (2016b); Matera et al. (2016); Napoli et al. (2016)]. Recently, it is shown that coherence quantifies the amount of unpredictable intrinsic randomness from measuring quantum states [Yuan et al. (2015, 2016)]. Such a relation has been applied to develop source-independent quantum random number generators [Ma et al. (2017)]. Take a qubit as an example, the state $|\psi_A\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ can yield intrinsic randomness when measured in the Z basis, which is unpredictable to an adversary, Eve. In comparison, the measurement result of $\rho_A = (|0\rangle\langle 0| + |1\rangle\langle 1|)/2$ with zero coherence can be fully determined by Eve if she holds the purification of ρ_A, that is, $|\psi_{AE}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

In this chapter, we investigate the significant role of coherence played in QKD, via considering the relation between coherence and intrinsic randomness. This chapter is

邵钰棻202031134 0承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

organized as follows. In Table 6.1, we list the notations used in the following discussions. In Sec. 6.1, we introduce the security analysis framework based on quantifying coherence, and present an explicit key rate formula related to the coherence of the bipartite state in the key generation basis. In Sec. 6.2, by applying the framework to the BB84 and six-state protocols, we reproduce the original key rate formulas. Then, in Sec. 6.3, with analytical tools well developed under the resource theory of coherence, we improve the key rates of these two protocols by using fine-grained parameters in postprocessing the measurement outcomes. Furthermore, in Sec. 6.4, we apply the framework to solve a practical issue in QKD, detection efficiency mismatch, where two detectors are not identical in terms of the detection efficiency. The derived key rate shows an advantage over previous analyses. We also discuss the interplay among coherence, entanglement, and QKD security in Sec. 6.5. Finally, the discussion and outlook are contained in Sec. 6.6. The content of this chapter is from the work [Ma et al. (2018)], where I am a co-first author.

Table 6.1 Notations in Chapter 6

I	a reference basis of $\mathcal{H}_d$, $\{\|0\rangle, \ldots, \|d-1\rangle\}$
ρ^{diag}	diagonal state of ρ in the reference basis, $\sum_i \langle i\| \rho \|i\rangle \|i\rangle \langle i\|$
$H(a)$	Shannon entropy of a random variable a, $-\sum_a q(a) \log q(a)$
$H(e)$	binary Shannon entropy function, $-e \log e - (1-e) \log(1-e)$
$H(a\|b)$	conditional entropy of two random variables a and b, $H(ab) - H(b)$
$S(\rho)$	von Neumann entropy of ρ, $-\mathrm{Tr}[\rho \log(\rho)]$
$S(A\|B)$	conditional quantum entropy of ρ_{AB}, $S(\rho_{AB}) - S(\rho_B)$
Γ_i	positive operator valued measure (POVM) on bipartite Hilbert space $\mathcal{H}_{AB}$
$\mathbf{\Gamma}$	set of the operators Γ_i, $\{\Gamma_i\}$
Z basis	reference basis of a qubit, $\{\|0\rangle, \|1\rangle\}$
X basis	conjugate basis of a qubit, $\{\|+\rangle, \|-\rangle\}$, where $\|\pm\rangle = (\|0\rangle \pm \|1\rangle)/\sqrt{2}$
Y basis	conjugate basis of a qubit, $\{\|+i\rangle, \|-i\rangle\}$, where $\|\pm i\rangle = \frac{1}{\sqrt{2}}(\|0\rangle \pm i\,\|1\rangle)$
Π^+	Z-basis parity projector on a 2-qubit space, $\|00\rangle\langle 00\| + \|11\rangle\langle 11\|$
Π^-	Z-basis parity projector on a 2-qubit space, $\|01\rangle\langle 01\| + \|10\rangle\langle 10\|$
Π_x^+	X-basis parity projector on a 2-qubit space, $\|++\rangle \langle --\| + \|--\rangle \langle --\|$
Π_x^-	X-basis parity projector on a 2-qubit space, $\|+-\rangle \langle +-\| + \|-+\rangle \langle -+\|$
Π_y^-	Y-basis parity projector on a 2-qubit space, $\|+i+i\rangle \langle +i+i\| + \|-i-i\rangle \langle -i-i\|$
$\Phi(\rho)$	partial dephasing channel, $\Pi^+ \rho \Pi^+ + \Pi^- \rho \Pi^-$
$\mathcal{Z}$	Z-basis measurement result

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

6.1 Security framework with coherence

In this section, we provide a framework that relates the security analysis of QKD to the resource theory of coherence.

In the scenario of QKD, two legitimated users, Alice and Bob, intend to share a sequence of private and identical bits, called secret key. In a QKD security analysis, one always needs to consider two steps in postprocessing. One is information reconciliation that ensures the keys shared by Alice and Bob to be identical. The other is privacy amplification that extracts secure key from the raw key. In general, information reconciliation is a standard classical process; while privacy amplification is determined by the quantum procedures of the protocol. Privacy amplification plays a central role in all security proofs. For example, in the Shor-Preskill security proof [Shor et al. (2000)], privacy amplification is linked to the phase error correction in an equivalent entanglement protocol [Lo et al. (1999)]. In this chapter, we examine the postprocessing in an alternative way. After information reconciliation, the amount of secret key that can be extracted from privacy amplification is essentially determined by the intrinsic randomness that is unknown to Eve. This intrinsic randomness can be quantified by the coherence of the joint system of Alice and Bob. For example, in the entanglement version of the BB84 protocol [Bennett et al. (1984, 1992)], suppose there are only phase errors left, the final state shared by Alice and Bob is a mixture of $(|00\rangle + |11\rangle)/\sqrt{2}$ and $(|00\rangle - |11\rangle)/\sqrt{2}$. If the phase error rate takes the worst case of 50%, the state becomes $(|00\rangle\langle 00| + |11\rangle\langle 11|)/2$, which has no coherence in the Z basis, and hence no secret key can be generated. Following this spirit, we propose a generic security analysis framework for QKD, under which, we show that the key generation rate is closely related to the amount of coherence within the joint quantum states.

In the following discussions, we consider an entanglement-based QKD scheme, since the prepare-and-measure schemes can be converted to the entanglement-based ones with the standard technique [Shor et al. (2000)]. Also, we consider the security analysis with respect to the condition that the shared states between Alice and Bob of different rounds are i.i.d. This is the collective attack scenario considered in QKD [Devetak et al. (2005)]. Then, a generic QKD protocol can be described in Fig. 6.1.

In a security proof, the parameter estimation is a crucial step, which determines the amount of secure keys that can be extracted in QKD. Essentially, Alice and Bob perform some measurement $\Gamma_i \in \mathbf{\Gamma}$ to estimate the information of ρ_{AB}, with the expectation value

邵钰菓2020311340承诺学位论文仅作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

- (I). N pairs of qubit states, $\rho_{AB}^{\otimes N}$, are distributed to Alice and Bob.
- (II). They randomly sample $N-n$ copies of ρ_{AB} for parameter estimation, where $0<n<N$.
- (III). For the remaining n copies of ρ_{AB}, Alice and Bob each performs the Z-basis measurement to generate the raw key.
- (IV). They perform classical information reconciliation on the raw key to share identical keys.
- (V). They perform privacy amplification based on the information provided in the parameter estimation to share private keys.

Figure 6.1 Generic QKD against collective attacks

being $\gamma_i = \mathrm{Tr}(\rho_{AB}\Gamma_i)$. As a result, ρ_{AB} should fulfill a set of constraints, $\rho_{AB}\in\mathbf{S}$, where $\mathbf{S}$ denotes the set which contains all the states satisfying constraints from parameter estimation,

$$\mathbf{S} := \{\rho_{AB}|\mathbf{\Gamma} : \mathrm{Tr}(\rho_{AB}\Gamma_i)=\gamma_i\}. \tag{6-1}$$

Now we provide the main result of this chapter, which connects the key rate of QKD with the relative entropy of coherence. Our derivation is based on the close relation between intrinsic randomness and quantum coherence.

Theorem 6.1： In the asymptotic limit where $n, N\to\infty$, the secret key rate of the above QKD protocol is given by

$$K = \min_{\rho_{AB}\in\mathcal{S}} C(\Phi(\rho_{AB})) - I_{ec}, \tag{6-2}$$

where $\Phi(\cdot)$ is the partial dephasing operation defined in Table 6.1, $C(\cdot)$ is the relative entropy of coherence on the computational basis $Z_A\otimes Z_B$, and I_{ec} is the information leakage during key reconciliation.

Note that I_{ec} in Eq. (6-2), which accounts for the private key consumed in the information reconciliation step, can be directly estimated by the measurement statistics from parameter estimation. Sometimes parameter estimation is not even needed here as long as an error verification step is applied after information reconciliation [Fung et al. (2010)]. Thus, the minimization is only on the first term that quantifies the security of the key by quantum coherence. Without loss of generality, in the following analysis, we employ the one-way information reconciliation scheme such that $I_{ec} = H(\mathcal{Z}_A|\mathcal{Z}_B)$ ①. We need to emphasize that our result can be applied to more general postprocessing protocols, e.g., two-way classical-communication protocol [Gottesman et al. (2003)]. This is possible because our framework entirely decouples the privacy amplification step from the information reconciliation step. In the following proof, we show an equivalent virtual protocol which employs quantum bit error correction that commutes with the Z-basis measurement. This follows the same spirit of Lo-Chau's and Shor-Preskill's proofs for the BB84 protocol [Lo et al. (1999); Shor et al. (2000)].

Proof. Let $K(\rho_{AB})$ denote the key rate when the shared quantum state is known to be ρ_{AB}. To estimate the secret key rate K, one should consider *the worst case* of $\rho_{AB} \in \mathcal{S}$, i.e.

$$K = \min_{\rho_{AB} \in \mathcal{S}} K(\rho_{AB}). \tag{6-3}$$

where $\mathcal{S}$ is the set of quantum states ρ_{AB} that consistent with the measurement statistics obtained in the parameter estimation step, as defined in Table 6.1.

First, we consider an equivalent virtual protocol, where Alice and Bob perform the information reconciliation before the Z-basis measurement, i.e., step (iii) and (iv) in Fig. 6.1 are exchanged. Then, step (iii) and step (iv) are replaced by

(iii') With the Z-basis measurement results obtained in parameter estimation, Alice and Bob perform quantum bit error correction on the n copies of ρ_{AB}, which is equivalent to apply a global Z-basis parity projector $\{\Pi^+, \Pi^-\}$ on the joint state. Then, Alice (or Bob) applies the $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ to rotate all the joint states to the subspace Π^+.

(iv') Alice and Bob perform the Z-basis measurement on the error corrected state to generate the identical key.

Note that the quantum bit error correction in step (iii') commutes with the Z-basis measurement, since all operations are performed in the Z basis. Thus, this virtual protocol is equivalent to the one shown in Fig. 6.1. The quantum bit error correction in the virtual protocol can be realized with pre-shared $nH(\mathcal{Z}_A|\mathcal{Z}_B)$ EPR pairs. In the original protocol, the amount of key cost is given by the conditional entropy $H(\mathcal{Z}_A|\mathcal{Z}_B)$. This step is essentially classical. See D.1 for more detailed discussions. Define the bit error rate,

---

① Here, one-way information reconciliation means that in the post-processing stage, Alice (or Bob) could determine the final key from her (or his) sifted key directly. For example, one can use Alice's sifted key after privacy-amplification hashing as the final key.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

$e_b = \mathrm{Tr}(\Pi^- \rho_{AB})$ and

$$H(\mathcal{Z}_A|\mathcal{Z}_B) \leq H(e_b), \tag{6-4}$$

where the equality holds for the symmetric case.

After the quantum bit error correction step (iii'), the original $\rho_{AB}^{\otimes n}$ is transformed to $n(1-e_b)$ copies of $\rho_{AB}^+ = \Pi^+ \rho_{AB} \Pi^+ / \mathrm{Tr}(\Pi^+ \rho_{AB})$ and ne_b copies of $\sigma_x^B \rho_{AB}^- \sigma_x^B$, with $\rho_{AB}^- = \Pi^- \rho_{AB} \Pi^- / \mathrm{Tr}(\Pi^- \rho_{AB})$. In step (iv'), when Alice and Bob measure these states in the Z basis, they will get identical keys.

To perform the privacy amplification in step (v), one essentially needs to characterize the amount of intrinsic randomness in the error corrected keys that are unpredictable to Eve. Thus the key rate shows

$$K(\rho_{AB}) = \frac{1}{n}\left\{n(1-e_b)R(\rho_{AB}^+) + ne_b R(\sigma_x^B \rho_{AB}^- \sigma_x^B) - nH(\mathcal{Z}_A|\mathcal{Z}_B)\right\}. \tag{6-5}$$

Recall the relation between intrinsic randomness and coherence shown in Eq. (2-30),

$$R(\rho) = C(\rho), \tag{6-6}$$

where the reference basis of relative entropy of coherence C coincides with the basis $Z_A \otimes Z_B$. Then we have

$$\begin{aligned} K(\rho_{AB}) &= \frac{1}{n}\left\{n(1-e_b)C(\rho_{AB}^+) + ne_b C(\sigma_x^B \rho_{AB}^- \sigma_x^B) - nH(\mathcal{Z}_A|\mathcal{Z}_B)\right\} \\ &= (1-e_b)C(\rho_{AB}^+) + e_b C(\rho_{AB}^-) - H(\mathcal{Z}_A|\mathcal{Z}_B) \\ &= C((1-e_b)\rho_{AB}^+ + e_b \rho_{AB}^-) - H(\mathcal{Z}_A|\mathcal{Z}_B) \\ &= C(\Phi(\rho_{AB})) - H(\mathcal{Z}_A|\mathcal{Z}_B), \end{aligned} \tag{6-7}$$

where the third equality employs the additivity property of coherence and the Hilbert space of ρ_{AB}^+ and ρ_{AB}^- are orthogonal [Yu et al. (2016)]. Inserting Eq. (6-7) to Eq. (6-3), one obtains Eq. (6-2). ■

Note that in the symmetric case, where the bit value of the raw key is evenly distributed, the information reconciliation part is given by Eq. (6-4) with equality, then the key rate formula can be further written as,

$$K = \min_{\rho_{AB} \in \mathcal{S}} C(\Phi(\rho_{AB})) - H(e_b). \tag{6-8}$$

We need to point out that in general, for the asymmetric case, $H(e_b) \geq H(\mathcal{Z}_A|\mathcal{Z}_B)$ on account of Fano's inequality.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

6.2 Key rates of BB84 and six-state QKD

As examples, we apply the framework to the security analysis of the BB84 and six-state QKD protocols in the collective-attack scenario. One can see that the secret key rates of these two protocols can be directly derived with the tools well developed within the resource theory of coherence [Streltsov et al. (2017a)]. We list the results of these two re-derivations as the following corollaries. Note that these two protocols only differ from each other on the measurement $\{\Gamma_i\}$ performed in parameter estimation. For simplicity, we consider the symmetric case, where Eq. (6-8) holds.

6.2.1 BB84 protocol

Consider the entanglement-based version of BB84 protocol, where in parameter estimation, Alice and Bob obtain the bit error rate $e_b = \mathrm{Tr}(\Pi^- \rho_{AB})$ and the phase error rate $e_p = \mathrm{Tr}(\Pi_x^- \rho_{AB})$. Then following Theorem 6.1, we have the following corollary.

Corollary 6.1： The key rate of the BB84 QKD protocol K_{BB84} is given by

$$\begin{aligned} K_{BB84} &= \min_{\rho_{AB} \in \mathcal{S}} C(\Phi(\rho_{AB})) - H(e_b) \\ &= 1 - H(e_p) - H(e_b). \end{aligned} \tag{6-9}$$

where $\mathcal{S}$ contains all the states yielding the same bit error rate e_b and phase error rate e_p obtained from parameter estimation.

The result is consistent with the one from the Shor-Preskill security proof [Shor et al. (2000)]. We prove this corollary by first showing that $K(\rho_{AB}) \geq K_{BB84}$ for all $\rho_{AB} \in \mathcal{S}$, and then giving a specific state in this set to saturate the inequality.

Proof. First note that the four eigenstates of $Z_A \otimes Z_B$ and $X_A \otimes X_B$ are a pair of mutually unbiased bases in the 4-dimensional system $H_A^2 \otimes H_B^2$. Denote the $\Delta_{Z_{AB}}$ ($\Delta_{X_{AB}}$) to be the projective measurement outcome on the $Z_A \otimes Z_B$ ($X_A \otimes X_B$) basis, respectively. Due to the entropy uncertainty relation [Berta et al. (2010); Maassen et al. (1988)], for any state ρ, we have

$$H(\Delta_{Z_{AB}}(\rho)) + H(\Delta_{X_{AB}}(\rho)) \geq 2 + S(\rho). \tag{6-10}$$

Hence the relative entropy of coherence in the Z basis satisfies [Ma et al. (2017)],

$$C_{Z_{AB}}(\rho) = H(\Delta_{Z_{AB}}(\rho)) - S(\rho) \geq 2 - H(\Delta_{X_{AB}}(\rho)). \tag{6-11}$$

Denoting the rank-2 projective measurement $\{\Pi_x^+, \Pi_x^-\}$ outcomes by Δ_{XX}, one has the key rate in Eq. (6-8),

$$\begin{aligned} K_{BB84}(\rho_{AB}) &= C(\Phi(\rho_{AB})) - H(e_b) \\ &\geq 2 - H(\Delta_{X_{AB}}(\Phi(\rho_{AB}))) - H(e_b) \\ &= 1 - H(\Delta_{XX}(\Phi(\rho_{AB}))) - H(e_b) \\ &= 1 - H(e_p) - H(e_b) \end{aligned} \tag{6-12}$$

where Eq. (6-11) is applied for state $\Phi(\rho_{AB})$ in the second line. The third line holds due to the following reason. For the state $\Phi(\rho_{AB})$ which is the partially dephased state on Π^+ and Π^- subspaces, it satisfies,

$$\begin{aligned} \langle ++|\,\Phi(\rho_{AB})\,|++\rangle = \langle --|\,\Phi(\rho_{AB})\,|--\rangle = \tfrac{1-e_p}{2}, \\ \langle +-|\,\Phi(\rho_{AB})\,|+-\rangle = \langle -+|\,\Phi(\rho_{AB})\,|-+\rangle = \tfrac{e_p}{2}. \end{aligned} \tag{6-13}$$

That is, it has equal probabilities inside each of the rank-2 projectors of X basis, thus $H(\Delta_{X_{AB}}(\Phi(\rho_{AB}))) = 1 + H(\Delta_{XX}(\Phi(\rho_{AB}))) = 1 + H(e_p)$.

Finally, one can see that the Bell diagonal state with probabilities on $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ being $\{(1-e_b)(1-e_p), (1-e_b)e_p, e_b(1-e_p), e_b e_p\}$ reaches the minimal key rate K_{BB84} in the state set $\mathcal{S}$. ■

6.2.2 Six-state protocol

Consider the entanglement-based six-state protocol, where in parameter estimation, Alice and Bob perform the measurement in the X, Y and Z basis respectively. Then, they estimate the error in these three basis $e_x = e_p$, $e_y = \mathrm{Tr}(\Pi_y^- \rho_{AB})$, and $e_z = e_b$. Hence here we have three parameters e_x, e_y and e_z to constrain the state ρ_{AB}.

Suppose that the diagonal terms of ρ_{AB}, when represented in the Bell diagonal basis $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, is $\{p_0, p_1, p_2, p_3\}$ with $p_i \geq 0$ and $\sum_i p_i = 1$. Note that these p_i are directly related to the error rates estimated, i.e.

$$e_x = p_1 + p_3, \tag{6-14}$$

$$e_y = p_1 + p_2, \tag{6-15}$$

$$e_z = p_2 + p_3. \tag{6-16}$$

Then following Theorem 6.1, we have the following corollary.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Corollary 6.2： The key rate of the six-state QKD protocol K_{six} is given by,

$$\begin{aligned} K_{six} &= \min_{\rho_{AB}\in\mathcal{S}} C(\Phi(\rho_{AB})) - H(e_b) \\ &= 1 - H(\{p_i\}), \end{aligned} \tag{6-17}$$

where $\mathcal{S}$ contains all the states yielding the same error rates e_x, e_y and e_z obtained from parameter estimation.

The result is consistent with the one from the previous security proof [Lo (2001)]. Note that the state set $\mathcal{S}$ is more restrained compared to the one in the BB84 protocol. We prove this corollary by first showing that $K(\rho_{AB}) \geq K_{six}$ for all $\rho_{AB} \in \mathcal{S}$, and then giving a specific state in this set to saturate the inequality.

Proof. Considering $\sum_i p_i = 1$, with Eqs. (6-14) to (6-16) $\{p_i\}$ can be estimated by

$$\begin{aligned} p_0 &= \frac{2 - e_x - e_y - e_z}{2}, \\ p_1 &= \frac{e_x + e_y - e_z}{2}, \\ p_2 &= \frac{e_y + e_z - e_x}{2}, \\ p_3 &= \frac{e_z + e_x - e_y}{2}. \end{aligned} \tag{6-18}$$

Applying Eq. (6-8), the key rate is given by

$$\begin{aligned} K_{six}(\rho_{AB}) &= C(\Phi(\rho_{AB})) - H(e_z) \\ &= (1 - e_z)C(\rho_{AB}^{+}) + e_z C(\rho_{AB}^{-}) - H(e_z) \\ &\geq (1 - e_z)\left[1 - H\left(\frac{p_0}{p_0 + p_1}\right)\right] + e_z\left[1 - H\left(\frac{p_2}{p_2 + p_3}\right)\right] - H(e_z) \\ &= 1 - (1 - e_z)H\left(\frac{p_0}{p_0 + p_1}\right) - e_z H\left(\frac{p_2}{p_2 + p_3}\right) - H(e_z) \\ &= 1 - H(\{p_i\}), \end{aligned} \tag{6-19}$$

where in the last line we substitute the relation of e_z in Eq. (6-16). The third line can be derived as follows. For the Z and X bases, two mutually unbiased bases of a qubit, the uncertainty relation for coherence measures is given by [Ma et al. (2017)]

$$C_Z(\rho) = H(\Delta_Z(\rho)) - S(\rho) \geq 1 - H(\Delta_X(\rho)). \tag{6-20}$$

Since ρ_{AB}^{+} is rank-2, it can be viewed as a "qubit" state and the corresponding Z and X bases are $Z' = \{|00\rangle, |11\rangle\}$ and $X' = \{|\Phi^{+}\rangle, |\Phi^{-}\rangle\}$ respectively, where $|\Phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Thus, applying Eq.(6-20) to ρ^{+}_{AB} one has

$$C_{Z'}(\rho^{+}_{AB}) \geq 1 - H(\Delta_{X'}(\rho^{+}_{AB})) = 1 - H\left(\frac{p_0}{p_0 + p_1}\right). \tag{6-21}$$

Similarly,

$$C_{Z''}(\rho^{-}_{AB}) \geq 1 - H(\Delta_{X''}(\rho^{-}_{AB})) = 1 - H\left(\frac{p_2}{p_2 + p_3}\right). \tag{6-22}$$

where Z'' and X'' basis are $\{|01\rangle, |10\rangle\}$ and $\{|\Psi^{+}\rangle, |\Psi^{-}\rangle\}$ respectively, where $|\Psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. Based on Eq. (6-21) and Eq. (6-22), we obtain the inequality in the third line of Eq. (6-19).

Finally, it is not hard to check that the Bell diagonal state with probabilities $\{p_0, p_1, p_2, p_3\}$ reaches the minimal key rate K_{six} in the state set $\mathcal{S}$. ■

6.3 Improve the key rate with the framework

In this section, we show that the above security proof framework allows us to improve the key rates using fine-grained parameters obtained in the measurement outcomes. Essentially, if one can acquire more information about ρ_{AB} in the parameter estimation step, the state set $\mathcal{S}$ in Eq. (6-2) will be constrained more tightly, then the key rate can be improved.

We would like to point out an important fact about Theorem 6.1. In order to estimate the secret key rate generated by an unknown ρ_{AB}, it suffices to gain the information of $\Phi(\rho_{AB})$, rather than the full information of ρ_{AB}. To be more specific, Alice and Bob only need to estimate

$$\Phi(\rho_{AB}) = \begin{pmatrix} m_{00} & 0 & 0 & m_{03} \\ 0 & m_{11} & m_{12} & 0 \\ 0 & m_{21} & m_{22} & 0 \\ m_{30} & 0 & 0 & m_{33} \end{pmatrix}, \tag{6-23}$$

where m_{ij} are the density matrix elements of ρ_{AB} in the Z basis, $\sum_i m_{ii} = 1$, $m_{12} = m^{*}_{21}$ and $m_{03} = m^{*}_{30}$. The form in Eq. (6-23) provides clear clues to improve the key rates. In the following two subsections, we show the refined key rates for BB84 and six-state protocols with the tools from the resource theory of coherence.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

6.3.1 BB84 protocol

In the BB84 protocol, the relations between the error rates e_b, e_p and the matrix elements of ρ_{AB}, as shown in Eq.(6-23), are

$$\begin{aligned} e_b &= m_{11} + m_{22}, && \text{(6-24)} \\ e_p &= 1/2 - \mathrm{Re}[m_{03}] - \mathrm{Re}[m_{12}]. && \text{(6-25)} \end{aligned}$$

In parameter estimation, Alice and Bob carry out Z_A and Z_B measurement, respectively. Thus from the measurement results they can obtain not only the bit error rate e_b, but also the four diagonal elements in the $Z_A \otimes Z_B$ basis, i.e., m_{00}, m_{11}, m_{22}, m_{33}. Hence the bit error rate e_b can be seen as a coarse-grained parameter from the four diagonal elements.

Based on this observation, we give the refined key rate formula for the BB84 protocol. First, let us define the following optimization problem.

Problem 6.1： Minimize $C(\rho(a,b))$ that is subject to $a + b = 1/2 - e_p$, $|a| \leq \sqrt{m_{00}m_{33}}$ and $|b| \leq \sqrt{m_{11}m_{22}}$ with $a, b \in \mathbb{R}$, where C is the relative entropy of coherence, and

$$\rho(a,b) = \begin{pmatrix} m_{00} & 0 & 0 & a \\ 0 & m_{11} & b & 0 \\ 0 & b & m_{22} & 0 \\ a & 0 & 0 & m_{33} \end{pmatrix}. \qquad \text{(6-26)}$$

This optimization problem can be efficiently solved via some numerical methods. In addition, when the diagonal elements satisfy $m_{00}/m_{33} = m_{11}/m_{22}$ (or $m_{00}/m_{33} = m_{22}/m_{11}$), it can be analytically solved, as shown in Lemma D.1 in D.2. We have the following theorem to improve the key rate of the BB84 protocol.

Theorem 6.2： The secret key rate of the BB84 QKD protocol can be estimated via

$$K_{BB84}^{opt} = C(\rho(\bar{a},\bar{b})) - H(e_b) \qquad \text{(6-27)}$$

where $\{\bar{a},\bar{b}\}$ is the solution to Problem 6.1.

Proof. From Eq. (6-8), we need to prove that

$$\begin{aligned} K &= \min_{\rho_{AB} \in \mathcal{S}} C(\Phi(\rho_{AB})) - H(e_b) && \text{(6-28)} \\ &= K_{BB84}^{opt}, \end{aligned}$$

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

where $\mathcal{S}$ contains all the states sharing the same diagonal elements $m_{00}, m_{11}, m_{22}, m_{33}$ and the phase error rate e_p obtained from parameter estimation.

Define σ_{AB} as the state by removing the imaginary parts of the off-diagonal terms in $\Phi(\rho_{AB})$,

$$\sigma_{AB} = \begin{pmatrix} m_{00} & 0 & 0 & \mathrm{Re}[m_{03}] \\ 0 & m_{11} & \mathrm{Re}[m_{12}] & 0 \\ 0 & \mathrm{Re}[m_{21}] & m_{22} & 0 \\ \mathrm{Re}[m_{30}] & 0 & 0 & m_{33} \end{pmatrix}. \tag{6-29}$$

It is not hard to see that $C(\Phi(\rho_{AB})) \geq C(\sigma_{AB})$, due to the fact that the magnitude of the off-diagonal elements is reduced. Specifically, considering a qubit density matrix,

$$\rho = \begin{pmatrix} \beta & |c|e^{i\varphi} \\ |c|e^{-i\varphi} & 1-\beta \end{pmatrix}, \tag{6-30}$$

after applying the incoherent operation $\hat{O}_r(\rho) = \frac{1}{2}U\rho U^\dagger + \frac{1}{2}\rho$ with $U = |0\rangle\langle 0| + e^{2i\varphi}|1\rangle\langle 1|$, one can get,

$$\hat{O}_r(\rho) = \begin{pmatrix} \beta & |c|\cos(\varphi) \\ |c|\cos(\varphi) & 1-\beta \end{pmatrix}, \tag{6-31}$$

where the imaginary part of the off-diagonal terms are removed. As coherence does not increase under incoherent operation, $C(\rho) \geq C(\hat{O}_r(\rho))$ [Baumgratz et al. (2014)].

Since $\Phi(\rho_{AB})$ locates in the two rank-2 subspaces Π_+ and Π_-, similarly, one can get $C(\Phi(\rho_{AB})) \geq C(\sigma_{AB})$ via applying incoherent operations on these two subspaces respectively. As a result, for any state $\rho_{AB} \in \mathcal{S}$,

$$\begin{aligned} K(\rho_{AB}) &= C(\Phi(\rho_{AB})) - H(e_b) \\ &\geq C(\sigma_{AB}) - H(e_b), \\ &\geq \min_{\sigma_{AB} \in \mathcal{S}_\sigma} C(\sigma_{AB}) - H(e_b), \\ &= C(\rho(\bar{a}, \bar{b})) - H(e_b), \end{aligned} \tag{6-32}$$

where $\mathcal{S}_\sigma$ consists of all the corresponding σ_{AB} from $\Phi(\rho_{AB})$, and the last line is on account of the definition of Problem 6.1. Note that σ_{AB} is also a quantum state belonging to the state set $\mathcal{S}$, i.e., $\sigma_{AB} \in \mathcal{S}$, thus the inequality above can be saturated and we get Eq. (6-28). ■

Now we have the following corollary.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Corollary 6.3： For the BB84 QKD protocol, K_{BB84}^{opt} in Eq.(6-27) generally yields a higher secret key rate than the Shor-Preskill one K_{BB84} in Eq. (6-9),

$$K_{BB84}^{opt} \geq K_{BB84}. \tag{6-33}$$

Corollary 6.3 can be directly obtained from Eq. (6-9) and Eq. (6-28). Specifically, since more parameters are utilized to constrain the state ρ_{AB}, the state set $\mathcal{S}$ in Eq. (6-28) is the subset of the one in Eq. (6-9). As a result, one has $K_{BB84}^{opt} \geq K_{BB84}$. The proof of Corollary 6.1 is based on entropy uncertainty relation. Here, we prove Corollary 6.3 with the tools from the coherence theory [Streltsov et al. (2017a)]. In this way, it is clear to see when the inequality in Eq. (6-33) is saturated.

Proof. Define $\hat{O}_{ij}$ as the operation

$$\hat{O}_{ij}(\rho) = \frac{1}{2} S_{ij} \rho S_{ij} + \frac{1}{2}\rho, \tag{6-34}$$

where $S_{ij} = |i\rangle\langle j| + |j\rangle\langle i|$. Then, we consider the state $\sigma'_{AB} = \hat{O}_{12} \circ \hat{O}_{03}(\sigma_{AB})$, where σ_{AB} is defined in Eq.(6-29). Here the labels $\{0, 1, 2, 3\}$ represent the Z basis $\{|00\rangle, |01\rangle\, |10\rangle\, |11\rangle\}$ respectively. And we have σ'_{AB},

$$\sigma'_{AB} = \begin{pmatrix} \frac{1-e_b}{2} & 0 & 0 & \mathrm{Re}[m_{03}] \\ 0 & \frac{e_b}{2} & \mathrm{Re}[m_{12}] & 0 \\ 0 & \mathrm{Re}[m_{21}] & \frac{e_b}{2} & 0 \\ \mathrm{Re}[m_{30}] & 0 & 0 & \frac{1-e_b}{2} \end{pmatrix}, \tag{6-35}$$

where the diagonal elements of the density matrix become equal in two subspaces Π^+ and Π^- respectively after the operation. Clearly, $\hat{O}_{ij}$ is an incoherent operation, thus the coherence of σ'_{AB} is not larger than that of σ_{AB}, i.e.,

$$C(\sigma_{AB}) \geq C(\sigma'_{AB}). \tag{6-36}$$

By definition, one has

$$\begin{aligned} K_{BB84}^{opt} &= \min_{\sigma_{AB} \in \mathcal{S}_\sigma} C(\sigma_{AB}) - H(e_z), \\ &\geq \min_{\sigma_{AB} \in \mathcal{S}'_\sigma} C(\sigma'_{AB}) - H(e_z), \end{aligned} \tag{6-37}$$

where $\mathcal{S}'_\sigma$ contains all the state σ'_{AB} obtained from σ_{AB}, as shown in Eq. (6-35). In fact, the minimization in the second line is a special case of Problem 6.1. By applying lemma

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

D.1 in D.2, one can get the minimal value, $1 - H(e_p) - H(e_b)$. In the end, we have $K_{BB84}^{opt} \geq K_{BB84}$. ■

From Eq. (6-35), it is clear to see that $K_{BB84}^{opt} = K_{BB84}$ when the diagonal elements in the two subspaces Π^+ and Π^- are balanced, i.e. $m_{00} = m_{33}$ and $m_{11} = m_{22}$. In practice, in order to achieve this improvement of the key rate, Alice and Bob need to replace the estimation of e_b with more refined parameters m_{00}, m_{11}, m_{22}, m_{33} in the parameter estimation step, then perform privacy amplification with the updated key rate formula Eq.(6-27). Note that this modification does not require extra quantum or classical communications between Alice and Bob.

6.3.2 Six-state protocol

Similar to the case of BB84 protocol, one can improve the key rate of six-state protocol by utilizing more refined parameters, i.e., diagonal elements m_{00}, m_{11}, m_{22}, m_{33}, instead of the coarse-grained one, e_z. Here, we provide the following theorem.

Theorem 6.3： The secret key rate of six-state QKD protocol can be estimated via

$$K_{six}^{opt} = C(\tau) - H(e_z), \tag{6-38}$$

where

$$\tau = \begin{pmatrix} m_{00} & 0 & 0 & (1 - e_x - e_y)/2 \\ 0 & m_{11} & (e_y - e_x)/2 & 0 \\ 0 & (e_y - e_x)/2 & m_{22} & 0 \\ (1 - e_x - e_y)/2 & 0 & 0 & m_{33} \end{pmatrix}. \tag{6-39}$$

Proof. The proof is similar to that of Theorem 6.2. We need to prove that

$$\begin{aligned} K &= \min_{\rho_{AB} \in \mathcal{S}} C(\Phi(\rho_{AB})) - H(e_b) \qquad (6\text{-}40) \\ &= K_{six}^{opt}, \end{aligned}$$

where $\mathcal{S}$ contains all the states sharing the same diagonal elements m_{00}, m_{11}, m_{22}, m_{33} and the error rates e_x and e_y obtained from parameter estimation. Recall Eq.(6-32),

$$\begin{aligned} K &= \min_{\rho_{AB} \in \mathcal{S}} C(\Phi(\rho_{AB})) - H(e_b) \qquad (6\text{-}41) \\ &\geq \min_{\sigma_{AB} \in \mathcal{S}_\sigma} C(\sigma_{AB}) - H(e_z) \end{aligned}$$

邵钰栗2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

where σ_{AB} is defined in Eq.(6-29). Here, $\mathcal{S}_\sigma = \{\tau\}$ only has one element, since terms in σ_{AB} can all be determined by parameter estimation in the six-state protocol. Namely, one has

$$\begin{aligned} e_x &= 1/2 - \mathrm{Re}[m_{03}] - \mathrm{Re}[m_{12}], && (6\text{-}42)\\ e_y &= 1/2 - \mathrm{Re}[m_{03}] + \mathrm{Re}[m_{12}], && (6\text{-}43)\\ e_z &= m_{11} + m_{22}, && (6\text{-}44) \end{aligned}$$

while m_{00}, m_{11}, m_{22}, m_{33} can be estimated with the $Z_A \otimes Z_B$ measurement. Inserting $\sigma_{AB} = \tau$ into Eq.(6-41) and noting that $\tau \in \mathcal{S}$, we obtain Eq.(6-40). ■

Corollary 6.4： For the six-state QKD protocol, K_{six}^{opt} in Eq.(6-38) generally yields a higher secret key rate than the original one K_{six} in Eq. (6-17),

$$K_{six}^{opt} \geq K_{six} \tag{6-45}$$

Like in the BB84 case, one can obtain Corollary 6.4 directly from Eq. (6-17) and Eq. (6-40). Here we show a proof based on the coherence theory [Streltsov et al. (2017a)].

Proof. Similar to the proof in Corollary 6.3, we apply the incoherent operation $\hat{O}$ on the state τ, and get $\tau' = \hat{O}_{12} \circ \hat{O}_{03}(\tau)$, that is

$$\tau' = \begin{pmatrix} \frac{1-e_z}{2} & 0 & 0 & (1-e_x-e_y)/2 \\ 0 & \frac{e_z}{2} & (e_y-e_x)/2 & 0 \\ 0 & (e_y-e_x)/2 & \frac{e_z}{2} & 0 \\ (1-e_x-e_y)/2 & 0 & 0 & \frac{1-e_z}{2} \end{pmatrix}. \tag{6-46}$$

Due to monotonicity of coherence under incoherent operation, one has

$$\begin{aligned} K_{six}^{opt} &= C(\tau) - H(e_z) \qquad (6\text{-}47)\\ &\geq C(\tau') - H(e_z) \\ &= 1 - H(\{p_i\}) \\ &= K_{six}. \end{aligned}$$

Here, we substitute the probabilities p_i on Bell diagonal basis for the error rates e_x, e_y and e_z with Eqs. (6-14) to (6-16), and calculate the coherence $C(\tau')$. ■

From Eq. (6-46), it is clear to see that $K_{six}^{opt} = K_{six}$ when the diagonal elements in the two subspaces Π^+ and Π^- are balanced, i.e. $m_{00} = m_{33}$ and $m_{11} = m_{22}$. In practice,

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

to achieve this improvement of the key rate, Alice and Bob need to replace the estimation of e_z with the more refined parameters m_{00}, m_{11}, m_{22}, m_{33} in the parameter estimation step, then perform the privacy amplification with updated key rate formula Eq. (6-38). Note that this modification does not require extra quantum or classical communications between Alice and Bob.

Here, we have some remarks regarding the improvement of the key rates. In Sec 6.3.1 and 6.3.2, we have shown that under the coherence-based framework, one can improve the key rates of BB84 and six-state protocol with fine-grained parameters. These key rate improvements can be understood as a fine-grained estimation of coherence in $\Phi(\rho_{AB})$. On the other hand, by utilizing other key rate formulas, such as the Devetak-Winter approach, one may also get similar improvements of the key rates by using fine-grained parameters. See D.5 for more discussions.

6.3.3 Numerical simulation

To illustrate the improvement on the security analysis via the coherence framework, we numerically compare the four key rates analyzed above in Fig. 6.2, i.e., K_{BB84} in Eq. (6-9), K_{BB84}^{opt} in Eq. (6-27), K_{six} in Eq. (6-17) and K_{six}^{opt} in Eq. (6-38). Here we set typical experimental parameters for simulation, and use a parameter α to describe the unbalance of the diagonal elements of ρ_{AB}, i.e. $m_{00}/m_{33} = m_{22}/m_{11} = \frac{\alpha}{1-\alpha}$.

The numerical result shows that the coherence-based key rate of six-state protocol enjoys the highest key rate, while the Shor-Preskill key rate of BB84 possesses the lowest key rate. As $\alpha = 0.5$, that is, there is no unbalance of diagonal elements, $K_{BB84}^{opt} = K_{BB84}$ and $K_{six}^{opt} = K_{six}$; as α departures from 0.5, the unbalance becomes significant and it is clear to see the improvements on the key rates.

We remark that the unbalance of the diagonal elements could happen in practical QKD scenarios. In the next section, one can clearly see that the asymmetry of the detectors can lead to this phenomenon (see ρ_{AB}^{Z} in Eq. (6-57) for an example).

6.4 Practical issue: detection efficiency mismatch

In this section, we apply our coherence framework to QKD security analysis when considering a practical issue — detection efficiency mismatch. Here, we focus on analysing the BB84 protocol. We show that the key rate derived by our framework is generally higher than the previous analyses [Fung et al. (2009)].

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

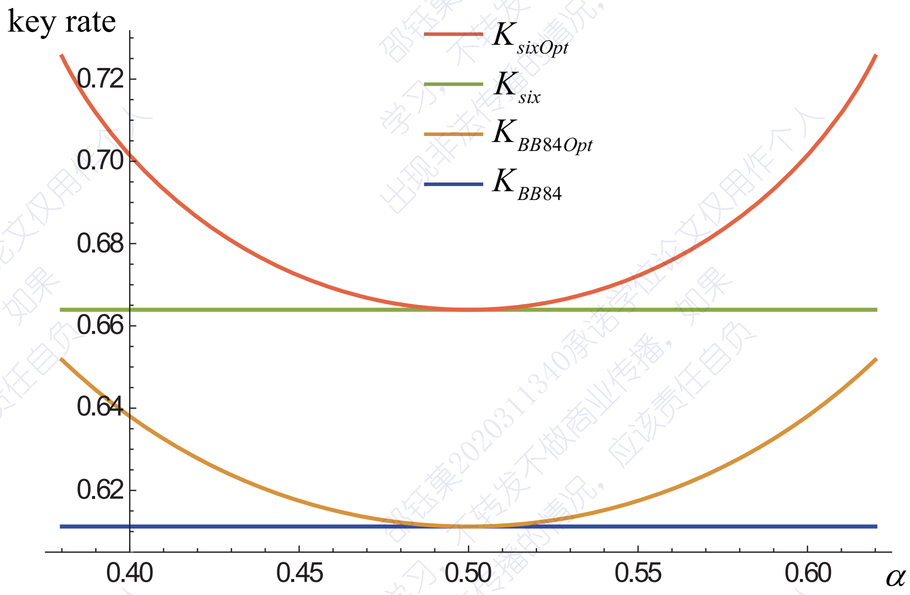


Figure 6.2 Comparison between the key rates. We set $e_x(e_p) = e_y = e_z(e_b) = 3\%$. The parameter α describes the unbalance of the diagonal elements, $m_{00}/m_{33} = m_{22}/m_{11} = \frac{\alpha}{1-\alpha}$. Here $\alpha \in [0.38, 0.62]$ to guarantee the non-negativity of the state ρ_{AB}.

Ideally, the two detectors which detect $|0\rangle$ and $|1\rangle$ in Z basis ($|+\rangle$ and $|-\rangle$ in X basis) respectively are assumed to be identical. However, in practical scenarios, there are always imperfections in the channels and detectors, which may lead to different efficiencies for $|0\rangle$ and $|1\rangle$ (or $|+\rangle$ and $|-\rangle$) [Zhao et al. (2008)].

6.4.1 Detector model

In practice, the detection efficiency of a detector is normally related to other degrees of freedoms of the inputting photons, such as time, space, or spectrum [Fung et al. (2009)]. For example, Fig. 6.3 shows the detection efficiency mismatch that is related to the temporal degree of freedom of the injecting photons. Employing the analytical methods in Ref. [Fung et al. (2009)], here we model the measurement by the two detectors on Bob' side by POVM elements

$$M_0 = \eta_0 \left|0\right\rangle_B \left\langle 0\right|, \tag{6-48}$$

$$M_1 = \eta_1 \left|1\right\rangle_B \left\langle 1\right|, \tag{6-49}$$

where $0 \leq \eta_0, \eta_1 \leq 1$ are the efficiencies of the two detectors. We assume η_0 and η_1 can be calibrated thus are known to Alice and Bob.

Here, we decompose M_0 and M_1 by a filtering operation F_z and an ideal Z-basis

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

measurement, where

$$F_z = \sqrt{\eta_0}\,|0\rangle_B\,\langle 0| + \sqrt{\eta_1}\,|1\rangle_B\,\langle 1|\,. \tag{6-50}$$

Similarly, the measurement in the X basis with the two nonidentical detectors can be decomposed by a filtering operation,

$$F_x = \sqrt{\eta_0}\,|+\rangle_B\,\langle +| + \sqrt{\eta_1}\,|-\rangle_B\,\langle -| \tag{6-51}$$

followed by an ideal X-basis measurement $\{|+\rangle_B\,\langle +|, |-\rangle_B\,\langle -|\}$.

Under this decomposition, before the ideal Z-basis measurement, the state is transformed to

$$\rho_{AB}^{Z} = \frac{F_z \rho_{AB} F_z}{\mathrm{Tr}(F_z \rho_{AB} F_z)}, \tag{6-52}$$

and the obtained bit error rate is represented by

$$e_b = \mathrm{Tr}(\Pi^- \rho_{AB}^{Z}). \tag{6-53}$$

Similarly, for the X-basis measurement, one has

$$\rho_{AB}^{X} = \frac{F_x \rho_{AB} F_x}{\mathrm{Tr}(F_x \rho_{AB} F_x)}, \tag{6-54}$$

and the obtained phase error rate is

$$e_p = \mathrm{Tr}(\Pi_x^- \rho_{AB}^{X}), \tag{6-55}$$

where $\Pi_x^- = |+-\rangle\,\langle +-| + |-+\rangle\,\langle -+|$. We remark that e_p is *not* the phase error corresponding to the state measured in the Z basis. Instead, the later should be

$$e_p' = \mathrm{Tr}(\Pi_x^- \rho_{AB}^{Z}). \tag{6-56}$$

Note that the discrepancy between e_p and e_p' origins from the detection efficiency mismatch of the two detectors.

6.4.2 Derivation of the key rate

Essentially, the task of deriving the final key rate is to estimate e_p' with the knowledge of the measurement results in the Z and X bases.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

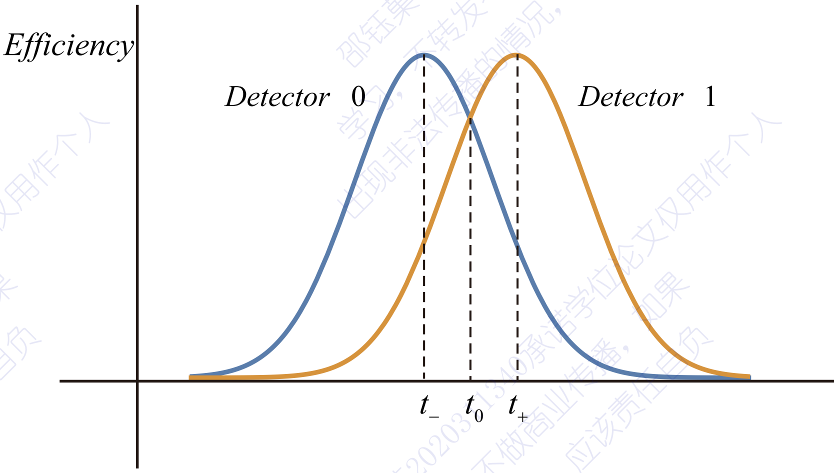


Figure 6.3 Illustration of detector efficiency mismatch in the time domain. Due to optical path difference between the two detectors, the two detectors have different detection efficiency in the time domain. If the arrival time of the signal is t_0, the efficiencies of two detectors are the same. However, if the arrival time is t_- (t_+), the efficiency of Detector 0 is higher (lower).

Let us explicitly write down ρ_{AB}^Z in Eq. (6-52),

$$\rho_{AB}^Z = \frac{1}{\Gamma}\begin{pmatrix} \eta_0 m_{00} & \cdot & \cdot & \sqrt{\eta_0\eta_1} m_{03} \\ \cdot & \eta_1 m_{11} & \sqrt{\eta_0\eta_1} m_{12} & \cdot \\ \cdot & \sqrt{\eta_0\eta_1} m_{21} & \eta_0 m_{22} & \cdot \\ \sqrt{\eta_0\eta_1} m_{30} & \cdot & \cdot & \eta_1 m_{33} \end{pmatrix}, \tag{6-57}$$

where the matrix elements that are not related to the parameter estimation is represented by “·", and the normalization factor is

$$\Gamma = \eta_0 m_{00} + \eta_1 m_{11} + \eta_0 m_{22} + \eta_1 m_{33}. \tag{6-58}$$

Employing Eq. (6-25), one has

$$\begin{aligned} e_p' &= 1/2 - \frac{\sqrt{\eta_0\eta_1}}{\Gamma}\{\mathrm{Re}[m_{03}] + \mathrm{Re}[m_{12}]\}, \\ &= 1/2 - \frac{\sqrt{\eta_0\eta_1}}{\Gamma}(1/2 - e_p''), \end{aligned} \tag{6-59}$$

where the second line applies Eq. (6-25) for e_p'', and e_p'' is defined as

$$e_p'' = \mathrm{Tr}(\Pi_x^- \rho_{AB}). \tag{6-60}$$

Actually, Γ and e_p'' in Eq. (6-59) both can be obtained from measurement results. Denote the probabilities of obtaining $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ when both sides are

邵钰莱2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

measured in the Z basis by $\hat{m}_{00}, \hat{m}_{11}, \hat{m}_{22}$ and $\hat{m}_{33}$, respectively. Then from Eq. (6-57) one has

$$\begin{aligned} \hat{m}_{00} &= \eta_0 m_{00}/\Gamma\,, \quad \hat{m}_{11} = \eta_1 m_{11}/\Gamma\,, \\ \hat{m}_{22} &= \eta_0 m_{22}/\Gamma\,, \quad \hat{m}_{33} = \eta_1 m_{33}/\Gamma\,, \end{aligned} \tag{6-61}$$

Since $m_{00} + m_{11} + m_{22} + m_{33} = 1$, Γ can be represented as

$$\Gamma = \frac{1}{\hat{m}_{00}/\eta_0 + \hat{m}_{11}/\eta_1 + \hat{m}_{22}/\eta_0 + \hat{m}_{33}/\eta_1}. \tag{6-62}$$

Similarly, one can explicitly write down ρ_{AB}^X in Eq. (6-54) in the X basis,

$$\rho_{AB}^X = \frac{1}{\Gamma'} \begin{pmatrix} \eta_0 m'_{00} & \cdot & \cdot & \sqrt{\eta_0\eta_1} m'_{03} \\ \cdot & \eta_1 m'_{11} & \sqrt{\eta_0\eta_1} m'_{12} & \cdot \\ \cdot & \sqrt{\eta_0\eta_1} m'_{21} & \eta_0 m'_{22} & \cdot \\ \sqrt{\eta_0\eta_1} m'_{30} & \cdot & \cdot & \eta_1 m'_{33} \end{pmatrix}, \tag{6-63}$$

where $m'_{i,j}$ denotes the matrix elements of ρ_{AB} in the X basis and the normalization factor is

$$\Gamma' = \eta_0 m'_{00} + \eta_1 m'_{11} + \eta_0 m'_{22} + \eta_0 m'_{22}. \tag{6-64}$$

Denote the probabilities of obtaining $|{+}{+}\rangle$, $|{+}{-}\rangle$, $|{-}{+}\rangle$, and $|{-}{-}\rangle$ when both sides are measured in the X basis by $\hat{m}'_{00}, \hat{m}'_{11}, \hat{m}'_{22}$ and $\hat{m}'_{33}$, respectively. Then one has

$$\begin{aligned} \hat{m}'_{00} &= \eta_0 m'_{00}/\Gamma'\,, \quad \hat{m}'_{11} = \eta_1 m'_{11}/\Gamma'\,, \\ \hat{m}'_{22} &= \eta_0 m'_{22}/\Gamma'\,, \quad \hat{m}'_{33} = \eta_1 m'_{33}/\Gamma'\,, \end{aligned} \tag{6-65}$$

Similar as Γ in Eq. (6-62) for the Z basis, Γ' can be represented as

$$\Gamma' = \frac{1}{\hat{m}'_{00}/\eta_0 + \hat{m}'_{11}/\eta_1 + \hat{m}'_{22}/\eta_0 + \hat{m}'_{33}/\eta_1}. \tag{6-66}$$

By definition in Eq. (6-60), we have

$$\begin{aligned} e''_p &= m'_{11} + m'_{22} \\ &= \Gamma'(\hat{m}'_{11}/\eta_1 + \hat{m}'_{22}/\eta_0). \end{aligned} \tag{6-67}$$

With Eqs. (6-59), (6-62), (6-66) and (6-67), the phase error e'_p can be precisely estimated from the measurement results in Z and X bases. By contrast, e'_p is roughly

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

upper bounded in previous results [Fung et al. (2009)]. This precise estimation of e'_p allows Alice and Bob to obtain a higher key rate than the previous analysis. Also, the key rate can be further improved by applying Theorem 6.2 to ρ^Z_{AB}.

Therefore, with fine-grained parameters, one can expect a higher key rate than the previous ones. This is to be illustrated in the following subsection.

6.4.3 Analytical key rate formula under symmetric attack

To simplify the analysis, we assume Eve's attack to be symmetric between bits 0 and 1 in the Z/X-basis, i.e., the diagonal elements of ρ_{AB} in both the Z basis and the X basis are balanced. That is

$$\begin{aligned} m_{00} &= m_{33} = c, \\ m_{11} &= m_{22} = d, \end{aligned} \tag{6-68}$$

with the normalization condition $2(c+d)=1$. Meanwhile, for the X basis, one has

$$\begin{aligned} m'_{00} &= m'_{33} = c', \\ m'_{11} &= m'_{22} = d', \end{aligned} \tag{6-69}$$

with $2(c'+d')=1$. Then via Eq. (6-58), one has

$$\begin{aligned} \Gamma &= \eta_0 c + \eta_1 d + \eta_0 d + \eta_1 c \\ &= (\eta_0+\eta_1)(c+d) \\ &= (\eta_0+\eta_1)/2, \end{aligned} \tag{6-70}$$

where Γ is a constant related to the detection efficiency.

With Eqs. (6-55), (6-63) and (6-64), one has

$$\begin{aligned} e_p &= (\eta_1 m'_{11} + \eta_0 m'_{22})/\Gamma' \\ &= \frac{\eta_1 m'_{11} + \eta_0 m'_{22}}{\eta_0 m'_{00} + \eta_1 m'_{11} + \eta_0 m'_{10} + \eta_1 m'_{22}} \\ &= \frac{(\eta_0+\eta_1)d'}{(\eta_0+\eta_1)(c'+d')} \\ &= e''_p. \end{aligned} \tag{6-71}$$

where the last line is on account of the definition of e''_p. Inserting Eqs. (6-70) and (6-71)

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

into Eq. (6-59), we have

$$e_p' = 1/2 - \frac{2\sqrt{\eta_0\eta_1}}{\eta_0+\eta_1}(1/2 - e_p), \tag{6-72}$$

which means e_p' can be precisely estimated with e_p.

With Eq. (6-72), one can estimate the key rate by applying Theorem 6.2. For the current scenario that is restricted to the symmetric attack, the optimization Problem 6.1 can be solved analytically. See D.3 for detailed derivation. The key rate is given by

$$K = H(x) - H(f(x, e_p)) - H(e_b), \tag{6-73}$$

where

$$\begin{aligned} x &= \frac{\eta_0}{\eta_0+\eta_1}, \\ f(x, e_p) &= 1/2 + \sqrt{(1/2-x)^2 + x(1-x)(1-2e_p)^2}. \end{aligned}$$

Comparatively, Ref. [Fung et al. (2009)] proposes two methods of analyzing the key rate with the detection efficiency mismatch issue. There, one key rate formula is obtained via the data discarding process,

$$K_1 = \frac{2min\{\eta_0, \eta_1\}}{\eta_0+\eta_1}\Big(1 - H(e_p) - H(e_b)\Big). \tag{6-74}$$

The other key rate is obtained via a virtual protocol based on Koashi's complimentary approach [Koashi (2009)],

$$K_2 = \frac{2min\{\eta_0, \eta_1\}}{\eta_0+\eta_1}\Big(1 - H(e_p)\Big) - H(e_b). \tag{6-75}$$

To compare above key rates, K, K_1 and K_2, we first consider the *noiseless* case, where $e_p = e_b = 0$. Then, one has $K = H(\frac{\eta_0}{\eta_0+\eta_1})$ and $K_1 = K_2 = \frac{2min\{\eta_0,\eta_1\}}{\eta_0+\eta_1}$. It is clear that $K \geq K_1 = K_2$. In the *noisy* case, the key rates obtained from the three analysis are plotted in Fig. 6.4. It shows that K is larger than K_2 for any efficiency mismatch extent; while K is larger than K_1 if the mismatch is not too serious. This manifests the advantage of coherence framework for analysing QKD security.

When the efficiency mismatch becomes large (x approaches 0 in Fig. 6.4), K becomes negative; but K_1 keeps positive and thus larger than K. This fact can be understood as follows. Suppose the initial state before measurement ρ_{AB} possesses positive key rate (bit and phase error are both small). The data discarding approach effectively transforms the

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

state ρ^Z_{AB} to ρ_{AB} with probability $\frac{2min\{\eta_0,\eta_1\}}{\eta_0+\eta_1}$, thus the key rate K_1 is always positive. As $x \to 0$ ($\eta_0 \to 0$), the probability of successful transform approaches 0, thus $K_1 \to 0$. On the other hand, as $x \to 0$, the phase error of the state ρ^Z_{AB} in Eq. (6-72) approaches $1/2$. Consequently, the first two terms in Eq.(6-73) approaches zero, and $K \to -H(e_b) \leq 0$.

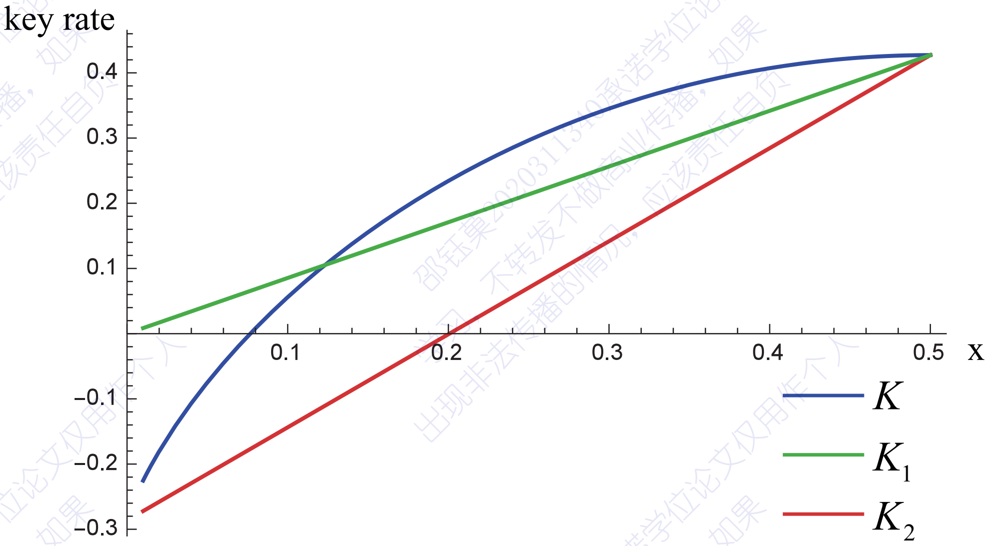


Figure 6.4 Comparison between the key rates obtained from three analyses targeting the detection efficiency mismatch issue. The blue, green and red curves represent K, K_1 and K_2, respectively. We set $e_p = e_b = 5\%$, and plot the key rates versus $x = \frac{\eta_0}{\eta_0+\eta_1}$, which describes the efficiency mismatch. Without loss of generality, we assume $\eta_0 \leq \eta_1$ and hence $0 \leq x \leq 0.5$.

6.5 Relation with entanglement

The existing security analyses [Lo et al. (1999); Shor et al. (2000)] usually starts from entanglement distillation protocols [Bennett et al. (1996a); Horodecki et al. (2009)], where entanglement is taken as an essential resource to deliver the security of the final key. On the contrary, our work is based on the relation between quantum coherence and intrinsic randomness, which is related to the security in QRNG and QKD. Specifically, after correcting the bit errors, we take Alice and Bob as a whole and analyse the intrinsic randomness out of reach of Eve. From this point of view, our approach shares similarity with Koashi's, which is based on the complementary arguments for the joint system [Koashi (2009)]. In addition, recently there are several works considering the interplay between coherence and entanglement [Ma et al. (2016a); Streltsov et al. (2015)]. However, we remark that in these works the authors normally investigate converting subsystem coherence (not the coherence in the bipartite system) into global correlations and the incoherent operations used there cannot be directly applied into the QKD security analysis.

Here, we show some relations between our key rate and the entanglement property of the input state ρ_{AB}. As shown in Eq. (6-8), the key rate can be enhanced if Alice and Bob acquire more information of the shared state ρ_{AB} and estimate the coherence of $\Phi(\rho_{AB})$ more accurately. Suppose Alice and Bob perform a full tomography of ρ_{AB} in the parameter estimation step, then the state set S only contains one state ρ_{AB}. An upper bound for the key rate is shown in the following proposition.

Proposition 6.1： Consider a protocol in which a full tomography on ρ_{AB} is performed in the parameter estimation, then the key rate is upper bounded by

$$K(\rho_{AB}) = C(\Phi(\rho_{AB})) - H(e_b) \leq S(\mathrm{Tr}_A(\Phi(\rho_{AB}))) - S(\Phi(\rho_{AB})). \tag{6-76}$$

Note that the right side of Eq. (6-76) is the hashing inequality for the state $\Phi(\rho_{AB})$, which is a lower bound for one-way LOCC entanglement distillation protocol [Devetak et al. (2005); Horodecki et al. (2009)]. We remark that the projection operation Φ on state ρ_{AB} is a non-local operation, hence our analysis framework based on coherence could potentially yield higher key rate than the usual entanglement distillation analysis. For conciseness, we leave the proof of Proposition 6.1 in D.4. And we also compare our key rate with the Devetak-Winter formula [Devetak et al. (2005)] in D.5.

Now we define a key rate that is independent of measurement basis by maximizing the key rate generated by state ρ_{AB} over all local basis, i.e.,

$$K^m(\rho_{AB}) = \max_{Z_A \otimes Z_B} \Big\{ C(\Phi(\rho_{AB})) - H(e_b) \Big\}, \tag{6-77}$$

where $Z_A \otimes Z_B$ labels all the local basis of Alice and Bob respectively.

One can see that given a pure state $|\Psi_{AB}\rangle$, the maximal key rate is its entanglement entropy, i.e., $K^m(\Psi_{AB}) = S(\rho_A)$, with $\Psi_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}|$ and $\rho_A = \mathrm{Tr}_B(\Psi_{AB})$. To be specific, suppose $|\Psi\rangle_{AB} = a_0 |\psi_0\rangle_A |\psi_0'\rangle_B + a_1 |\psi_1\rangle_A |\psi_1'\rangle_B$ is the the Schmidt decomposition of $|\Psi\rangle_{AB}$, one can choose $\{|\psi_0\rangle_A, |\psi_1\rangle_A\}$ and $\{|\psi_0'\rangle_B, |\psi_1'\rangle_B\}$ as the optimal local basis that maximizes the key rate. In addition, it is clear for a product state $|\Psi_{AB}\rangle = |\psi_0\rangle_A |\psi_0'\rangle_B$, the maximal key rate is zero. And the following proposition gives an upper bound for the maximal key rate for general state.

Proposition 6.2: The maximal key rate of the state ρ_{AB} optimized over all local bases is upper bounded by the entanglement of formation,

$$K^m(\rho_{AB}) \leq \min_{\{p_i,\Psi_i\}} \sum_i p_i K^m(\Psi_i) = E^{form}(\rho_{AB}), \tag{6-78}$$

where the minimization is over all the convex decompositions of $\rho_{AB} = \sum p_i \Psi_i$.

Proof. Note that the key rate K is convex due to the convexity of the relative entropy of coherence and the concavity of the von Neumann entropy. Hence, for any decomposition of $\rho_{AB} = \sum p_i \Psi_i$,

$$K^m(\rho_{AB}) = K(\rho_{AB})_{Z_A^o \otimes Z_B^o} \leq \sum_i p_i K(\Psi_i)_{Z_A^o \otimes Z_B^o} \leq \sum_i p_i K^m(\Psi_i), \tag{6-79}$$

where $Z_A^o \otimes Z_B^o$ represents the optimal local basis for ρ_{AB} and the last inequality holds since one can improve the key rate of Ψ_i further by choosing specific optimal basis for each of them. Consequently, the maximal key rate is upper bounded by the entanglement of formation as shown in Eq. (6-78). ■

And it is also clear to see that the key rate for any separable state $K^m(\rho_{AB}^{sep}) \leq 0$, since they can be written as the combination of product states [Curty et al. (2004)].

6.6 Discussion

In general, the proposed coherence-based framework provides us convenience to analyse the key rate by using tools from resource theory of coherence. Along this direction, a number of problems can be explored in the future. Apart from the currently studied cases, the framework has potential to be applied to many other QKD protocols, such as three state protocol [Boileau et al. (2005); Fung et al. (2006)] and B92 protocol [Bennett (1992)]. There, similar derivation and improvement on the key rate are expected. In particular, the framework can be naturally extended to measurement-device-independent QKD [Lo et al. (2012)], since bipartite quantum states are directly distributed and measured in this kind of protocol. In addition, generalization to high dimensional QKD and continuous-variable QKD [Scarani et al. (2009)] is also interesting. Also, we expect our framework to be useful in addressing more practical issues in QKD, the solutions to many of which are missing or very complicated at the moment.

Moreover, we should remark that it is intriguing to reexamine the previous QKD security analyses from the coherence theory point of view. To be specific, a common

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

technique of security analysis is to transform the original protocol to equivalent virtual protocols, which are easier to analyse but share same amount of secure keys. In the virtual protocol, the operations conducted there are incoherent operations [Streltsov et al. (2017a)] (more specifically, dephasing-covariant incoherent operation [Chitambar et al. (2016b); Marvian et al. (2016a)]), which commute with the final Z-basis measurement to generate key. In addition, it is also interesting to investigate the connection between coherence and entanglement [Coles (2012); Ma et al. (2016a); Streltsov et al. (2015, 2017b); Yao et al. (2015)] under the scenario of security analysis, which not only deepens our understanding of these basic quantum resources, but also inspires useful applications in quantum information processing.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Chapter 7 Interaction-free measurement as quantum channel discrimination

Quantum measurement is a fundamental concept in the quantum theory. The measurement process extracts the information stored in the quantum system to the classical world, where the quantum state is required to change adaptively based on the measurement outcome. In fact, the measurement on the target system, say A, is accomplished indirectly by coupling it to another system B and implementing measurement on that system alternatively. However, even the nonobservance of a particular result of B would modify the wave function of A, which is called the "negative result measurement" [Dicke (1981); Renninger (1960)].

Following these former works, Elitzur and Vaidman introduced a "counterfactual" protocol dubbed interaction-free measurement (IFM) [Elitzur et al. (1993)]. In this IFM protocol, a photon is sent to a standard Mach-Zehnder interferometer to detect an opaque object, where the maximum efficiency for a successful detection without photon absorption is 50% [Elitzur et al. (1993); Kwiat et al. (1995)]. However, by a modification on account of the quantum Zeno effect [Misra et al. (1977)], the efficiency can approach 100% as the interrogation cycle goes to infinity [Kwiat et al. (1995, 1999)] (see Fig. 7.1 for detailed discussions. It is clear that this kind of "counterfactual" detection arises from the coherence of the incident photon in the superposition between the two arms of the interferometer.

Interaction-free measurement has been used to detect fragile objects, like single atom [Karlsson et al. (1998); Volz et al. (2011)] or photon-sensitive substances [Inoue et al. (2000)]. And the application to electron microscopy is also developed [Kruit et al. (2016); Putnam et al. (2009); Thomas et al. (2014)], which should facilitate the biological molecules imaging. Besides the original optical setup [Kwiat et al. (1995, 1999)], there are many other different schemes proposed [Chirolli et al. (2010); Paraoanu (2006); Putnam et al. (2009); Zilberberg et al. (2016)], or realized [Hafner et al. (1997); Ma et al. (2014); Tsegaye et al. (1998)] to achieve "quantum-Zeno-like" IFM. However, the physical model behind them is essentially the same; they all involve utilizing the quantum Zeno effect to keep the photon state unchanged, in the presence of an object.

In this chapter, with the help of quantum channel theory, we build the general model

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

of quantum-Zeno-like IFM, where the object to be detected is semitransparent and the number of interrogation cycle is finite. Two important probabilities named P_{loss} and P_{error} are proposed to describe the photon loss rate and the error of discrimination in the IFM process. In order to find the minimums of the P_{loss} and P_{error} and the corresponding initial photon input states to reach them, we simplify the iteration of the quantum channels to transfer matrices operating on pure state. With this compact simplification, the minimum properties of P_{loss} and P_{error} can be systemically studied. In addition, it shows that the entangled photon input state can not enhance the performance of IFM, considering P_{loss} and P_{error} respectively.. To be specific, we focus on two main quantities to benchmark the performance of IFM, namely (i) the loss probability P_{loss} and (ii) the error probability P_{error}, which respectively describe the photon loss rate and the minimum error of discriminating the object. Specifically, the minimum values of these two probabilities are investigated analytically, for any given values of the object transparency a^2 and the interrogation number N.

This chapter is organized as follows. In section 7.1, we introduce the background of IFM. In Section 7.2, we construct a general model with the use of quantum channel. In Section 7.3, we simplify the quantum channels for pure input state. In Section 7.4, 7.5, we study the cases of opaque object and semitransparent object respectively. Discussion is contained in Section 7.6. The content of this chapter is from the work [Zhou et al. (2017a)].

7.1 Interaction-free measurement

Here we consider an optical setup [Kwiat et al. (1999)] to illustrate the principle of IFM, as showed in Fig. 7.1. Let us denote respectively the state $|1\rangle$, $|2\rangle$, and $|3\rangle$ as the representation for,

$$\text{up} \Leftrightarrow |1\rangle, \quad \text{down} \Leftrightarrow |2\rangle, \quad \text{loss} \Leftrightarrow |3\rangle \tag{7-1}$$

state of the incident photon. A light-absorbing object (e.g. a photon-sensitive bomb in [Elitzur et al. (1993)]) is placed in the path of the down state photon. And the probability for this object to appear is denoted by $\Pr(\text{here}) = q$.

In fact, in order to describe the incident photon state transformation when the object is present explicitly, we mimic the effect of this object with a mirror, followed by a photon detector [Kwiat et al. (1995)] (see Fig. 7.1 for detailed illustration). Let us consider the

邵钰栗2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

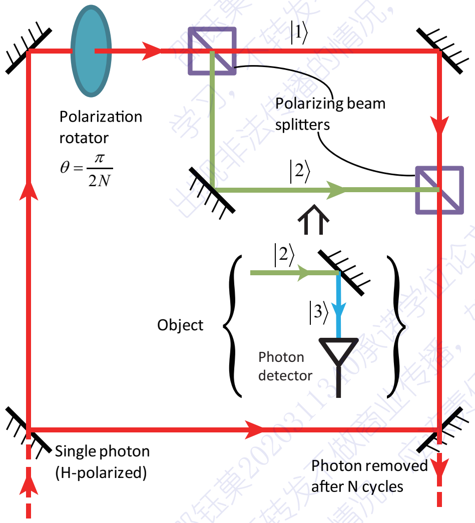

$|1\rangle$
Polarizing beam splitters
Polarization rotator
$\theta = \frac{\pi}{2N}$
$|2\rangle$
$|2\rangle$
$|3\rangle$
Object
Photon detector
Single photon (H-polarized)
Photon removed after N cycles

Figure 7.1 The “quantum-Zeno-like" IFM setup. We illustrate the principle of IFM using the optical scheme in ref [Kwiat et al. (1999)]. The polarization rotator can rotate the photon polarization by $\theta = \frac{\pi}{2N}$ in each cycle. And the polarizing beam splitter can separate the photon to up or down path if the photon is horizontal polarized H or vertical polarized V. So the polarizations of the photon label the up state $|1\rangle$ and the down state $|2\rangle$ in $Eq.(7-1)$ respectively. In addition, the object is mimicked by a mirror followed by a photon detector. The mirror can transform the down state $|2\rangle$ to the loss state $|3\rangle$. And the photon detector implements the projective measurement on the two $\{|1\rangle, |2\rangle\}$ and $\{|3\rangle\}$ subspaces. After N interrogation cycles, we can judge whether there is an object in the down path with the final polarization state of the photon, without any photon absorption.

essential idea of interaction-free measurement: first, an incident photon is prepared in the up path, with a quantum state labeled by $|1\rangle$. Then, the incident photon is rotated by an angle θ through a beamsplitter,

$$R_\theta |1\rangle = \cos\theta |1\rangle + \sin\theta |2\rangle, \tag{7-2}$$

where $\theta = \pi/2N$. Here N will be identified as the total number of interrogation cycle.

Presence of the object: If there exists an object along the down path, the photon in the down state $|2\rangle$ will be totally transferred to the loss state $|3\rangle$ by the mirror, i.e.,

$$U_\mathrm{I} |2\rangle = |3\rangle, \tag{7-3}$$

where the subscript of U_I stands for interaction. Furthermore, when applying it to a quantum superposition, we have

$$U_\mathrm{I}(\cos\theta |1\rangle + \sin\theta |2\rangle) = \cos\theta |1\rangle + \sin\theta |3\rangle. \tag{7-4}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Then followed by the projective measurement M by the photon detector,

$$\begin{aligned} P_0 &= |1\rangle\langle 1| + |2\rangle\langle 2|, \\ P_1 &= |3\rangle\langle 3|, \end{aligned} \tag{7-5}$$

the final state in Eq. (7-4) becomes a mixed state,

$$\cos^2\theta\,|1\rangle\langle 1| + \sin^2\theta\,|3\rangle\langle 3|, \tag{7-6}$$

where the probability of the photon traveling along up path without absorption is given by $\Pr(|1\rangle) = \cos^2\theta$. And the probability of which the photon is transformed to the loss state $|3\rangle$ and absorbed by the detector is $\Pr(|3\rangle) = \sin^2\theta$.

In the probability subspace of P_1, the loss state photon will not participate in the following interrogation cycle, i.e., the IFM process halts in this case. Consequently, the probability of finding $|1\rangle$ after N cycles equals to $\Pr(|1\rangle) = \cos^{2N}(\theta)$. When N approaches infinity, we have

$$\lim_{N\to\infty}\cos^{2N}(\theta) = 1. \tag{7-7}$$

Therefore, one can find the final state to be $|1\rangle$ with probability 1 without any photon loss, in the presence of an object.

Absence of object: If there is no object, i.e., the down state $|2\rangle$ will travel straight through without getting absorbed (or reflected by the mirror); the rotation R_θ is directly applied N times. Thus, the input photon state $|1\rangle$ can be rotated to $|2\rangle$ at the end, that is,

$$(R_\theta)^N\,|1\rangle = R_{N\theta}\,|1\rangle = |2\rangle\,. \tag{7-8}$$

In summary, after N cycles, if we get $|1\rangle$, it implies the existence of the object, while $|2\rangle$ implies the absence; we can therefore unambiguously detect the presence of an object (because state $|1\rangle$ and $|2\rangle$ are orthogonal), without any photon absorption by the object. This is the essential idea of the interaction-free measurement, based on the physics of quantum Zeno effect.

7.1.1 Finite rounds and imperfect absorption

In practice, there are two problems one should consider, in implementing the interaction-free measurement. First, the number of interrogation cycle N has to be finite; it is also impossible to make the rotation angle arbitrarily small.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Second, the absorption of photon by object may not be perfect, as assumed in Eq. (7-3). In general, we should consider the absorption probability to be less than unity, i.e.,

$$U_{\mathrm{I}}\left|2\right\rangle = a\left|2\right\rangle + \sqrt{1-a^2}\left|3\right\rangle, \tag{7-9}$$

where a^2 characterizes the transparency of the object. Here a is assumed to be an non-negative real number for simplicity.

In this scenario, we can substitute a beam splitter, whose transparency is a^2, for the mirror in Fig. 7.1 to mimic the corresponding semitransparent object. This treatment is similar to [García-Escartín et al. (2005)], and other works [Mitchison et al. (2001); Thomas et al. (2014)] gave different but equivalent treatments.

7.1.2 Related works

Previous work has shown that the successful rate of IFM decreases if the object is semitransparent, compared with the opaque case [García-Escartín et al. (2005); Jang (1999); Vaidman (2003)]. The performance can be improved by increasing the interrogation cycle number N and the object can also be detected perfectly without any photon absorption when $N \to \infty$ [Azuma (2006); Kwiat (1998)].

In the literature [Azuma (2006); García-Escartín et al. (2005); Jang (1999); Kwiat (1998)], the initial input state is usually taken as a pure state, namely $\left|1\right\rangle$. In the presence of an object, the successful probability

$$P_{\text{success}} = \left|\left\langle 1\right|\hat{O}_{\mathrm{IFM}}\left|1\right\rangle\right|^2, \tag{7-10}$$

is used to characterize the performance of the IFM process. Here $\hat{O}_{IFM}$ is a linear operator, but not necessarily unitary due to the possibility of photon loss. The value of P_{suc} specifies the probability that one can receive a $\left|1\right\rangle$ photon after sending a $\left|1\right\rangle$ photon at the beginning, in the presence of an object. In this case, one can confirm the presence of an object without photon being absorbed.

To the best of our knowledge, there is no work aiming to optimize the IFM process through a search of optimal input states of the photon. In particular, the possibility of using quantum correlation to enhance the ability of channel discrimination have been achieved in the context of quantum illumination [Lloyd (2008)], and here we also study the possibility of this kind of enhancement in IFM process.

7.1.3 Main results

Our main results are summarized as follows:

For unentangled input states:

- There exists a unique quantum state $|\varphi_0\rangle$ minimizing P_{loss}, for any finite N, which approaches 0 asymptotically as $N \to \infty$.
- There are two states $|\varphi_\pm\rangle$ that leads to $P_{\text{error}} = 0$, i.e. perfect discrimination, as long as the following inequality is fulfilled,

$$\frac{1+a}{1-a}\ \sin(\frac{\pi}{2N}) \leq 1. \tag{7-11}$$

- The photon loss rate of $|\varphi_+\rangle$ is smaller than that of $|\varphi_-\rangle$, i.e., $(P_{\text{loss}})_{|\varphi_+\rangle} < (P_{\text{loss}})_{|\varphi_-\rangle}$, which means $|\varphi_+\rangle$ is better than $|\varphi_-\rangle$ in term of P_{loss}.
- For $N \to \infty$, both $|\varphi_0\rangle$ and $|\varphi_+\rangle$ approach the same state $|1\rangle$, where both $(P_{\text{loss}})_{|\varphi_0\rangle}$, $(P_{\text{loss}})_{|\varphi_+\rangle}$ share similar asymptotic behavior $O(1/N)$.
  $(P_{\text{loss}})_{|\varphi_0\rangle} \sim O(1/N)$

In addition, we studied how quantum correlation of input states can facilitate the IFM process by utilizing entangled photons in the setting of quantum illumination [Lloyd (2008)]: send one photon in an entangled pair to the IFM cycle but keep the other photon. At the end, a joint POVM measurement is performed on both photons. We found that

For entangled input states:

- The optimal state to reach the minimal P_{loss} is the product state $|\varphi_0\rangle\,|\phi_0\rangle$, where $|\phi_0\rangle$ is any state of the second photon.
- The two solutions $|\varphi_\pm\rangle$ expand to a family of quantum states in the larger Hilbert space. Specifically, all members of the form,

$$\alpha\,|\varphi_+\rangle\,|\phi_1\rangle + \beta\,|\varphi_-\rangle\,|\phi_1^\perp\rangle, \tag{7-12}$$

  can be employed to achieve $P_{\text{error}} = 0$, where $|\phi_1\rangle, |\phi_1^\perp\rangle$ are any two orthogonal states of the second photon. However, the one with the minimal P_{loss} in this family of states is the unentangled state $|\varphi_+\rangle\,|\phi_1\rangle$.

In other words, entangled photons cannot minimize P_{loss}, or P_{error} better than the case with unentangled photons. Therefore, we conclude that entanglement cannot improve the IFM process.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

7.2 The general model

In this section, we present a general model of interaction-free measurement, taking into account of a semitransparent object and a finite number of interrogation cycle. In addition, we shall consider sending entangled photons as the input state as well.

First of all, the IFM process can be described as a quantum channel, which is sequentially-applied N times on the input photon state, depending on the presence/absence of the object. Thus, detecting the object is equivalent to a channel discrimination problem.

In both cases, a unitary rotation operator (see Eq. (7-2))

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{7-13}$$

is applied for each step at first, where the matrix is wriiten in the $|1\rangle$, $|2\rangle$ and $|3\rangle$ basis. It can be regarded as the following channel,

$$\mathcal{E}_\theta(\rho) = R_\theta\, \rho\, R_\theta^\dagger, \tag{7-14}$$

where ρ is the density matrix of the input state.

If a generic semitransparent object is present, the partial absorption effect can be represented by an effective quantum channel $\mathcal{E}_I$ (I is short for interaction) on the photon state (see Appendix. E.1 for detailed derivation):

$$\mathcal{E}_I(\rho) = \sum_{i=0,1} A_i \rho A_i^\dagger, \tag{7-15}$$

$$\begin{aligned} A_0 &= |1\rangle\langle 1| + a|2\rangle\langle 2| + |3\rangle\langle 3|, \\ A_1 &= \sqrt{1-a^2}|3\rangle\langle 2|, \end{aligned} \tag{7-16}$$

where A_0 and A_1 are the Kraus operators fulfilling $\sum_{i=0,1} A_i^\dagger A_i = I$. A_0 describes the process that the down state $|2\rangle$ component partially decays to the loss state $|3\rangle$ component; A_1 is for the increase of the population on loss state, which indicates the photon loss probability.

It is necessary to clarify that $\mathcal{E}_I$ is not just a mere combination of the unitary U_I and the projective measurement M, since the population on loss state $|3\rangle$ component will be absorbed by the detector and not participate in the following cycle, indicating that the photon loss is an irreversible process.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

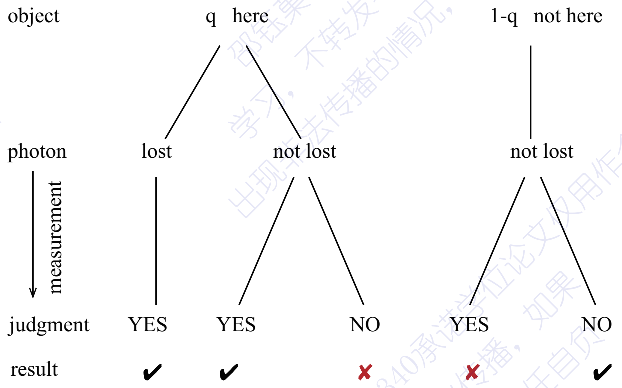


Figure 7.2 Illustration for the error happening in IFM. At the end of IFM, we implement POVM on the final output photon state, and we will make error when giving the judgment NO (YES) in the presence (absence) of the object. The final line shows the result (right or wrong) of the judgment. And we can find that if the photon is lost, one can definitely confirm the presence of the object since the photon should not be lost in the absence of the object. Hence we can give the right judgment YES and make no error in this case.

Then the channels that describe the whole interrogation can be written down by cycling the above channels for N times as below

$$\rho' = [\mathcal{E}_{\mathrm{I}}\, \mathcal{E}_{\theta}]^{N}(\rho) = \mathcal{E}'(\rho), \tag{7-17}$$

$$\rho'' = [\mathcal{E}_{\theta}]^{N}(\rho) = \mathcal{E}''(\rho), \tag{7-18}$$

where ρ' is the output density matrix, if the object is present; ρ'' is the output density matrix for the object absence case. The corresponding overall quantum channels are denoted by $\mathcal{E}'$ and $\mathcal{E}''$ respectively.

Our main concerns in IFM are two probabilities: one is the photon loss probability P_{loss}, which describes the damage to the object. This concern is important if the detected object is fragile, like electronic devices or biological matters. In fact, it is just the population accumulating on the loss state $|3\rangle$ component after the full IFM process,

$$P_{\mathrm{loss}} = q\, \langle 3|\mathcal{E}'(\rho)|3\rangle, \tag{7-19}$$

where q is the probability for the presence of the object.

The other is the probability for making a error in the detection. Given the object existing probability Pr(here), the error happens when one give the wrong judgement after

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

the interrogation cycles (see Fig. 7.2), that is,

$$P_{\text{error}} = \Pr(\text{here})\,\Pr(\text{NO}|\text{here}) + \Pr(\text{not here})\,\Pr(\text{YES}|\text{not here}), \tag{7-20}$$

where one gives the judgment NO in the presence of the object or YES in the absence of the object.

To be specific, one sends a input photon state ρ, and receives the output photon state $\mathcal{E}'(\rho)/\mathcal{E}''(\rho)$ depending on the presence/absence of the object. Then one makes the judgment by implementing a two-value POVM measurement $\{\Pi_1, \Pi_2\}$ on the final output photon. Here Π_1, Π_2 are positive operators fulfilling $\Pi_1 + \Pi_2 = I$. Specifically, if obtaining the measurement result 1(2), one makes the judgment that the object is here(not here). Hence, the corresponding conditional probabilities in the above equation become $\Pr(\text{NO}|\text{here}) = \text{Tr}[\Pi_2\mathcal{E}'(\rho)]$ and $\Pr(\text{YES}|\text{not here}) = \text{Tr}[\Pi_1\mathcal{E}''(\rho)]$. And substitute them into Eq. (7-21), we get

$$P_{\text{error}} = q\text{Tr}[\Pi_2\mathcal{E}'(\rho)] + (1-q)\text{Tr}[\Pi_1\mathcal{E}''(\rho)]. \tag{7-21}$$

where the definition Pr(here) = q is used.

Following the minimum-error scheme [Helstrom (1976); Herzog (2004)] in quantum state discrimination, by choosing a proper POVM measurement, the reachable minimal error shows the following form,

$$P_{\text{error}} = \frac{1}{2}[1 - \|q\mathcal{E}'(\rho) - (1-q)\mathcal{E}''(\rho)\|], \tag{7-22}$$

where $||O|| = Tr(\sqrt{O^{\dagger}O})$ denotes the trace norm of any operator O. It indicates that the lager the trace norm distance between the two output state $\mathcal{E}'(\rho)/\mathcal{E}''(\rho)$ normalized by the corresponding probabilities $q/1-q$, the smaller the error is.

One may argue that in each cycle the photon detector may click (bomb exploding in [Elitzur et al. (1993)]), then the presence of the object can be confirmed at the middle of the whole process, thus it is not necessary to finish the following interrogation and discriminate the state at the end. However, in fact, they are equivalent; as will be showed explicitly in Eq. (7-33), the loss probability of every cycle that accumulates on the loss state $|3\rangle$ component can be excluded from the P_{error}, just because we can always make no error and confirm there is an object if the photon is lost (see Fig. 7.2).

The main focus of our IFM study is to find the minimums of these two probabilities P_{loss} and P_{error}, and the initial input photon states to reach them. Fortunately, with the

邵钰莱2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

following theorem, we can reduce the range of the input state from any density matrix ρ, say mixed or pure, to just pure state $|\varphi\rangle$ in the Hilbert space of the photon.

Theorem 7.1： The minimums of the loss probability P_{loss} and the error probability P_{error} can be both reached by the pure state.

Proof. Due to the linearity of the quantum channel, we have

$$\begin{aligned} P_{\text{loss}} &= q\langle 3|\mathcal{E}'(\rho)|3\rangle, \\ &= q\langle 3|\mathcal{E}'(\sum_i p_i\varphi_i)|3\rangle, \\ &= q\langle 3|\sum_i p_i\mathcal{E}'(\varphi_i)|3\rangle, \\ &= \sum_i p_i q\langle 3|\mathcal{E}'(\varphi_i)|3\rangle, \\ &= \sum_i p_i P^i_{\text{loss}}, \end{aligned} \tag{7-23}$$

where φ_i represents the density matrix of the pure state $|\varphi_i\rangle$, P^i_{loss} is the corresponding loss probability for it, and $\sum_i p_i\varphi_i$ is any convex decomposition of the input state ρ.

Eq. (7-23) shows that the loss probability P_{loss} of the mixed state ρ equals to the weighted average of P^i_{loss} of the corresponding pure state. Thus there is at least one pure state φ_i whose loss probability $P^i_{\text{loss}} \le P_{\text{loss}}$.

Moreover, combining the convex property of the trace norm, we also have

$$\begin{aligned} P_{\text{error}} &= \frac{1}{2}[1 - \|q\mathcal{E}'(\rho) - (1-q)\mathcal{E}''(\rho)\|], \\ &= \frac{1}{2}[1 - \|q\mathcal{E}'(\sum_i p_i\varphi_i) - (1-q)\mathcal{E}''(\sum_i p_i\varphi_i)\|], \\ &= \frac{1}{2}\{1 - \|\sum_i p_i[q\mathcal{E}'(\varphi_i) - (1-q)\mathcal{E}''(\varphi_i)]\|\}, \\ &\ge \sum_i p_i\{\frac{1}{2}[1 - \|q\mathcal{E}'(\varphi_i) - (1-q)\mathcal{E}''(\varphi_i)\|]\}, \\ &= \sum_i p_i P^i_{\text{error}}. \end{aligned} \tag{7-24}$$

Still one can always find the specific pure state in the decomposition, whose $P^i_{\text{error}} \le P_{\text{error}}$. As a consequence, we can study the minimums of the two important probabilities just investigating the pure state in the Hilbert space. ■

Quantum correlations [Modi et al. (2012)] like entanglement, discord are essential resources for quantum communication and computation [Nielsen et al. (2010)], and also

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

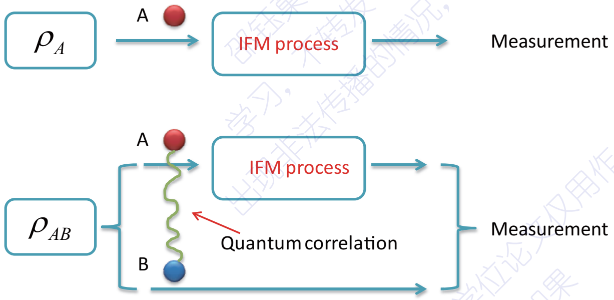


Figure 7.3 The single photon and entangled photon input IFM

for quantum metrology [Braunstein et al. (1996); Giovannetti et al. (2006)]. The efficiency of many tasks can be enhanced utilizing quantum correlation resources, e.g. quantum illumination [Lloyd (2008)] etc. So here we also want to study the effect of quantum correlation to IFM and investigate whether quantum correlation can enhance the performance of IFM or not.

The new setup (Fig. 7.3), employing bipartite photon input state, is like this: The task of the photon A is still to detect the object as in traditional IFM (Fig. 7.1) and the photon B remains unchanged in the whole process. However, there may be some quantum correlations between photon A and photon B. Because quantum channels on photon A are also quantum channels on combined system A and B, Th. 7.1 can also be applied to this input case and we just need to consider the pure state in this bipartite scenario. That is to say, the quantum correlation between photon A and B is just entanglement. Therefore this input case is dubbed as the entangled photon input IFM.

Further more, we will give another theorem below, which describes the relation between the single photon input case and the bipartite photon input case about the two important probabilities P_{loss} and P_{error}.

Theorem 7.2： Generally, bipartite photon input case is the same as single photon input case considering P_{loss}, but not worse than single photon input case considering P_{error}, that is,

$$P_{\text{loss}}(\rho_{AB}) = P_{\text{loss}}(\rho_A) \tag{7-25}$$

$$P_{\text{error}}(\rho_{AB}) \leq P_{\text{error}}(\rho_A) \tag{7-26}$$

where ρ_{AB} is the bipartite input state and $\rho_A = Tr_B(\rho_{AB})$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Proof. For P_{loss}, by the definition in Eq. (7-19), Eq. (7-25) shows

$$\langle 3|Tr_B[\mathcal{E}'(\rho_{AB})]|3\rangle = \langle 3|\mathcal{E}'(\rho_A)|3\rangle, \tag{7-27}$$

which is right since partial trace operation on system B and the quantum channel on system A commute with each other. It means that any bipartite input state ρ_{AB} behaves the same as its corresponding marginal state ρ_A considering P_{loss}.

For P_{error}, using the definition in Eq. (7-22), Eq. (7-26) is equivalent to

$$\|q\mathcal{E}'(\rho_{AB}) - (1-q)\mathcal{E}''(\rho_{AB})\| \geq \|q\mathcal{E}'(\rho_A) - (1-q)\mathcal{E}''(\rho_A)\|. \tag{7-28}$$

It is also right because partial trace operation on B is certainly a trace-preserving operation that is contractive under the measure of trace distance (see [Nielsen et al. (2010)] and Appendix. E.2), i.e.,

$$\begin{aligned}
&\|q\mathcal{E}'(\rho_{AB}) - (1-q)\mathcal{E}(\rho_{AB})\| \\
&\geq \|qTr_B[\mathcal{E}'(\rho_{AB})] - (1-q)Tr_B[\mathcal{E}(\rho_{AB})]\| \\
&= \|q\mathcal{E}'(\rho_A) - (1-q)\mathcal{E}(\rho_A)\|
\end{aligned}$$

where the last line is due to partial trace on system B commuting with the quantum channel on system A. ■

7.3 Simplify the quantum channel for pure state

Owing to $Th.$ 7.1, we just need to focus on the pure input state scenario and the quantum channels defined in $Sec.$ 7.2 can be simplified when the input state is pure.

First, the input photon state is set as the general form $|\varphi\rangle = \alpha|1\rangle + \beta|2\rangle$. Then, for the presence of the object scenario, since the IFM process halts in the probability subspace where the photon decays to the loss state $|3\rangle$, we just need to monitor the probability subspace where the photon is not absorbed; and the corresponding unnormalized state (due to absorption process) is denoted as $|\varphi'\rangle$. Therefore the final photon state with the object existing is the combination of $|\varphi'\rangle\langle\varphi'|$ (not absorbed part) and $(1-\langle\varphi'|\varphi'\rangle)|3\rangle\langle 3|$ (absorbed part), i.e.,

$$\rho' = |\varphi'\rangle\langle\varphi'| + (1-\langle\varphi'|\varphi'\rangle)|3\rangle\langle 3|\,. \tag{7-29}$$

And for the absence of the object scenario, the final output photon state is denoted by $|\varphi''\rangle$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Then the quantum channels can be replaced by the corresponding transforming matrices for pure state in the $|1\rangle, |2\rangle$ basis as

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right]^N |\varphi\rangle = |\varphi'\rangle, \tag{7-30}$$

$$\left[\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right]^N |\varphi\rangle = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}|\varphi\rangle = |\varphi''\rangle. \tag{7-31}$$

Here, Eqs. (7-30), (7-31) give the relations between $|\varphi\rangle = \alpha|1\rangle + \beta|2\rangle$ and $|\varphi'\rangle$, $|\varphi''\rangle$. Eq. (7-31) is just the unitary transformation generated by the rotation operation R_θ (Eq. (7-13)) on the photon state in each cycle and we obtain the final state by iterating it for N times. *Eq*. (7-30) is not a unitary, describing the decaying of photon to the loss state due to absorption. The state first undergoes the rotation operation, and then the matrix accounting for decay generated by the Kraus operator A_0 in Eq. (7-16) operates on it; and the final photon state is also obtained by iterating this process. Actually, $\langle\varphi'|\varphi'\rangle$ is just the conditional probability that the photon is not absorbed conditioning on the object present.

Then P_{loss} and P_{error} can be written in the new form for pure input state as

$$\begin{aligned} P_{\text{loss}} &= q\,\langle 3|\rho'|3\rangle, \\ &= q\,\langle 3||\varphi'\rangle\langle\varphi'| + (1-\langle\varphi'|\varphi'\rangle)|3\rangle\langle 3||3\rangle, \\ &= q\,(1-\langle\varphi'|\varphi'\rangle), \end{aligned} \tag{7-32}$$

where the last equality is due to the state $|\varphi'\rangle$ living on the subspace expanded by $|1\rangle, |2\rangle$ basis and having no component on $|3\rangle$.

$$\begin{aligned} P_{\text{error}} &= \frac{1}{2}\{1 - \|q\rho' - (1-q)|\varphi''\rangle\langle\varphi''|\|\}, \\ &= \frac{1}{2}\{1 - \|q[|\varphi'\rangle\langle\varphi'| + (1-\langle\varphi'|\varphi'\rangle)|3\rangle\langle 3|] - (1-q)|\varphi''\rangle\langle\varphi''|\|\}, \\ &= \frac{1}{2}\{1 - \|q|\varphi'\rangle\langle\varphi'| + P_{\text{loss}}|3\rangle\langle 3|] - (1-q)|\varphi''\rangle\langle\varphi''|\|\}, \\ &= \frac{1}{2}\{1 - P_{\text{loss}} - \|q|\varphi'\rangle\langle\varphi'| - (1-q)|\varphi''\rangle\langle\varphi''|\|\}. \end{aligned} \tag{7-33}$$

Here the definition of P_{loss} in Eq. (7-32) is employed in the third line; and in the last line, $P_{\text{loss}}|3\rangle\langle 3|$ term is extracted from the trace norm since $|\varphi'\rangle, |\varphi''\rangle$ are both in the space spanned by $|1\rangle, |2\rangle$. To be specific, it describes the fact that we will make no error and can always confirm there is an object if the photon is absorbed by it.

The general form of the entangled photon input state is $|\varphi_e\rangle = \alpha|1\rangle|\phi_1\rangle + \beta|2\rangle|\phi_2\rangle$, where $|\phi_1\rangle$, $|\phi_2\rangle$ are any pure states of the photon B part. It is not hard to find that the transforming matrices Eqs. (7-30), (7-31) and the P_{loss}, P_{error} expressions Eqs. (7-32), (7-33) are also suitable for the entangled photon input case because the transfer matrices play the same role as quantum channels for the photon A part. In the rest of our article, the single photon and entangled photon input state we consider are $|\varphi_s\rangle = \alpha|1\rangle + \beta|2\rangle$ and $|\varphi_e\rangle = \alpha|1\rangle|\phi_1\rangle + \beta|2\rangle|\phi_2\rangle$ type respectively.

At the end of this section, we show another useful theorem below that describes the condition where the error probability P_{error} can reach 0. In other words, we can judge whether there is an object without any error.

Theorem 7.3： P_{error} equals to 0 for pure input state iff $\langle \varphi'' \rangle\, \varphi' = 0$.

Before we prove Th. 7.3, let us show a lemma below that is useful to our proof.

Lemma 7.1： Given two pure quantum state, $|\psi_1\rangle$, $|\psi_2\rangle$ and a positive real number p, the following relation hold,

$$\| p|\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2| \| = \sqrt{(p+1)^2 - 4p|\langle\psi_1|\psi_2\rangle|^2}. \tag{7-34}$$

And we leave the proof of Lemma. 7.1 in the Appendix. D-16 for conciseness. Now we begin to prove Th. 7.3.

Proof. With the definition in Eq. (7-33), P_{error} being

$$\begin{aligned}
P_{\text{error}} =& \frac{1}{2}\{1 - P_{\text{loss}} - \|q|\varphi'\rangle\langle\varphi'| - (1-q)|\varphi''\rangle\langle\varphi''|\|\},\\
=& \frac{1}{2}\{q\langle\varphi'|\varphi'\rangle + 1 - q - \|q|\varphi'\rangle\langle\varphi'| - (1-q)|\varphi''\rangle\langle\varphi''|\|\},\\
=& \frac{1}{2}\{q\langle\varphi'|\varphi'\rangle + 1 - q\\
& - (1-q)\|\frac{q\,\langle\varphi'|\,\varphi'\rangle}{1-q}\frac{|\varphi'\rangle\langle\varphi'|}{\langle\varphi'|\,\varphi'\rangle} - |\varphi''\rangle\langle\varphi''|\|\},\\
=& \frac{1}{2}\{q\langle\varphi'|\varphi'\rangle + 1 - q\\
& - \sqrt{(q\langle\varphi'|\varphi'\rangle + 1 - q)^2 - 4q(1-q)|\langle\varphi''|\varphi'\rangle|^2}\},
\end{aligned} \tag{7-35}$$

where in the second line we apply the definition of P_{loss} in Eq. (7-32); and in the last line we employ Lemma. 7.1, by substituting $\frac{|\varphi'\rangle}{\sqrt{\langle\varphi'|\varphi'\rangle}}$, $|\varphi''\rangle$ for $|\psi_1\rangle$, $|\psi_2\rangle$, and $\frac{q\langle\varphi'|\varphi'\rangle}{1-q}$ for p. Then, let us observe the last line in Eq. (7-35): the second part in the square root, i.e., $4q(1-q)|\langle\varphi''|\varphi'\rangle|^2$, is non-negative, so it is not hard to find that P_{error} can reach 0 iff $\langle\varphi''\rangle\,\varphi' = 0$. ■

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

7.4 Opaque object case

We study IFM of opaque object with finite interrogation cycle N in this section. Our task is to use the model simplified in $Sec.$ 7.3 to find the minimal values of the two important probabilities P_{loss} and P_{error}, and the corresponding states to reach them. When the object is opaque, i.e., $a = 0$, $Eq.$ (7-30) shows:

$$\begin{pmatrix} \cos^N\theta & -\sin\theta\cos^{N-1}\theta \\ 0 & 0 \end{pmatrix} |\varphi\rangle = |\varphi'\rangle. \tag{7-36}$$

7.4.1 P_{loss} and P_{error} study with single photon input state

First, let us focus on the loss probability P_{loss}. Setting the input state as $|\varphi\rangle = \alpha|1\rangle + \beta|2\rangle$ and using $Eqs.$ (7-36), (7-32), we can get

$$|\varphi'\rangle = \cos^{N-1}\theta(\alpha\cos\theta - \beta\sin\theta)|1\rangle, \tag{7-37}$$

$$\begin{aligned} P_{\text{loss}} &= q(1 - |\cos^{N-1}\theta(\alpha\cos\theta - \beta\sin\theta)|^2), \\ &\geq q(1 - \cos^{2(N-1)}\theta), \end{aligned} \tag{7-38}$$

where the inequality in the second line of Eq. (7-38) is due to the fact that the absolute value of the inner product for the two vectors $(\cos\theta, -\sin\theta)^T$ and $(\alpha, \beta)^T$ is not larger than 1. And it is not hard to find that the minimum can be reached by the state $|\varphi_a\rangle = \cos\theta|1\rangle - \sin\theta|2\rangle$, with the global phase neglected (since the global phase actually makes no difference to the state in the IFM process, we always neglect it without announcement in the following).

Then we study the error probability P_{error}. And we calculate the value of $\langle\varphi''|\varphi'\rangle$ and check whether there are input states can fulfill the condition stated in $Th.$ 7.3 and let P_{error} reach 0. With the help of $Eq.$ (7-31) and $Eq.$ (7-37), we have

$$|\varphi''\rangle = -\beta|1\rangle + \alpha|2\rangle, \tag{7-39}$$

$$\langle\varphi''|\varphi'\rangle = -\beta^*\cos^{N-1}\theta(\alpha\cos\theta - \beta\sin\theta). \tag{7-40}$$

It is not difficult to find that there are two states can make $\langle\varphi''|\varphi'\rangle = 0$. The first one is $|\varphi_b\rangle = |1\rangle$, and the second one is $|\varphi_c\rangle = \sin\theta|1\rangle + \cos\theta|2\rangle$. That is, we can both realize zero error in IFM with these two states.

Thus, it is necessary to compare the loss probability P_{loss} of $|\varphi_b\rangle$, $|\varphi_c\rangle$. And the P_{loss} of the two states are $q(1 - \cos^{2N}\theta)$ and q respectively, by the definition of $Eq.$ (7-32). It

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

indicates that the first state is better than the second one considering P_{loss}, since when N is large enough,

$$q(1 - \cos^{2N}\theta) \simeq q\frac{\pi^2}{4N} \ll q. \tag{7-41}$$

And note that the P_{loss} of $|\varphi_b\rangle$ will approaches 0, as $N \to \infty$ [Kwiat et al. (1995, 1999)]. For the second state $|\varphi_c\rangle$, the photon is always lost if the object is there; it is the reason why $|\varphi_c\rangle$ can detect the object without any error. But it is useless in our problem since it violates the principle of IFM, i.e., detecting the object with as small as possible photon loss probability.

7.4.2 P_{loss} and P_{error} study with entangled photon input state

Here we want to study the power of quantum correlation for IFM in the opaque object case. So we set the initial input state as the general form $|\varphi\rangle = \alpha|1\rangle|\phi_1\rangle + \beta|2\rangle|\phi_2\rangle$, where $|\phi_1\rangle$, $|\phi_2\rangle$ are any pure states of the photon B part and α, β are non-negative real numbers (one can always remove the phase information in α, β to the states $|\phi_1\rangle$, $|\phi_2\rangle$ of the photon B part to obtain this form).

As mentioned earlier, the equations utilized in the single photon input case can also be used in this entangled photon input case. And we should do the transforming matrix operations on the photon A part and evaluate the two probabilities P_{loss} and P_{error} in the same way as in 7.4.1.

We first study the loss probability P_{loss}. Using $Eq.$ (7-36), we have

$$|\varphi'\rangle = \cos^{N-1}\theta|1\rangle(\alpha\cos\theta|\phi_1\rangle - \beta\sin\theta|\phi_2\rangle), \tag{7-42}$$

and with the help of $Eq.$ (7-32), the loss probability shows

$$\begin{aligned} P_{\text{loss}} &= q[1 - |\cos^{N-1}\theta(\alpha\cos\theta|\phi_1\rangle - \beta\sin\theta|\phi_2\rangle)|^2], \\ &\geq q[1 - \cos^{2(N-1)}\theta(\alpha\cos\theta + \beta\sin\theta)^2], \\ &\geq q[1 - \cos^{2(N-1)}\theta]. \end{aligned} \tag{7-43}$$

Here the first inequality is saturated when $|\phi_1\rangle = -|\phi_2\rangle$, and the second inequality is saturated when $\alpha = \cos\theta$ and $\beta = \sin\theta$. Thus, the minimum of P_{loss} can be reached by the state $|\varphi_a^*\rangle = (\cos\theta|1\rangle - \sin\theta|2\rangle)|\phi_1\rangle$, where we use the superscript $*$ label the bipartite state. Especially, it is a product state, which is equivalent to the state $|\varphi_a\rangle$ in the single photon input case after neglecting the photon B part.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Next, we study the error probability P_{error} in this entangled photon input case. With $Eq.$ (7-37), we can obtain the output state in the absence of the object as

$$|\varphi''\rangle = \alpha|2\rangle|\phi_1\rangle - \beta|1\rangle|\phi_2\rangle, \tag{7-44}$$

and applying Eq. (7-42), the value of $\langle\varphi''|\varphi'\rangle$ shows the following form

$$\langle\varphi''|\varphi'\rangle = (-\alpha\beta\cos\theta\langle\phi_2|\phi_1\rangle + \beta^2\sin\theta)\cos^{N-1}\theta. \tag{7-45}$$

From Eq. (7-45), we can get a family of the solutions for $\langle\varphi''|\varphi'\rangle = 0$ which satisfies

$$\frac{\beta\sin\theta}{\alpha\cos\theta} = \langle\phi_2|\phi_1\rangle. \tag{7-46}$$

The two solutions in the single photon input case are both included in $Eq.$ (7-46). They are the states $|\varphi_b^*\rangle = |1\rangle|\phi_1\rangle$ and $|\varphi_c^*\rangle = (\sin\theta|1\rangle + \cos\theta|2\rangle)|\phi_1\rangle$. Now we shall check which one is the best state in this family considering P_{loss}. Using $Eqs.$ (7-32), (7-46), we get

$$P_{\text{loss}} = q[1 - \cos\theta^{2(N-1)}(\alpha^2\cos^2\theta - \beta^2\sin^2\theta)]. \tag{7-47}$$

It is clear that $|\varphi_b^*\rangle = |1\rangle|\phi_1\rangle$ reaches the minimum $q(1 - \cos^{2N}\theta)$ in this family, which is equivalent to $|\varphi_b\rangle$ in the single photon input case.

From 7.4.1, 7.4.2, we conclude that the entangled photon input state makes no enhancement to the optimization for the two important probabilities P_{loss} and P_{error} respectively, compared with single photon input state, and the states which reach the minimums are the same in some sense in these two cases. In addition, the state $|1\rangle$ is the optimal state which can make P_{loss} and P_{error} both reach zero when $N \to \infty$.

7.5 Semitransparent object case

In this section, we go further for the general case. In practical application of IFM, the object is always semitransparent, i.e., partially absorbing the photon. Thus, we will study the minimal P_{loss} and P_{error}, and the states to reach them also in this semitranparent object case, just like in the opaque object case. In addition, the effect of quantum entanglement is also investigated.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

7.5.1 Simplify the transforming matrix

The major difficulty to study the general case is to simplify the transforming matrix in $Eq.$ (7-30). First we can represent the matrix in one interrogation cycle with Pauli matrices as

$$
\begin{aligned}
C_0 =&\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \\
=&\frac{(1-a)\cos\theta}{2}\sigma_z - \frac{i(1+a)\sin\theta}{2}\sigma_y - \frac{(1-a)\sin\theta}{2}\sigma_x \\
&+\frac{(1+a)\cos\theta}{2}I.
\end{aligned}
\tag{7-48}
$$

Then we changes the basis by applying a unitary transformation $U = e^{-i\frac{\sigma_y}{2}\theta}$ and obtain

$$
\begin{aligned}
C_1 =&UC_0U^\dagger, \\
=&\frac{(1-a)}{2}\sigma_z - \frac{i(1+a)\sin\theta}{2}\sigma_y + \frac{(1+a)\cos\theta}{2}I, \\
=&\frac{(1-a)}{2}(\sigma_z - ik_1\sigma_y + k_2 I),
\end{aligned}
\tag{7-49}
$$

where we use

$$
\begin{aligned}
k_1 &= \frac{(1+a)\sin\theta}{1-a}, \\
k_2 &= \frac{(1+a)\cos\theta}{1-a},
\end{aligned}
\tag{7-50}
$$

for simplicity, and they are both positive numbers. Because we sample all the states in the Hilbert space, the change of the basis or the unitary transformation does not matter. Thus hereafter, we handle the semitransparent object scenario IFM in the new basis for simplicity. And in the following, any matrix O should be changed to $UOU^\dagger$; $|\varphi\rangle$ labels a specific vector coordinate in the new basis for convenience and $U^\dagger|\varphi\rangle$ is the same state but the coordinate value is obtained in the old basis.

The power N of the matrix C_1, labeled by C, can be calculated by expanding the binomial with the help of the equality $(\sigma_z - ik_1\sigma_y)^2 = 1 - k_1^2$, which is the result of the

邵钰莱2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

anti-commutation relation $\{\sigma_z, \sigma_y\} = 0$.

$$\begin{aligned} C =& C_1^N, \\ =&(\frac{1-a}{2})^N[(\sigma_z - ik_1\sigma_y) + k_2 I)]^N, \\ =&(\frac{1-a}{2})^N[\sum_{k\in odd}\binom{N}{k}(1-k_1^2)^{\frac{k-1}{2}}k_2^{N-k}(\sigma_z - ik_1\sigma_y) \\ &+ \sum_{k\in even}\binom{N}{k}(1-k_1^2)^{\frac{k}{2}}k_2^{N-k}I], \\ =&(\frac{1-a}{2})^N[f_1(\sigma_z - ik_1\sigma_y) + f_2 I], \end{aligned} \tag{7-51}$$

where we substitute f_1 and f_2 for the summations before the operators $(\sigma_z - ik_1\sigma_y)$ and I respectively. In fact, f_1 and f_2 are related to the summations of the even and odd terms in the corresponding binomial.

Thus, we define Σ_1 and Σ_2 as below, which are sum of the odd and even terms of the corresponding binomial. When $k_1 \leq 1$:

$$\begin{cases} \Sigma_1 = \dfrac{(\sqrt{1-k_1^2} + k_2)^N - (-\sqrt{1-k_1^2} + k_2)^N}{2} \\ \Sigma_2 = \dfrac{(\sqrt{1-k_1^2} + k_2)^N + (-\sqrt{1-k_1^2} + k_2)^N}{2} \end{cases} \tag{7-52}$$

when $k_1 > 1$:

$$\begin{cases} \Sigma_1 = \dfrac{(i\sqrt{k_1^2-1} + k_2)^N - (-i\sqrt{k_1^2-1} + k_2)^N}{2} \\ \Sigma_2 = \dfrac{(i\sqrt{k_1^2-1} + k_2)^N + (-i\sqrt{k_1^2-1} + k_2)^N}{2} \end{cases} \tag{7-53}$$

Then we can obtain the expressions for f_1 and f_2 in $Eq.$ (7-51) with Σ_1 and Σ_2, when $k_1 \leq 1$:

$$\begin{cases} f_1 = \dfrac{\Sigma_1}{\sqrt{1-k_1^2}} \\ f_2 = \Sigma_2 \end{cases} \tag{7-54}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

when $k_1 > 1$:

$$\begin{cases} f_1 = \dfrac{\Sigma_1}{i\sqrt{k_1^2 - 1}} \\ f_2 = \Sigma_2 \end{cases} \tag{7-55}$$

The insight of the above result is that the eigenstates of C_1 and C should be the same and the eigenvalues from C are just the power N of the ones from C_1 . So the structures of $Eq.$ (7-49), (7-51) are also the same, linear combination of $(\sigma_z - ik_1\sigma_y)$ and I. Especially, $(\sigma_z - ik_1\sigma_y)$ determines the eigenstates and the eigenvalues of it are $\pm\sqrt{1 - k_1^2}$. That's why we have the formulas like $Eq.$ (7-52), (7-53), (7-54), (7-55) . Clearly, f_1 and f_2 are functions of a and θ and we will show that they are both real positive number in the following theorem.

Theorem 7.4： f_1 and f_2 are both real positive numbers no matter what value k_1 is.

Proof. When $k_1 \le 1$, Σ_1 and Σ_2 are the sum of odd and even terms of $(\sqrt{1 - k_1^2} + k_2)^N$ respectively. It is obvious that f_1 and f_2 are both real positive numbers. When $k_1 > 1$, Σ_1 and Σ_2 are the imaginary and real part of $(i\sqrt{k_1^2 - 1} + k_2)^N$. We just need to check which quadrant this complex number locates in. Because $\frac{\sqrt{k_1^2-1}}{k_2} \le \frac{k1}{k2} = \tan\theta$ and $N\theta = \frac{\pi}{2}$, we know it locates in the first quadrant. Then f_1 and f_2 are also real positive numbers in this case by the definition Eq. (7-55). ■

7.5.2 P_{loss} study with single photon and entangled photon input state

With the knowledge of 7.5.1, now we can get the photon loss probability P_{loss} in the new basis by the definition Eq. (7-32) as

$$\begin{aligned} P_{\text{loss}} &= q(1 - \langle\varphi'|\varphi'\rangle), \\ &= q(1 - \langle\varphi|C^\dagger C|\varphi\rangle), \\ &= q[1 - \mathrm{Tr}_{AB}(C^\dagger C|\varphi\rangle\langle\varphi|)], \\ &= q[1 - \mathrm{Tr}_A(C^\dagger C\rho_A)], \end{aligned} \tag{7-56}$$

where in the final line we trace out the photon B part since the transforming matrix C just operates on the photon A. Eq. (7-56) reminds us that the entangled photon input state $|\varphi_{AB}\rangle$ behaves the same as $\mathrm{Tr}_B(\varphi_{AB}) = \rho_A$ for P_{loss}, as showed in $Th.$ 7.2. Especially, if one reaches the minimum of P_{loss} with the single photon input state $|\varphi_A\rangle$, one can surely

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

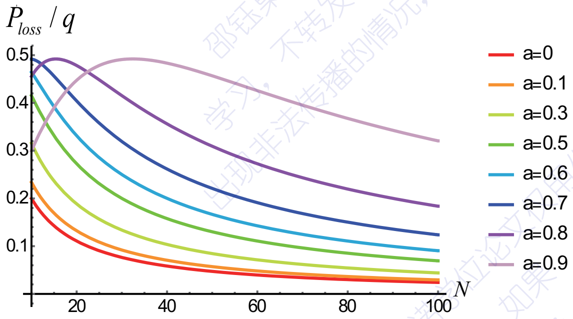


Figure 7.4 $(P_{\text{loss}}/q)_{min}$ vs the interrogation cycle N for different transparency a^2

find any pure state like $|\varphi_A\rangle|\phi_B\rangle$ to reach the same minimal value. Hence we just need to study P_{loss} in the single photon input case.

Thus $\langle\varphi|C^\dagger C|\varphi\rangle$ in $Eq.$ (7-56) should be maximized only for single photon input state, and $C^\dagger C$ can be expanded as

$$C^\dagger C = (\frac{1-a}{2})^{2N}[f_1^2(1+k_1^2)+f_2^2]I + 2f_1(f_2\sigma_z - f_1k_1\sigma_x). \tag{7-57}$$

It is the same as to find the larger eigenvalue for a single spin Hamiltonian. Thus, no matter what the value of k_1 is, it is not hard to obtain the minimal P_{loss} being

$$(P_{\text{loss}})_{min} = q[1-(\frac{1-a}{2})^{2N}(f_1+\sqrt{f_2^2+f_1^2k_1^2})^2]. \tag{7-58}$$

Utilizing $Eq.$ (7-58), the relation between the normalized photon loss rate $(P_{\text{loss}}/q)_{min}$ and the interrogation cycle N for different transparency a^2 is exhibited in $Fig.$ 7.4. It shows that when N is large enough, $(P_{\text{loss}}/q)_{min}$ decreases with the increasing of N no matter what value a is. Generally speaking, $(P_{\text{loss}}/q)_{min}$ of small a is always less than that of large a for a fixed large enough N. However, $(P_{\text{loss}}/q)_{min}$ can increase and then decrease for large enough a with the increasing of N. Via numerical analysis, we find that the maximum of the curve for a given large a can be obtained at N', which is slightly larger than the one determined by the equation $k_1 = \frac{1+a}{1-a}\sin(\frac{\pi}{2N}) = 1$, as showed in Fig. 7.6.

The state reaching the minimum of P_{loss}, named $|\varphi_0\rangle$, is just the eigenstate of $C^\dagger C$ with larger eigenvalue. $|\varphi_0\rangle\langle\varphi_0|$ is on the xz plane of the Bloch sphere with the angle between state the $|\varphi_0\rangle\langle\varphi_0|$ and the z direction is $\theta_1 = \arctan(\frac{f_1k_1}{f_2})$ (see Fig. 7.5). The corresponding vector $U^\dagger|\varphi_0\rangle$ is the one which reach the minimal P_{loss} in the old basis. And it is not hard to find $U^\dagger|\varphi_0\rangle = |\varphi_a\rangle$ when the transparency $a^2 = 0$, i.e., opaque object case.

7.5.3 P_{error} study with single photon and entangled photon input state

Here, we derive the error probability P_{error} of IFM in both single photon and entangled photon input scenarios.

For convenience, we label the unitary transformation in $Eq.$ (7-31) by D, as the object is absent.

$$D = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y. \tag{7-59}$$

In $Th.$ 7.3, we have showed that P_{error} can reach 0 iff $\langle\varphi''|\varphi'\rangle = 0$, no matter which type the input state is. By definition, we get $\langle\varphi''|\varphi'\rangle$ in the new basis as

$$\begin{aligned} \langle\varphi''|\varphi'\rangle =& \langle\varphi|UD^{\dagger}U^{\dagger}C|\varphi\rangle, \\ =& \langle\varphi|D^{\dagger}C|\varphi\rangle, \\ =& \mathrm{Tr}_{AB}(D^{\dagger}C|\varphi\rangle\langle\varphi|), \\ =& \mathrm{Tr}_{A}(D^{\dagger}C\rho_A). \end{aligned} \tag{7-60}$$

In the second line, we use the fact that U commutes with $D^{\dagger}$; The third line is due to the fact that $D^{\dagger}$ and C only operate on the photon A part. From the definition of D and C, we have $D^{\dagger}C$ being

$$D^{\dagger}C = \left(\frac{1-a}{2}\right)^{N} [f_1 k_1 I + (i f_2 \sigma_y - f_1 \sigma_x)]. \tag{7-61}$$

In the meantime, ρ_A has the following Bloch sphere representation,

$$\rho_A = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}). \tag{7-62}$$

Then Eq. (7-60) becomes $\langle\varphi''|\varphi'\rangle = (\frac{1-a}{2})^N (f_1 k_1 - f_1 r_x + i f_2 r_y)$ with the fact that the trace of pauli matrix is 0. In order to make $P_{\text{error}} = 0$, we should let $r_x = k_1$ and $r_y = 0$.

When $k_1 \leq 1$, there are two pure state solutions $\rho_A = |\varphi_{\pm}\rangle\langle\varphi_{\pm}| = \frac{1}{2}(I + k_1\sigma_x \pm \sqrt{1-k_1^2}\sigma_z)$ of photon A. The angle between each pure solution $|\varphi_{\pm}\rangle\langle\varphi_{\pm}|$ and the z axis is $\theta_2 = \arctan(\frac{k_1}{\sqrt{1-k_1^2}})$ on the Bloch sphere (see $Fig.$ 7.5). And it is straightforward to see that any convex mixing of the two pure solutions can also lead to $Tr_A(D^{\dagger}C\rho_A) = 0$. Therefore, in the bipartite scenario, the solution to $P_{\text{error}} = 0$ is $\alpha\,|\varphi_+\rangle\,|\phi_1\rangle + \beta\,|\varphi_-\rangle\,|\phi_1^{\perp}\rangle$, where $\langle\phi_1^{\perp}|\,\phi_1\rangle = 0$ and α, β are two arbitrary state coefficients. Like in $a = 0$ case, we have a family of best states which reach $P_{\text{error}} = 0$ in the entangled photon input scenario.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

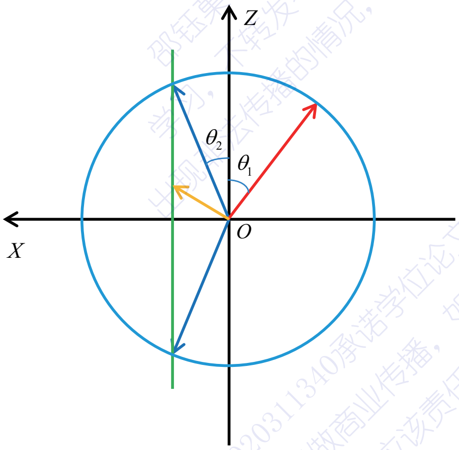


Figure 7.5 The positions of the states on Bloch sphere which reach the minimal P_{loss} and P_{error} in the new basis. The red vector represents the state $|\varphi_0\rangle\langle\varphi_0|$ which reaches the minimal P_{loss}. The two blue vectors represent $|\varphi_\pm\rangle\langle\varphi_\pm|$. Any mixed state on the green line which is the connection between the end of the two blue vectors can satisfy $\text{Tr}_A(D^\dagger C\rho_A) = 0$. The yellow vector represents one of these mixed states and its purification is a entangled photon input state $\alpha\,|\varphi_+\rangle\,|\phi_1\rangle + \beta\,|\varphi_-\rangle\,|\phi_1^\perp\rangle$, which makes $P_{\text{error}} = 0$.

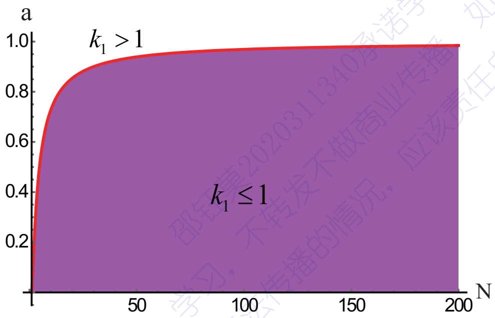


Figure 7.6 Red curve: transparency a vs interrogation cycle N determined by $k_1 = \frac{1+a}{1-a}\sin(\frac{\pi}{2N}) = 1$. Shadow purple region indicates the parameter domain where we can reach $P_{\text{error}} = 0$.

Furthermore, we aim to find the solution that minimize the photon loss rate P_{loss} given in Eq. (7-56) in this family. Combining the solution to $P_{\text{error}} = 0$, we can show that the optimal state in this family is $|\varphi_+\rangle\langle\varphi_+| = \frac{1}{2}(I + k_1\sigma_x + \sqrt{1-k_1^2}\sigma_z)$ with the minimal P_{loss} value being

$$(P_{\text{loss}})_{|\varphi_+\rangle} = q[1 - (\frac{1-a}{2})^{2N}(f_1\sqrt{1-k_1^2} + f_2)^2]. \tag{7-63}$$

which means entangled photon input state does no good to P_{error} in this k_1 regime.

When $k_1 > 1$, there is no solution to $\langle\varphi''|\varphi'\rangle = 0$ or equivalently $P_{\text{error}} = 0$. Nevertheless, we can still analyze the nonzero minimum of P_{error}. Using Eqs. (7-35), (7-

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

56) and (7-60), we have the general expression of P_{error} being

$$\begin{aligned} P_{\text{error}} = & \frac{1}{2}\{qTr[C^{\dagger}C\rho_A] + (1-q) \\ & - \sqrt{(qTr[C^{\dagger}C\rho_A] + 1 - q)^2 - 4q(1-q)|Tr[D^{\dagger}C\rho_A]|^2}\}, \end{aligned} \tag{7-64}$$

which is suitable no matter what value k_1 is. It indicates that $|\varphi_{AB}\rangle$ appears in the form $Tr_B(\varphi_{AB}) = \rho_A$ for P_{error} in all k_1 regime. It is crucial to emphasize that the expression for P_{error} of Eq. (7-64) is suitable for any pure states, single photon or entangled photon input, but not for mixed state ρ_A, because our pure state prerequisite. Moreover, we find the entangled photon input state can not enhance the performance on P_{error} for any values of k_1, compared with the single photon input state, i.e., the minimum of Eq. (7-64) should be reached by pure state $\rho_A = |\varphi_A\rangle\langle\varphi_A|$. The detailed discussion about the effect of the quantum correlation to P_{error} is arranged in Appendix. E.4.

7.5.4 $N \to \infty$ behavior

In the above subsections, we have systematically analysed the general IFM model of the semitransparent object with finite interrogation cycle. Now, in this part, we study the asymptotic behavior of the relevant quantities when the interrogation cycle $N \to \infty$. The behavior of the minimal values for P_{loss}, P_{error} and the initial input states which can reach the minimums are investigated in the $N \to \infty$ condition.

When the interrogation cycle $N \to \infty$, $k_1 = \frac{1+a}{1-a}\sin(\frac{\pi}{2N}) \to 0 < 1$ for any fixed a. Therefore we always have the state $|\varphi_+\rangle$ to reach $P_{\text{error}} = 0$. First we consider the asymptotic behavior of $(P_{\text{loss}})_{|\varphi_+\rangle}$, described by $Eq.$ (7-63). With the help of $Eqs.$ (7-52), (7-54) and the definitions of k_1, k_2 (Eq. (7-50)), we have

$$\begin{aligned} & (\frac{1-a}{2})^{2N}(f_1\sqrt{1-k_1^2} + f_2)^2, \\ =& (\frac{1-a}{2})^{2N}(\Sigma_1 + \Sigma_2)^2, \\ =& [\frac{1-a}{2}(k_2 + \sqrt{1-k_1^2})]^{2N}, \\ =& [\frac{(1+a)\cos\theta + \sqrt{(1-a)^2 - (1+a)^2\sin^2\theta}}{2}]^{2N}, \\ \simeq& [1 - \frac{1+a}{1-a}\frac{\pi^2}{8N^2} + O(\frac{1}{N^4})]^{2N}, \\ \simeq& 1 - \frac{1+a}{1-a}\frac{\pi^2}{4N} + O(\frac{1}{N^3}), \end{aligned} \tag{7-65}$$

where we use the fact the $\cos\theta = 1 - \frac{\theta^2}{2} + O(\theta^4)$, $\sin\theta = \theta - O(\theta^3)$ and $\theta = \frac{\pi}{2N}$. Then the

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

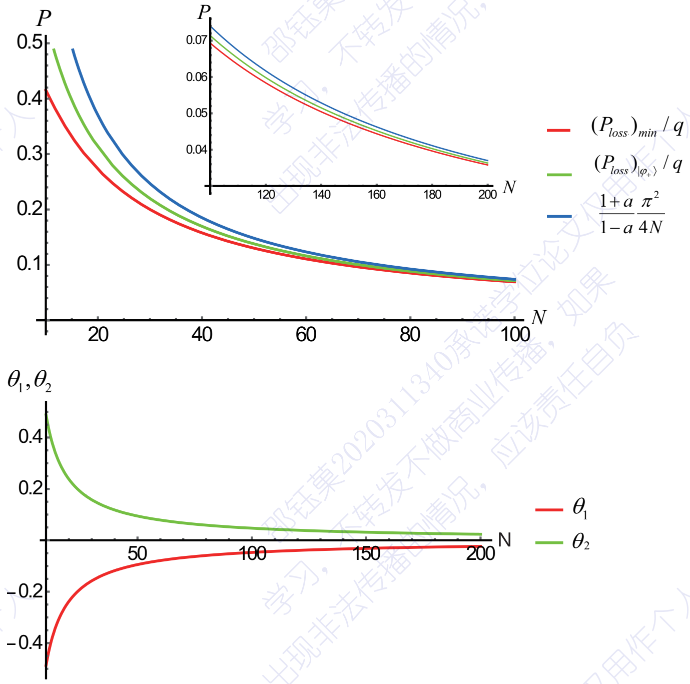


Figure 7.7 All the graphs are plotted at $a = 0.5$. (a) The asymptotic behaviors of $(P_{\text{loss}})_{|\varphi_+\rangle}/q, (P_{\text{loss}})_{min}/q$ as $N \to \infty$. The green line $(P_{\text{loss}})_{|\varphi_+\rangle}/q$ is always above the red line $(P_{\text{loss}})_{min}/q$. The main term of the asymptotic expressions in Eqs. (7-66), (7-67), i.e., $\frac{1+a}{1-a}\frac{\pi^2}{4N}$, is also shown in the plot with blue line. Inset: N ranges from 100 to 200. All the three terms go to zero asymptotically when $N \to \infty$. (b) The asymptotic behavior of θ_1 and θ_2. We use negative sign for θ_1 because it locates at the negative X axis side, as showed in Fig. 7.5.

asymptotic expression of $Eq.$ (7-63) is

$$(P_{\text{loss}})_{|\varphi_+\rangle}^{N\to\infty} \simeq q[\frac{1+a}{1-a}\frac{\pi^2}{4N} - O(\frac{1}{N^3})]. \tag{7-66}$$

Clearly, whatever the value of a is, $(P_{\text{loss}})_{|\varphi_+\rangle}$ goes to 0 for sufficient large N.

Furthermore, we aim to consider the asymptotic behavior of $Eq.$ (7-58), the minimum of P_{loss}. Utilizing the similar approximation technique as for $(P_{\text{loss}})_{|\varphi_+\rangle}$, it shows

$$(P_{\text{loss}})_{min}^{N\to\infty} \simeq q[\frac{1+a}{1-a}\frac{\pi^2}{4N} - O(\frac{1}{N^2})]. \tag{7-67}$$

And the detailed derivation is put in the Appendix. E.5. In addition, the asymptotic behavior of $(P_{\text{loss}})_{|\varphi_+\rangle}/q, (P_{\text{loss}})_{min}/q$ have been plotted in $Fig.$ 7.7.

When $N \to \infty$, θ_1 and θ_2, relating to the initial input states $|\varphi_0\rangle$, $|\varphi_+\rangle$, both go to zero (see Fig. 7.7). And the unitary $U = e^{-i\frac{\sigma_y}{2}\theta}$ of changing basis goes to identity. Hence, the corresponding vectors $U^\dagger|\varphi_0\rangle$ which reaches the $(P_{\text{loss}})_{min}$ and $U^\dagger|\varphi_+\rangle$ which reaches the minimum of P_{loss} but keeping $P_{\text{error}} = 0$ in the old basis , go to the same vector $(1,0)^T$, i.e.,

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

$|1\rangle$ in our system. That is to say, as $N \to \infty$, we can use $|1\rangle$ to realize $P_{\text{loss}} = P_{\text{error}} = 0$ asymptotically, perfect detecting the object without photon loss even if the object is a semitransparent one.

7.6 Discussion

We remark that $P_f = P_{\text{loss}} + P_{\text{error}}$ is a more significant criteria to evaluate IFM process, because it describes all the possibilities where the IFM process is a failure, including both the photon loss (object damage) and the error making in the discrimination process. However, even for this criteria P_f, we can also come to the conclusion that the quantum correlation (entanglement in our problem) can not benefit IFM process(see Appendix. E.4). In addition, the asymptotic behaviors are also studied and we find that the state $|1\rangle$ in our system can perfectly detect the generic semitransparent object without any object damage when $N \to \infty$.

Our work provides support for the practical realization of IFM, like electron microscopy of biological substances or detection of fragile nano-materials. Moreover, our theoretical approaches, borrowing from quantum information theory, such as quantum channel theory, quantum state discrimination etc, can be applied to other quantum detection scenarios and the analysis of whether quantum correlation can benefit these processes or not is intriguing.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Bibliography

Aaronson S, Arkhipov A. 2011. The computational complexity of linear optics[C/OL]//STOC '11: Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing. New York, NY, USA: ACM: 333-342. http://doi.acm.org/10.1145/1993636.1993682.

Åberg J. 2014. Catalytic coherence[J]. Physical Review Letters, 113(15): 150402.

Acín A, Bruß D, Lewenstein M, et al. 2001. Classification of mixed three-qubit states[J/OL]. Phys. Rev. Lett., 87: 040401. https://link.aps.org/doi/10.1103/PhysRevLett.87.040401.

Amico L, Fazio R, Osterloh A, et al. 2008. Entanglement in many-body systems[J/OL]. Rev. Mod. Phys., 80: 517-576. https://link.aps.org/doi/10.1103/RevModPhys.80.517.

Azuma H. 2006. Interaction-free measurement with an imperfect absorber[J]. Physical Review A, 74 (5): 054301.

Bagan E, Bergou J A, Cottrell S S, et al. 2016. Relations between coherence and path information[J/OL]. Phys. Rev. Lett., 116: 160406. https://link.aps.org/doi/10.1103/PhysRevLett.116.160406.

Baumgratz T, Gross D, Cramer M, et al. 2013. Scalable reconstruction of density matrices[J/OL]. Phys. Rev. Lett., 111: 020401. https://link.aps.org/doi/10.1103/PhysRevLett.111.020401.

Baumgratz T, Cramer M, Plenio M B. 2014. Quantifying coherence[J/OL]. Phys. Rev. Lett., 113: 140401. https://link.aps.org/doi/10.1103/PhysRevLett.113.140401.

Bennett C H, Brassard G. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing [C/OL]//Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. New York: IEEE Press: 175-179. https://doi.org/10.1016/j.tcs.2014.05.025.

Bennett C H. 1992. Quantum cryptography using any two nonorthogonal states[J/OL]. Phys. Rev. Lett., 68: 3121-3124. https://link.aps.org/doi/10.1103/PhysRevLett.68.3121.

Bennett C H, Brassard G, Mermin N D. 1992. Quantum cryptography without bell's theorem[J/OL]. Phys. Rev. Lett., 68: 557-559. https://link.aps.org/doi/10.1103/PhysRevLett.68.557.

Bennett C H, Brassard G, Crépeau C, et al. 1993. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels[J/OL]. Phys. Rev. Lett., 70: 1895-1899. https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

Bennett C H, Brassard G, Popescu S, et al. 1996a. Purification of noisy entanglement and faithful teleportation via noisy channels[J/OL]. Phys. Rev. Lett., 76: 722-725. https://link.aps.org/doi/10.1103/PhysRevLett.76.722.

Bennett C H, DiVincenzo D P, Smolin J A, et al. 1996b. Mixed-state entanglement and quantum error correction[J]. Physical Review A, 54(5): 3824.

Berta M, Christandl M, Colbeck R, et al. 2010. The uncertainty principle in the presence of quantum memory[J]. Nature Physics, 6: 659-662.

Boileau J C, Tamaki K, Batuwantudawe J, et al. 2005. Unconditional security of a three state quantum key distribution protocol[J/OL]. Phys. Rev. Lett., 94: 040503. https://link.aps.org/doi/10.1103/PhysRevLett.94.040503.

Boixo S, Isakov S V, Smelyanskiy V N, et al. 2018. Characterizing quantum supremacy in near-term devices[J/OL]. Nature Physics, 14(6): 595-600. https://doi.org/10.1038/s41567-018-0124-x.

Born M. 1926. Zur quantenmechanik der stoßvorgänge[J/OL]. Zeitschrift für Physik, 37(12): 863-867. https://doi.org/10.1007/BF01397477.

Bourennane M, Eibl M, Kurtsiefer C, et al. 2004. Experimental detection of multipartite entanglement using witness operators[J/OL]. Phys. Rev. Lett., 92: 087902. https://link.aps.org/doi/10.1103/PhysRevLett.92.087902.

Boyd S, Vandenberghe L. 2004. Convex optimization[M]. [S.l.]: Cambridge university press

Branciard C, Rosset D, Liang Y C, et al. 2013. Measurement-device-independent entanglement witnesses for all entangled quantum states[J/OL]. Phys. Rev. Lett., 110: 060405. https://link.aps.org/doi/10.1103/PhysRevLett.110.060405.

Braunstein S L, Caves C M, Milburn G. 1996. Generalized uncertainty relations: Theory, examples, and lorentz invariance[J/OL]. Annals of Physics, 247(1): 135 - 173. http://www.sciencedirect.com/science/article/pii/S0003491696900408.

Briegel H J, Raussendorf R. 2001. Persistent entanglement in arrays of interacting particles[J/OL]. Phys. Rev. Lett., 86: 910-913. https://link.aps.org/doi/10.1103/PhysRevLett.86.910.

Britton J W, Sawyer B C, Keith A C, et al. 2012. Engineered two-dimensional ising interactions in a trapped-ion quantum simulator with hundreds of spins[J/OL]. Nature, 484: 489 EP -. https://doi.org/10.1038/nature10981.

Brunner N, Cavalcanti D, Pironio S, et al. 2014. Bell nonlocality[J/OL]. Rev. Mod. Phys., 86: 419-478. https://link.aps.org/doi/10.1103/RevModPhys.86.419.

Çakmak B, Karpat G, Fanchini F F. 2015. Factorization and criticality in the anisotropic xy chain via correlations[J]. Entropy, 17(2): 790-817.

Carleo G, Troyer M. 2017. Solving the quantum many-body problem with artificial neural networks [J/OL]. Science, 355(6325): 602-606. http://science.sciencemag.org/content/355/6325/602.

Chen K, Lo H K. 2007. Multi-partite quantum cryptographic protocols with noisy GHZ states [J/OL]. Quantum Information & Computation, 7(8): 689-715. http://www.rintonpress.com/xqic7/qic-7-8/689-715.pdf.

Chen L K, Li Z D, Yao X C, et al. 2017. Observation of ten-photon entanglement using thin bib 3 o 6 crystals[J]. Optica, 4(1): 77-83.

Chirolli L, Strambini E, Giovannetti V, et al. 2010. Electronic implementations of interaction-free measurements[J]. Physical Review B, 82(4): 045403.

Chitambar E, Streltsov A, Rana S, et al. 2016a. Assisted distillation of quantum coherence[J]. Physical Review Letters, 116(7): 070402.

Chitambar E, Gour G. 2016b. Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence[J/OL]. Phys. Rev. Lett., 117: 030401. https://link.aps.org/doi/10.1103/PhysRevLett.117.030401.

Chitambar E, Hsieh M H. 2016c. Relating the resource theories of entanglement and quantum coherence[J/OL]. Phys. Rev. Lett., 117: 020402. http://link.aps.org/doi/10.1103/PhysRevLett.117.020402.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Cirac J I, Ekert A K, Huelga S F, et al. 1999. Distributed quantum computation over noisy channels [J/OL]. Phys. Rev. A, 59: 4249-4254. https://link.aps.org/doi/10.1103/PhysRevA.59.4249.

Cleve R, Gottesman D, Lo H K. 1999. How to share a quantum secret[J/OL]. Phys. Rev. Lett., 83: 648-651. https://link.aps.org/doi/10.1103/PhysRevLett.83.648.

Coffman V, Kundu J, Wootters W K. 2000. Distributed entanglement[J]. Physical Review A, 61(5): 052306.

Coles P J. 2012. Unification of different views of decoherence and discord[J/OL]. Phys. Rev. A, 85: 042103. https://link.aps.org/doi/10.1103/PhysRevA.85.042103.

Coles P J, Metodiev E M, Lütkenhaus N. 2016. Numerical approach for unstructured quantum key distribution[J]. Nature Communications, 7(1): 11712.

Cramer M, Plenio M B, Flammia S T, et al. 2010. Efficient quantum state tomography[J/OL]. Nature Communications, 1: 149 EP -. https://doi.org/10.1038/ncomms1147.

Curty M, Lewenstein M, Lütkenhaus N. 2004. Entanglement as a precondition for secure quantum key distribution[J/OL]. Phys. Rev. Lett., 92: 217903. https://link.aps.org/doi/10.1103/PhysRevLett.92.217903.

Das Sarma S, Deng D L, Duan L M. 2019. Machine learning meets quantum physics[J/OL]. Physics Today, 72(3): 48-54. https://doi.org/10.1063/PT.3.4164.

Deng D L, Li X, Das Sarma S. 2017. Quantum entanglement in neural network states[J/OL]. Phys. Rev. X, 7: 021021. https://link.aps.org/doi/10.1103/PhysRevX.7.021021.

Devetak I, Winter A. 2005. Distillation of secret key and entanglement from quantum states[C]// Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences: volume 461. [S.l.]: The Royal Society: 207-235.

Dicke R H. 1954. Coherence in spontaneous radiation processes[J/OL]. Phys. Rev., 93: 99-110. https://link.aps.org/doi/10.1103/PhysRev.93.99.

Dicke R. 1981. Interaction-free quantum measurements: A paradox[J]. Am. J. Phys, 49(10): 925-930.

Djokovic D Z, Osterloh A. 2009. On polynomial invariants of several qubits[J/OL]. Journal of Mathematical Physics, 50(3): 033509. http://dx.doi.org/10.1063/1.3075830.

Du S, Bai Z, Guo Y. 2015a. Conditions for coherence transformations under incoherent operations[J]. Physical Review A, 91(5): 052120.

Du S, Bai Z, Qi X. 2015b. Coherence measures and optimal conversion for coherent states[J/OL]. Quantum Info. Comput., 15(15-16): 1307-1316. http://dl.acm.org/citation.cfm?id=2871378.2871381.

Dür W, Vidal G, Cirac J I. 2000. Three qubits can be entangled in two inequivalent ways[J/OL]. Phys. Rev. A, 62: 062314. https://link.aps.org/doi/10.1103/PhysRevA.62.062314.

Eisert J, Cramer M, Plenio M B. 2010. Colloquium: Area laws for the entanglement entropy[J/OL]. Rev. Mod. Phys., 82: 277-306. https://link.aps.org/doi/10.1103/RevModPhys.82.277.

Ekert A K. 1991. Quantum cryptography based on bell's theorem[J/OL]. Phys. Rev. Lett., 67: 661-663. https://link.aps.org/doi/10.1103/PhysRevLett.67.661.

Elitzur A C, Vaidman L. 1993. Quantum mechanical interaction-free measurements[J]. Foundations of Physics, 23(7): 987-997.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Eltschka C, Siewert J. 2014. Quantifying entanglement resources[J]. Journal of Physics A: Mathematical and Theoretical, 47(42): 424005.

Eltschka C, Bastin T, Osterloh A, et al. 2012. Multipartite-entanglement monotones and polynomial invariants[J]. Physical Review A, 85(2): 022301.

Flammia S T, Gross D, Liu Y K, et al. 2012. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators[J/OL]. New Journal of Physics, 14(9): 095022. http://stacks.iop.org/1367-2630/14/i=9/a=095022.

Fung C H F, Lo H K. 2006. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry[J/OL]. Phys. Rev. A, 74: 042342. https://link.aps.org/doi/10.1103/PhysRevA.74.042342.

Fung C H F, Tamaki K, Qi B, et al. 2009. Security proof of quantum key distribution with detection efficiency mismatch[J]. Quantum Information & Computation, 9(1): 131-165.

Fung C H F, Ma X, Chau H F. 2010. Practical issues in quantum-key-distribution postprocessing [J/OL]. Phys. Rev. A, 81: 012318. http://link.aps.org/doi/10.1103/PhysRevA.81.012318.

García-Escartín J C, Chamorro-Posada P. 2005. Quantum interrogation with particles[J]. arXiv preprint quant-ph/0512019.

Giovannetti V, Lloyd S, Maccone L. 2004. Quantum-enhanced measurements: Beating the standard quantum limit[J/OL]. Science, 306(5700): 1330-1336. http://science.sciencemag.org/content/306/5700/1330.

Giovannetti V, Lloyd S, Maccone L. 2006. Quantum metrology[J/OL]. Phys. Rev. Lett., 96: 010401. https://link.aps.org/doi/10.1103/PhysRevLett.96.010401.

Glauber R J. 1963. The quantum theory of optical coherence[J/OL]. Phys. Rev., 130: 2529-2539. https://link.aps.org/doi/10.1103/PhysRev.130.2529.

Gottesman D. 1997. Stabilizer codes and quantum error correction[J]. arXiv: quant-ph/9705052.

Gottesman D, Lo H K. 2003. Proof of security of quantum key distribution with two-way classical communications[J]. IEEE Transactions on Information Theory, 49(2): 457-475.

Gour G. 2005. Family of concurrence monotones and its applications[J]. Physical Review A, 71(1): 012318.

Gour G, Wallach N R. 2013. Classification of multipartite entanglement of all finite dimensionality [J]. Physical Review Letters, 111(6): 060502.

Greenberger D M, Horne M A, Zeilinger A. 1989. Going beyond belląŕs theorem[J]. In: Kafatos M. (eds) Belląŕs Theorem, Quantum Theory and Conceptions of the Universe. Fundamental Theories of Physics, vol 37. Springer, Dordrecht: 69-72.

Gross D, Liu Y K, Flammia S T, et al. 2010. Quantum state tomography via compressed sensing[J/OL]. Phys. Rev. Lett., 105: 150401. https://link.aps.org/doi/10.1103/PhysRevLett.105.150401.

Gühne O, Toth G. 2009. Entanglement detection[J/OL]. Physics Reports, 474(1): 1 - 75. http://www.sciencedirect.com/science/article/pii/S0370157309000623.

Guhne O, Toth G, Briegel H J. 2005. Multipartite entanglement in spin chains[J/OL]. New Journal of Physics, 7(1): 229. http://stacks.iop.org/1367-2630/7/i=1/a=229.

Gühne O, Tóth G, Hyllus P, et al. 2005. Bell inequalities for graph states[J/OL]. Phys. Rev. Lett., 95: 120405. https://link.aps.org/doi/10.1103/PhysRevLett.95.120405.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Gühne O, Lu C Y, Gao W B, et al. 2007. Toolbox for entanglement detection and fidelity estimation [J/OL]. Phys. Rev. A, 76: 030305. https://link.aps.org/doi/10.1103/PhysRevA.76.030305.

Hafner M, Summhammer J. 1997. Experiment on interaction-free measurement in neutron interferometry[J/OL]. Physics Letters A, 235(6): 563 - 568. http://www.sciencedirect.com/science/article/pii/S0375960197006968.

Harrow A W. 2013. The church of the symmetric subspace[J]. arXiv:quant-ph/1308.6595.

Harrow A W, Montanaro A. 2017. Quantum computational supremacy[J/OL]. Nature, 549: 203 EP -. https://doi.org/10.1038/nature23458.

Hein M, Eisert J, Briegel H J. 2004. Multiparty entanglement in graph states[J/OL]. Phys. Rev. A, 69: 062311. https://link.aps.org/doi/10.1103/PhysRevA.69.062311.

Hein M, Dür W, Eisert J, et al. 2006. Entanglement in Graph States and its Applications[J]. arXiv e-prints: quant-ph/0602096.

Helstrom C W. 1976. Quantum detection and estimation theory: volume 123[M]. [S.l.]: Academic press

Herrero-Collantes M, Garcia-Escartin J C. 2017. Quantum random number generators[J/OL]. Rev. Mod. Phys., 89: 015004. https://link.aps.org/doi/10.1103/RevModPhys.89.015004.

Herzog U. 2004. Minimum-error discrimination between a pure and a mixed two-qubit state[J]. Journal of Optics B: Quantum and Semiclassical Optics, 6(3): S24.

Hill S, Wootters W K. 1997. Entanglement of a pair of quantum bits[J]. Physical Review Letters, 78 (26): 5022.

Hillery M. 2016. Coherence as a resource in decision problems: The deutsch-jozsa algorithm and a variation[J/OL]. Phys. Rev. A, 93: 012111. https://link.aps.org/doi/10.1103/PhysRevA.93.012111.

Hillery M, Bužek V, Berthiaume A. 1999. Quantum secret sharing[J/OL]. Phys. Rev. A, 59: 1829-1834. https://link.aps.org/doi/10.1103/PhysRevA.59.1829.

Horodecki P. 1997. Separability criterion and inseparable mixed states with positive partial transposition[J/OL]. Physics Letters A, 232(5): 333 - 339. http://www.sciencedirect.com/science/article/pii/S0375960197004167.

Horodecki R, Horodecki P, Horodecki M, et al. 2009. Quantum entanglement[J/OL]. Rev. Mod. Phys., 81: 865-942. https://link.aps.org/doi/10.1103/RevModPhys.81.865.

Huber M, de Vicente J I. 2013. Structure of multidimensional entanglement in multipartite systems[J/OL]. Phys. Rev. Lett., 110: 030501. https://link.aps.org/doi/10.1103/PhysRevLett.110.030501.

Huelga S, Plenio M. 2013. Vibrations, quanta and biology[J/OL]. Contemporary Physics, 54(4): 181-207. https://doi.org/10.1080/00405000.2013.829687.

Ichikawa T, Sasaki T, Tsutsui I, et al. 2008. Exchange symmetry and multipartite entanglement[J/OL]. Phys. Rev. A, 78: 052105. https://link.aps.org/doi/10.1103/PhysRevA.78.052105.

Inoue S, Björk G. 2000. Experimental demonstration of exposure-free imaging and contrast amplification[J]. Journal of Optics B: Quantum and Semiclassical Optics, 2(3): 338.

Jang J S. 1999. Optical interaction-free measurement of semitransparent objects[J]. Physical Review A, 59(3): 2322.

邵钰菓2020311340承诺学位论文仅用于个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Jung E, Hwang M R, Park D, et al. 2009. Three-tangle for rank-three mixed states: Mixture of greenberger-horne-zeilinger, w, and flipped-w states[J]. Physical Review A, 79(2): 024306.

Karlsson A, Björk G, Forsberg E. 1998. “interaction” (energy exchange) free and quantum nondemolition measurements[J/OL]. Phys. Rev. Lett., 80: 1198-1201. https://link.aps.org/doi/10.1103/PhysRevLett.80.1198.

Karpat G, Çakmak B, Fanchini F. 2014. Quantum coherence and uncertainty in the anisotropic xy chain[J]. Physical Review B, 90(10): 104431.

Kimble H J. 2008. The quantum internet[J/OL]. Nature, 453: 1023 EP -. https://doi.org/10.1038/nature07127.

Kleinberg J, Tardos E. 2005. Algorithm design[M]. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Koashi M. 2009. Simple security proof of quantum key distribution based on complementarity[J]. New Journal of Physics, 11(4): 045018.

Kruit P, Hobbs R, Kim C S, et al. 2016. Designs for a quantum electron microscope[J/OL]. Ultramicroscopy, 164: 31 - 45. http://www.sciencedirect.com/science/article/pii/S0304399116300146.

Kwiat P, Weinfurter H, Herzog T, et al. 1995. Interaction-free measurement[J]. Physical Review Letters, 74(24): 4763.

Kwiat P G, White A, Mitchell J, et al. 1999. High-efficiency quantum interrogation measurements via the quantum zeno effect[J]. Physical Review Letters, 83(23): 4725.

Kwiat P. 1998. Experimental and theoretical progress in interaction-free measurements[J]. Physica Scripta, 1998(T76): 115.

Lanyon B P, Maier C, HolzMang pfel M, et al. 2017. Efficient tomography of a quantum many-bodyting system[J/OL]. Nature Physics, 13: 1158 EP -. https://doi.org/10.1038/nphys4244.

Liang Y C, Rosset D, Bancal J D, et al. 2015. Family of bell-like inequalities as device-independent witnesses for entanglement depth[J/OL]. Phys. Rev. Lett., 114: 190401. https://link.aps.org/doi/10.1103/PhysRevLett.114.190401.

Liao S K, Cai W Q, Liu W Y, et al. 2017. Satellite-to-ground quantum key distribution[J/OL]. Nature, 549: 43 EP -. https://doi.org/10.1038/nature23655.

Lloyd S. 1996. Universal quantum simulators[J/OL]. Science, 273(5278): 1073-1078. http://science.sciencemag.org/content/273/5278/1073.

Lloyd S. 2008. Enhanced sensitivity of photodetection via quantum illumination[J]. Science, 321 (5895): 1463-1465.

Lo H K, Chau H F. 1999. Unconditional security of quantum key distribution over arbitrarily long distances[J/OL]. Science, 283(5410): 2050. http://science.sciencemag.org/content/283/5410/2050.

Lo H K. 2001. Proof of unconditional security of six-state quatum key distribution scheme[J/OL]. Quantum Info. Comput., 1(2): 81-94. http://dl.acm.org/citation.cfm?id=2011333.2011337.

Lo H K, Curty M, Qi B. 2012. Measurement-device-independent quantum key distribution[J/OL]. Phys. Rev. Lett., 108: 130503. https://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

Lohmayer R, Osterloh A, Siewert J, et al. 2006. Entangled three-qubit states without concurrence and three-tangle[J]. Physical Review Letters, 97(26): 260502.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Lostaglio M, Jennings D, Rudolph T. 2015a. Description of quantum coherence in thermodynamic processes requires constraints beyond free energy[J]. Nature communications, 6.

Lostaglio M, Korzekwa K, Jennings D, et al. 2015b. Quantum coherence, time-translation symmetry, and thermodynamics[J]. Physical Review X, 5(2): 021001.

Lu H, Zhao Q, Li Z D, et al. 2018. Entanglement structure: Entanglement partitioning in multipartite systems and its experimental detection using optimizable witnesses[J/OL]. Phys. Rev. X, 8: 021072. https://link.aps.org/doi/10.1103/PhysRevX.8.021072.

Lücke B, Peise J, Vitagliano G, et al. 2014. Detecting multiparticle entanglement of dicke states[J/OL]. Phys. Rev. Lett., 112: 155304. https://link.aps.org/doi/10.1103/PhysRevLett.112.155304.

Luo X Y, Zou Y Q, Wu L N, et al. 2017. Deterministic entanglement generation from driving through quantum phase transitions[J/OL]. Science, 355(6325): 620-623. http://science.sciencemag.org/content/355/6325/620.

Ma J, Yadin B, Girolami D, et al. 2016a. Converting coherence to quantum correlations[J]. Physical Review Letters, 116(16): 160407.

Ma J, Yuan X, Hakande A, et al. 2017. Source-independent quantum random number generation via measuring coherence[J]. arXiv preprint arXiv:1704.06915.

Ma J, Zhou Y, Yuan X, et al. 2018. Operational interpretation of coherence in quantum key distribution [J]. arXiv: 1810.03267.

Ma X s, Guo X, Schuck C, et al. 2014. On-chip interaction-free measurements via the quantum zeno effect[J]. Physical Review A, 90(4): 042109.

Ma X, Yuan X, Cao Z, et al. 2016b. Quantum random number generation[J]. npj Quantum Information, 2: 16021.

Maassen H, Uffink J B M. 1988. Generalized entropic uncertainty relations.[J]. Physical Review Letters, 60(12): 1103-1106.

Markham D, Miyake A, Virmani S. 2007. Entanglement and local information access for graph states [J/OL]. New Journal of Physics, 9(6): 194. http://stacks.iop.org/1367-2630/9/i=6/a=194.

Marvian I, Spekkens R W. 2016a. How to quantify coherence: Distinguishing speakable and unspeakable notions[J/OL]. Phys. Rev. A, 94: 052324. https://link.aps.org/doi/10.1103/PhysRevA.94.052324.

Marvian I, Spekkens R W, Zanardi P. 2016b. Quantum speed limits, coherence, and asymmetry[J/OL]. Phys. Rev. A, 93: 052331. https://link.aps.org/doi/10.1103/PhysRevA.93.052331.

Matera J M, Egloff D, Killoran N, et al. 2016. Coherent control of quantum systems as a resource theory [J/OL]. Quantum Science and Technology, 1(1): 01LT01. http://stacks.iop.org/2058-9565/1/i=1/a=01LT01.

Misra B, Sudarshan E C G. 1977. The zenoąŕs paradox in quantum theory[J/OL]. Journal of Mathematical Physics, 18(4): 756-763. https://doi.org/10.1063/1.523304.

Mitchison G, Massar S. 2001. Absorption-free discrimination between semitransparent objects[J]. Physical Review A, 63(3): 032105.

Modi K, Brodutch A, Cable H, et al. 2012. The classical-quantum boundary for correlations: Discord and related measures[J/OL]. Rev. Mod. Phys., 84: 1655-1707. https://link.aps.org/doi/10.1103/RevModPhys.84.1655.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Monz T, Schindler P, Barreiro J T, et al. 2011. 14-qubit entanglement: Creation and coherence[J/OL]. Phys. Rev. Lett., 106: 130506. https://link.aps.org/doi/10.1103/PhysRevLett.106.130506.

Moroder T, Hyllus P, Tóth G, et al. 2012. Permutationally invariant state reconstruction[J/OL]. New Journal of Physics, 14(10): 105001. http://stacks.iop.org/1367-2630/14/i=10/a=105001.

Napoli C, Bromley T R, Cianciaruso M, et al. 2016. Robustness of coherence: An operational and observable measure of quantum coherence[J/OL]. Phys. Rev. Lett., 116: 150502. https://link.aps.org/doi/10.1103/PhysRevLett.116.150502.

Nielsen M A, Chuang I L. 2010. Quantum computation and quantum information[M]. [S.l.]: Cambridge university press

Orùs R. 2014. A practical introduction to tensor networks: Matrix product states and projected entangled pair states[J/OL]. Annals of Physics, 349: 117 - 158. http://www.sciencedirect.com/science/article/pii/S0003491614001596.

Osterloh A, Siewert J. 2005. Constructing n-qubit entanglement monotones from antilinear operators [J]. Physical Review A, 72(1): 012337.

Paraoanu G. 2006. Interaction-free measurements with superconducting qubits[J]. Physical review letters, 97(18): 180406.

Paris M, Rehacek J e. 2004. Quantum state estimation[J/OL]. in Lect. Notes Phys. https://doi.org/10.1007/b98673.

Perseguers S, Lapeyre G J, Cavalcanti D, et al. 2013. Distribution of entanglement in large-scale quantum networks[J/OL]. Reports on Progress in Physics, 76(9): 096001. https://doi.org/10.1088%2F0034-4885%2F76%2F9%2F096001.

Putnam W P, Yanik M F. 2009. Noninvasive electron microscopy with interaction-free quantum measurements[J]. Physical Review A, 80(4): 040902.

Raussendorf R, Briegel H J. 2001. A one-way quantum computer[J/OL]. Phys. Rev. Lett., 86: 5188-5191. https://link.aps.org/doi/10.1103/PhysRevLett.86.5188.

Raussendorf R, Browne D E, Briegel H J. 2003. Measurement-based quantum computation on cluster states[J/OL]. Phys. Rev. A, 68: 022312. https://link.aps.org/doi/10.1103/PhysRevA.68.022312.

Regula B, Adesso G. 2016. Entanglement quantification made easy: Polynomial measures invariant under convex decomposition[J]. Physical Review Letters, 116(7): 070504.

Renninger M. 1960. Messungen ohne störung des meßobjekts[J]. Zeitschrift für Physik, 158(4): 417-421.

Rossi M, Huber M, BruB D, et al. 2013. Quantum hypergraph states[J/OL]. New Journal of Physics, 15(11): 113022. http://stacks.iop.org/1367-2630/15/i=11/a=113022.

Scarani V, Acín A, Schenck E, et al. 2005. Nonlocality of cluster states of qubits[J/OL]. Phys. Rev. A, 71: 042325. https://link.aps.org/doi/10.1103/PhysRevA.71.042325.

Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. 2009. The security of practical quantum key distribution[J/OL]. Rev. Mod. Phys., 81: 1301-1350. https://link.aps.org/doi/10.1103/RevModPhys.81.1301.

Schlingemann D, Werner R F. 2001. Quantum error-correcting codes associated with graphs[J/OL]. Phys. Rev. A, 65: 012308. https://link.aps.org/doi/10.1103/PhysRevA.65.012308.

邵钰菓2020311340承诺学位论文仅用于个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Schmied R, Bancal J D, Allard B, et al. 2016. Bell correlations in a bose-einstein condensate[J/OL]. Science, 352(6284): 441-444. http://science.sciencemag.org/content/352/6284/441.

Schrödinger E. 1935. Die gegenwärtige situation in der quantenmechanik[J]. Naturwissenschaften, 23(48): 807-812.

Sentís G, Eltschka C, Gühne O, et al. 2016. Quantifying entanglement of maximal dimension in bipartite mixed states[J]. Physical Review Letters, 117(19): 190502.

Shahandeh F, Sperling J, Vogel W. 2014. Structural quantification of entanglement[J/OL]. Phys. Rev. Lett., 113: 260502. https://link.aps.org/doi/10.1103/PhysRevLett.113.260502.

Shor P W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J/OL]. SIAM J. Comput., 26(5): 1484-1509. http://dx.doi.org/10.1137/S0097539795293172.

Shor P W, Preskill J. 2000. Simple proof of security of the bb84 quantum key distribution protocol [J/OL]. Phys. Rev. Lett., 85: 441-444. https://link.aps.org/doi/10.1103/PhysRevLett.85.441.

Siewert J, Eltschka C. 2012. Quantifying tripartite entanglement of three-qubit generalized werner states[J]. Physical Review Letters, 108(23): 230502.

Song C, Xu K, Liu W, et al. 2017. 10-qubit entanglement and parallel logic operations with a superconducting circuit[J/OL]. Phys. Rev. Lett., 119: 180511. https://link.aps.org/doi/10.1103/PhysRevLett.119.180511.

Sørensen A S, Mølmer K. 2001. Entanglement and extreme spin squeezing[J/OL]. Phys. Rev. Lett., 86: 4431-4434. https://link.aps.org/doi/10.1103/PhysRevLett.86.4431.

Streltsov A, Singh U, Dhar H S, et al. 2015. Measuring quantum coherence with entanglement[J/OL]. Phys. Rev. Lett., 115: 020403. https://link.aps.org/doi/10.1103/PhysRevLett.115.020403.

Streltsov A, Adesso G, Plenio M B. 2017a. Colloquium[J/OL]. Rev. Mod. Phys., 89: 041003. https://link.aps.org/doi/10.1103/RevModPhys.89.041003.

Streltsov A, Rana S, Bera M N, et al. 2017b. Towards resource theory of coherence in distributed scenarios[J/OL]. Phys. Rev. X, 7: 011024. https://link.aps.org/doi/10.1103/PhysRevX.7.011024.

Takei N, Sommer C, Genes C, et al. 2016. Direct observation of ultrafast many-body electron dynamics in an ultracold rydberg gas[J/OL]. Nature Communications, 7: 13449 EP -. https://doi.org/10.1038/ncomms13449.

Tang Y L, Yin H L, Zhao Q, et al. 2016. Measurement-device-independent quantum key distribution over untrustful metropolitan network[J/OL]. Phys. Rev. X, 6: 011024. https://link.aps.org/doi/10.1103/PhysRevX.6.011024.

Terhal B M. 2002. Detecting quantum entanglement[J/OL]. Theoretical Computer Science, 287(1): 313 - 335. http://www.sciencedirect.com/science/article/pii/S0304397502001391.

Terhal B M, Vollbrecht K G H. 2000. Entanglement of formation for isotropic states[J]. Physical Review Letters, 85(12): 2625.

Thomas S, Kohstall C, Kruit P, et al. 2014. Semitransparency in interaction-free measurements[J]. Physical Review A, 90(5): 053840.

Tossavainen T. 2006. On the zeros of finite sums of exponential functions[J]. Australian Mathematical Society Gazette, 33(1): 47.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Tóth G, Wieczorek W, Gross D, et al. 2010. Permutationally invariant quantum tomography[J/OL]. Phys. Rev. Lett., 105: 250403. https://link.aps.org/doi/10.1103/PhysRevLett.105.250403.

Tóth G, Gühne O. 2005. Detecting genuine multipartite entanglement with two local measurements [J/OL]. Phys. Rev. Lett., 94: 060501. https://link.aps.org/doi/10.1103/PhysRevLett.94.060501.

Tsegaye T, Goobar E, Karlsson A, et al. 1998. Efficient interaction-free measurements in a high-finesse interferometer[J]. Physical Review A, 57(5): 3987.

Uhlmann A. 1998. Entropy and optimal decompositions of states relative to a maximal commutative subalgebra[J]. Open Systems & Information Dynamics, 5(3): 209-228.

Vaidman L. 2003. The meaning of the interaction-free measurements[J]. Foundations of Physics, 33 (3): 491-510.

Van den Nest M, Dehaene J, De Moor B. 2004. Graphical description of the action of local clifford transformations on graph states[J/OL]. Phys. Rev. A, 69: 022316. https://link.aps.org/doi/10.1103/PhysRevA.69.022316.

Verstraete F, Dehaene J, De Moor B. 2003. Normal forms and entanglement measures for multipartite quantum states[J]. Physical Review A, 68(1): 012103.

Vogel K, Risken H. 1989. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase[J/OL]. Phys. Rev. A, 40: 2847-2849. https://link.aps.org/doi/10.1103/PhysRevA.40.2847.

Vollbrecht K G H, Werner R F. 2001. Entanglement measures under symmetry[J]. Physical Review A, 64(6): 062307.

Volz J, Gehr R, Dubois G, et al. 2011. Measurement of the internal state of a single atom without energy exchange[J]. Nature, 475(7355): 210-213.

Wang X L, Chen L K, Li W, et al. 2016. Experimental ten-photon entanglement[J/OL]. Phys. Rev. Lett., 117: 210502. https://link.aps.org/doi/10.1103/PhysRevLett.117.210502.

Watrous J. 2011. Theory of quantum information[J]. University of Waterloo Fall, 128.

Wei T C. 2010. Exchange symmetry and global entanglement and full separability[J/OL]. Phys. Rev. A, 81: 054102. https://link.aps.org/doi/10.1103/PhysRevA.81.054102.

Wilde M M. 2013. Quantum information theory[M]. [S.l.]: Cambridge University Press

Wineland D J, Bollinger J J, Itano W M, et al. 1992. Spin squeezing and reduced quantum noise in spectroscopy[J/OL]. Phys. Rev. A, 46: R6797-R6800. https://link.aps.org/doi/10.1103/PhysRevA.46.R6797.

Wineland D J, Bollinger J J, Itano W M, et al. 1994. Squeezed atomic states and projection noise in spectroscopy[J/OL]. Phys. Rev. A, 50: 67-88. https://link.aps.org/doi/10.1103/PhysRevA.50.67.

Winter A, Yang D. 2016. Operational resource theory of coherence[J/OL]. Phys. Rev. Lett., 116: 120404. https://link.aps.org/doi/10.1103/PhysRevLett.116.120404.

Wölk S, Gühne O. 2016. Characterizing the width of entanglement[J/OL]. New Journal of Physics, 18(12): 123024. http://stacks.iop.org/1367-2630/18/i=12/a=123024.

Wootters W K. 1998. Entanglement of formation of an arbitrary state of two qubits[J]. Physical Review Letters, 80(10): 2245.

Yao Y, Xiao X, Ge L, et al. 2015. Quantum coherence in multipartite systems[J/OL]. Phys. Rev. A, 92: 022112. https://link.aps.org/doi/10.1103/PhysRevA.92.022112.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Yin J, Cao Y, Li Y H, et al. 2017. Satellite-to-ground entanglement-based quantum key distribution[J/OL]. Phys. Rev. Lett., 119: 200501. https://link.aps.org/doi/10.1103/PhysRevLett.119.200501.

Yu X D, Zhang D J, Xu G, et al. 2016. Alternative framework for quantifying coherence[J]. Physical Review A, 94(6): 060302.

Yuan X, Zhou H, Cao Z, et al. 2015. Intrinsic randomness as a measure of quantum coherence[J/OL]. Phys. Rev. A, 92: 022124. https://link.aps.org/doi/10.1103/PhysRevA.92.022124.

Yuan X, Zhao Q, Girolami D, et al. 2016. Interplay between local quantum randomness and non-local information access[J]. arXiv preprint arXiv:1605.07818.

Zeng B, Chen X, Zhou D L, et al. 2015. Quantum information meets quantum matter – from quantum entanglement to topological phase in many-body systems[J]. arXiv:1508.02595.

Zhao Q, Wang G, Yuan X, et al. 2019. Efficient and robust detection of multipartite greenberger-horne-zeilinger-like states[J]. arXiv:1902.07869.

Zhao Y, Fung C H F, Qi B, et al. 2008. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. Physical Review A, 78(4): 042333.

Zhong H S, Li Y, Li W, et al. 2018. 12-photon entanglement and scalable scattershot boson sampling with optimal entangled-photon pairs from parametric down-conversion[J/OL]. Phys. Rev. Lett., 121: 250505. https://link.aps.org/doi/10.1103/PhysRevLett.121.250505.

Zhou Y, Yung M H. 2017a. Interaction-free measurement as quantum channel discrimination[J/OL]. Phys. Rev. A, 96: 062129. https://link.aps.org/doi/10.1103/PhysRevA.96.062129.

Zhou Y, Zhao Q, Yuan X, et al. 2017b. Polynomial measure of coherence[J/OL]. New Journal of Physics, 19(12): 123033. https://doi.org/10.1088%2F1367-2630%2Faa91fa.

Zhou Y, Guo C, Ma X. 2019a. Entanglement detection under coherent noise[J]. under preparation.

Zhou Y, Guo C, Ma X. 2019b. Decomposition of symmetric multipartite observable[J]. arXiv:1902.07496.

Zhou Y, Zhao Q, Yuan X, et al. 2019c. Efficient detection of multipartite entanglement structure[J]. arXiv:1904.05001.

Zilberberg O, Romito A, Gefen Y. 2016. Many-body manifestation of interaction-free measurement: The elitzur-vaidman bomb[J/OL]. Phys. Rev. B, 93: 115411. http://link.aps.org/doi/10.1103/PhysRevB.93.115411.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Acknowledgements

衷心感谢我的导师马雄峰教授对本人的精心指导。他对于生活和科研乐观积极的态度对我产生了深远的影响，从他那里我学到了很多做人和做科研的道理。感谢我在博士学习期间课题组内的成员：袁骁，张振，马家俊，赵琦，周泓伊，曾培，张行健，张艺泓。我的成长离不开你们的帮助。感谢我的合作者，Aliocia Hamma 教授，翁文康教授，郭铖浩同学，与你们的讨论与合作让我收获良多。我还要感谢国内外学术访问期间热心招待我的老师和同学们。其中包括意大利卡塔尼亚大学 Luigi Amico 教授，日本东京大学的 Mio Murao 教授，以及国内中国科学技术大学的苑震生教授和山东大学的仝殿民教授。感谢交叉信息研究院的全体老师和同学对我帮助和鼓励。最后感谢我的父母和女友，你们对我的关爱让我可以踏实地去开展科学研究。本课题承蒙国家自然科学基金资助，特此致谢。

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

声 明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签 名：____________ 日 期：____________

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Appendix A Proofs of polynomial measure of coherence

This section contains proofs of polynomial measure of coherence in Chapter 3.

A.1 Proof of Theorem 3.1 for $d = 3$

In the main part, Theorem 3.1 for the case of $d \geq 4$ has been proved. Here we prove the $d = 3$ case. First, a Lemma that is an extension of Lemma 3.1 follows.

Lemma A.1： For any polynomial coherence measure $C_p(|\psi\rangle)$, and any two pure quantum states $|\psi_1\rangle, |\psi_2\rangle$ satisfying $|\langle\psi_2|\psi_1\rangle| < 1$, there is at least one zero-coherence state in the superposition space of them.

Proof. Like in Lemma.3.1, without loss of generality, we just need to consider the scenario of power $m = 1$. First, if $C_p(|\psi_2\rangle) = 0$, the Lemma holds automatically. So we focus on the $C_p(|\psi_2\rangle) \neq 0$ case in the following.

Let us denote $\langle\psi_1|\psi_2\rangle = ke^{i\theta}$ with $k < 1$. Then, after ignoring the global phase, any superposition state of $|\psi_1\rangle$ and $|\psi_2\rangle$ can be represented by

$$|\psi\rangle = \frac{|\psi_1\rangle + \omega|\psi_2\rangle}{Z(\omega)}, \tag{A-1}$$

where ω is a complex number and the normalization factor $Z(\omega) = \big||\psi_1\rangle + \omega|\psi_2\rangle\big| = \sqrt{1 + |\omega|^2 + 2|\omega|k\cos(\theta + \theta')}$ with $\omega = |\omega|e^{i\theta'}$.

Similar to Lemma. 3.1, we can factorize $C_p(|\psi\rangle)$ as

$$\begin{aligned} C_p(|\psi\rangle) &= \left|P_h\left(\frac{|\psi_1\rangle + \omega|\psi_2\rangle}{Z(\omega)}\right)\right| \\ &= \frac{1}{Z(\omega)^h}|P_h(|\psi_1\rangle + \omega|\psi_2\rangle)| \\ &= \frac{A'}{Z(\omega)^h}\Pi_{i=1}^h|\omega - z_i|, \end{aligned} \tag{A-2}$$

where A' is a constant and $z_i (i = 1, 2, \cdots, h)$ are the roots of the polynomial function $P_h(|\psi_1\rangle + \omega|\psi_2\rangle)$. Thus we can find at least one root in this $C_p(|\psi_2\rangle) \neq 0$ case, or equivalently, a zero-coherence state. ■

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

With the help of Lemma.A.1, now we prove Th. 3.1 for $d = 3$ case. First, similar to the main part, we can choose two states with non-zero coherence as,

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle). \end{aligned} \tag{A-3}$$

Even though these two states share overlap with each other, any superposition state $\alpha|\psi_1\rangle + \beta|\psi_2\rangle$ should not equal to the pure state $|i\rangle\,(i = 1, 2, \cdots, d)$ in the computational basis. As required by the criterion $(C1')$ in Table. 2.1, $|i\rangle\,(i = 1, 2, ..., d)$ are the only zero-coherence pure state. Thus, $C_p(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) > 0$. Nonetheless, it is contradict to Lemma. A.1. Consequently, there is no polynomial coherence measure satisfying the criterion $(C1')$ for $d = 3$ case.

A.2 Proof for $k = 0$ in Eq. (3-19)

In the main part, the coherence measure for the superposition state of $|\psi_1\rangle \in \mathcal{H}_{d_1}$ and $|\psi_2\rangle \in \mathcal{H}_{d_2}$ shows,

$$C_p(|\psi\rangle) = k(1 + |\omega|^2)^{-h/2}.$$

If $k > 0$, the coherence measure strictly decreases with the increasing of $|\omega|$. That is, for any superposition state $|\psi\rangle = (|\psi_1\rangle + \omega|\psi_2\rangle)/\sqrt{1 + |\omega|^2}$ with $|\omega| > 0$, we have $C_p(|\psi\rangle) < C_p(|\psi_1\rangle)$. We denote the state coefficients by $\alpha = (1 + |\omega|^2)^{-1/2}$ and $\beta = \omega(1+|\omega|^2)^{-1/2}$ here. In the following, we show that there exists a state $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$ with $\alpha < 1$ (or equivalently $|\omega| > 0$), such that $C_p(|\psi\rangle) \geq C_p(|\psi_1\rangle)$. As a result, this contradiction leads to $k = 0$.

From Refs. [Du et al. (2015a); Winter et al. (2016)], we know that $|\Psi\rangle = \sum_{i=1}^{d} \Psi_i |i\rangle$ can transform to $|\Phi\rangle = \sum_{i=1}^{d} \Phi_i |i\rangle$ via incoherent operation, if $(|\Psi_1|^2, ..., |\Psi_d|^2)^t$ is majorized by $(|\Phi_1|^2, ..., |\Phi_d|^2)^t$. Then combing the criteria $(C2)$ and $(C3)$ in Table. 2.1, we obtain that the coherence measure is non-increasing after incoherent operation. Thus, $C(|\Psi\rangle) \geq C(|\Phi\rangle)$ for any coherence measure.

In our case, first, we denote $|\psi_1\rangle = \sum_{i=1}^{d_1} a_i |i\rangle$ with $\forall i, |a_i| > 0$. And choose $|\psi_2\rangle = \frac{1}{\sqrt{d_2}} \sum_{i=d_1+1}^{d} |i\rangle$. Then we can build a state $|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle$ that satisfies $\alpha < 1$ and $C_p(|\psi\rangle) \geq C_p(|\psi_1\rangle)$, with the help of the aforementioned majorization condition.

邵钰莱2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

To be specific, if α satisfying,

$$\alpha^2|a_j|^2 \geq \beta^2/d_2, \tag{A-4}$$

where $|a_j|^2$ is the minimal value in $\{|a_i|^2\}$, then $(\alpha^2|a_1|^2, \alpha^2|a_2|^2, ..., \alpha^2|a_{d_1}|^2, \beta^2/d_2, ..., \beta^2/d_2)^t$ is majorized by $(|a_1|^2, |a_2|^2, ..., |a_{d_1}|^2, 0, ..., 0)^t$. Thus, $C_p(|\psi\rangle) \geq C_p(|\psi_1\rangle)$. In fact, $\alpha = (d_2|a_j|^2 + 1)^{-1/2} < 1$, when the inequality is saturated in Eq. A-4.

A.3 Derivation of Eq. (3-28)

As mentioned in the main part, the constraint for the pure state $|\psi\rangle = \sum_i a_i |i\rangle$ in Eq. (3-27) is the overlap $K = |\langle\Psi_d|\psi\rangle|^2$, i.e.,

$$|\sum_i a_i| = \sqrt{dK}, \tag{A-5}$$

and the coefficients a_i of the state should also satisfy the normalization condition,

$$\sum_i |a_i|^2 = 1. \tag{A-6}$$

When $0 \leq K \leq \frac{d-1}{d}$, we can always set one of the coefficients $a_j = 0$ with $j \in \{i\}$, and let the corresponding C_G equal to 0. Thus $\bar{C}_G(K) = 0$ in this K domain.

On the other hand, all the coefficients $a_i \neq 0$, when $\frac{d-1}{d} \leq K \leq 1$. In this K domain, we should minimize $C_G(|\psi\rangle) = d(\Pi_i|a_i|)^{\frac{2}{d}}$ under the constraints in Eq. (A-5) and Eq. (A-6). Note that $\sum_i |a_i| \geq |\sum_i a_i|$ and the equality can be reached when the coefficients share the same phase. Thus the constraint in Eq. (A-5) can be replaced by,

$$\sum_i |a_i| = \sqrt{dK}. \tag{A-7}$$

In fact, the function optimized here is the same to the one in Ref. [Sentís et al. (2016)] for the G-concurrence, after substituting the Schmidt coefficients for the state coefficients $|a_i|$. Thus, utilizing the same Lagrange multipliers in Supplemental Material of Ref. [Sentís et al. (2016)], we can obtain Eq. (3-28) in the main part. And we can show that $\bar{C}_G(K)$ is a concave function, when $\frac{d-1}{d} \leq K \leq 1$, by directly following the derivation there.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Appendix B Details of decomposition of symmetric multipartite observable

This section contains details of decomposition of symmetric multipartite observable in Chapter 4.

B.1 Proof of Theorem 4.1

Here we give the proof of Theorem 4.1 in the main part, which constructs a set of product-state basis for symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$, that is,

$$\mathcal{B} = \left\{ |\Phi_{\vec{j}}\rangle = \left(a_{0,j_0} |0\rangle + a_{1,j_1} |1\rangle + \cdots + a_{d-1,j_{d-1}} |d-1\rangle \right)^{\otimes N} \right\}, \tag{B-1}$$

where $\sum_{k=0}^{d-1} j_k = N$ and the coefficients a_{k,j_k} are selected from any matrix denoted by $A_{d,N}$ satisfying Eq. (4-6). Since $a_{0,j_0} = 1$ for any j_0, the basis set in Eq. (B-1) becomes,

$$\mathcal{B} = \left\{ |\Phi_{\vec{j}}\rangle = \left(|0\rangle + a_{1,j_1} |1\rangle + \cdots + a_{d-1,j_{d-1}} |d-1\rangle \right)^{\otimes N} \right\}, \tag{B-2}$$

and the constraint of j_k can be replaced with $\sum_{k=1}^{d-1} j_k \leq N$.

On the other hand, as shown in Eq. (4-4), there is another set of orthogonal (unnormalized) basis of $\mathrm{Sym}_N(\mathcal{H}_d)$ showing [Harrow (2013)],

$$\left\{ |\Psi_{\vec{i}}\rangle = \sum_{\pi} |0\rangle^{\otimes i_0} |1\rangle^{\otimes i_1} \cdots |d-1\rangle^{\otimes i_{d-1}} \right\}, \tag{B-3}$$

where $\vec{i} = (i_0, i_1, \cdots, i_{d-1})$ a d-dimensional vector, with $i_k \in \mathbb{N}$ and $\sum_{k=0}^{d-1} i_k = N$. It is the generalization of Eq. (4-9) from qubit to qudit case.

The number of vectors in $\mathcal{B}$ is $D_S = \binom{N+d-1}{d-1} = \frac{(N+d-1)!}{N!(d-1)!}$, the dimension of $\mathrm{Sym}_N(\mathcal{H}_d)$. Thus one only needs to show that the vectors in $\mathcal{B}$ are linearly independent. Here, we write $|\Phi_{\vec{j}}\rangle$ in the $\{|\Psi_{\vec{i}}\rangle\}$ basis, and the result shows

$$|\Phi_{\vec{j}}\rangle = \sum_{\vec{i}} \prod_{k=1}^{d-1} a_{k,j_k}^{i_k} |\Psi_{\vec{i}}\rangle . \tag{B-4}$$

The corresponding coefficient matrix of all $\{|\Phi_{\vec{j}}\rangle\}$ shows,

$$M_{\vec{i},\vec{j}}^{A_{d,n}} = \langle \Psi_{\vec{i}} | \Phi_{\vec{j}} \rangle = \prod_{k=1}^{d-1} a_{k,j_k}^{i_k}, \tag{B-5}$$

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

where each column vector is the coefficient of $|\Phi_{\vec{j}}\rangle$. We say $A_{d,N}$ *generating* $M^{A_{d,N}}$.

In the following we show that the determinant of $M^{A_{d,N}}$ is non-zero, by utilizing induction method on both d (the local dimension) and N (the qudit number). First, when $d = 1$ or $N = 1$, it is not hard to check that $\{|\Phi_{\vec{j}}\rangle\}$ are linearly independent and form a set of basis.

For general d and N, we do the following row transformation on $M^{A_{d,N}}$: for the row index $\vec{i}$ satisfying $i_1 = 0$, keep these rows unchanged; for the other ones with $1 \leq i_1 \leq N$, we find the corresponding row with index $\vec{i'} = (i_0 + 1, i_1 - 1, i_2, i_3, \cdots, i_{d-1})$, and subtract $a_{1,0}$ multiplying this row $\vec{i'}$. Note that we do this transformation in order from $i_1 = N$ to $i_1 = 1$, and the resulting matrix shows,

$$M'_{\vec{i},\vec{j}} = \begin{cases} \prod_{k=1}^{d-1} a_{k,j_k}^{i_k}, & i_1 = 0 \\ \prod_{k=1}^{d-1} a_{k,j_k}^{i_k} - a_{1,0} \prod_{k=1}^{d-1} a_{k,j_k}^{i_k-\delta(k-1)} & \\ = (a_{1,j_1} - a_{1,0}) \prod_{k=1}^{d-1} a_{k,j_k}^{i_k-\delta(k-1)}, & 1 \leq i_1 \leq N \end{cases} \tag{B-6}$$

where the function $\delta(k-1) = 1$ as $k = 1$, otherwise it equals to zero.

From Eq. (B-6), one can see that for the matrix elements $M_{\vec{i},\vec{j}}$ satisfying $1 \leq i_1 \leq N$ and $j_1 = 0$ equal to zero. That is, $M'_{\vec{i},\vec{j}}$ is a upper triangular block matrix, i.e.,

$$M'_{\vec{i},\vec{j}} = \begin{pmatrix} M^1_{\vec{i},\vec{j}} & M_\neg \\ 0 & M^2_{\vec{i},\vec{j}} \end{pmatrix}, \tag{B-7}$$

where $M^1_{\vec{i},\vec{j}}$ ($M^2_{\vec{i},\vec{j}}$) is square matrix which is located in the rows $i_1 = (>)0$ and columns $j_1 = (>)0$, and $M_\neg$ is the off-diagonal part. In the following, we show that the determinants of $M^1_{\vec{i},\vec{j}}$ and $M^2_{\vec{i},\vec{j}}$ both are non-zero by induction.

Since $i_1 = j_1 = 0$, $M^1_{\vec{i},\vec{j}}$ is generated by the following matrix,

$$A^1_{d-1,N} = \left\{ a^1_{k,j} = a_{k+1,j} \middle| k \in \{1, \cdots, d-2\}, j \in \{0, 1, \cdots, N\} \right\}. \tag{B-8}$$

Actually, the matrix $A^1_{d-1,N}$ is related to $d-1$ local dimension and N-fold tensor. By induction principle, we can get that $\det(M^1_{\vec{i},\vec{j}}) \neq 0$.

For the other submatrix $M^2_{\vec{i},\vec{j}}$ with $i_1, j_1 \geq 1$ shown in Eq. (B-6), the pre-coefficient $(a_{1,j_1} - a_{1,0}) \neq 0$, and it keeps the same in the same column. Since we only care about the

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

non-zero property of $\det(M^2_{\vec{i},\vec{j}})$, we can eliminate these unimportant pre-coefficients and check the determinant of the remaining matrix,

$$M^3_{\vec{i},\vec{j}} = \prod_{k=1}^{d-1} a_{k,j_k}^{i_k-\delta(k-1)}. \tag{B-9}$$

Denotes a new $i'_1 = i_1 - 1$ and $i'_k = i_k$ for $k \neq 1$, then one has $\sum_k i'_k = N - 1$. In this way, it is not hard to see that $M^3_{\vec{i},\vec{j}}$ can be generated by the following matrix,

$$A^3_{d,N-1} = \left\{ a^3_{k,j} \middle| k \in \{1, \cdots, d-1\}, j \in \{0, 1, \cdots, N-1\} \right\}, \tag{B-10}$$

where

$$a^3_{k,j} = \begin{cases} a_{k,j+1}, k = 1, \\ a_{k,j}, k = 2, \cdots, d-1. \end{cases} \tag{B-11}$$

In fact, $A^3_{d,N-1}$ is related to d local dimension and $(N-1)$-fold tensor. Again by induction principle, we have that $\det(M^3_{\vec{i},\vec{j}}) \neq 0$, and thus $\det(M^2_{\vec{i},\vec{j}}) \neq 0$.

Consequently, $\det(M^{A_{d,n}}) = \det(M^1_{\vec{i},\vec{j}}) \det(M^2_{\vec{i},\vec{j}}) \neq 0$, and $\{|\Phi_{\vec{j}}\rangle\}$ is a set of basis of the symmetric subspace $\mathrm{Sym}_N(\mathcal{H}_d)$.

B.2 Decomposition of PI state in the product-form basis

In this section, we show explicitly how to efficiently decompose a general PI state in the product-form basis.

The product operators in $\mathcal{B}_o$ in Eq. (4-17) form a basis of the operator symmetric subspace $\mathrm{Sym}_N(G_1)$,

$$\mathcal{B}_o = \left\{ O_{\vec{\alpha}} = (a_i \mathbb{I} + b_j \sigma_X + c_k \sigma_Y + \sigma_Z)^{\otimes N} \middle| 0 \leq i, j, k \leq N, \ i + j + k \leq N \right\}. \tag{B-12}$$

where we denote the product operator as $O_{\vec{\alpha}} = (a_i \mathbb{I} + b_j \sigma_X + c_k \sigma_Y + \sigma_Z)^{\otimes N}$, with $\vec{\alpha} = \{i, j, k\}$ being a three-dimensional vector as the index. In general, these linearly independent operators $O_{\vec{\alpha}}$ may be not orthogonal. Meanwhile, there is another orthogonal basis of $\mathrm{Sym}_N(G_1)$ shown in Eq. (4-16),

$$M_{\vec{\beta}} \doteq M_{i,j,k} = \sum_{\pi} \mathbb{I}^{\otimes i} \otimes \sigma_X^{\otimes j} \otimes \sigma_Y^{\otimes k} \otimes \sigma_Z^{\otimes (N-i-j-k)}. \tag{B-13}$$

where $\vec{\beta} = \{i, j, k\}$ also denotes a three-dimensional vector as the index of $M_{i,j,k}$.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

We show in the following how to express a general PI state Ψ^{PI} in the product-form basis $\{O_{\vec{\alpha}}\}$, i.e.,

$$\Psi^{PI} = \sum_{\vec{\alpha}} \gamma_{\vec{\alpha}} O_{\vec{\alpha}}, \tag{B-14}$$

where $\gamma_{\vec{\alpha}}$ are real coefficients that we need to figure out.

Our strategy is as follows. First, decompose the PI state on the orthogonal basis $\{M_{\vec{\beta}}\}$ as,

$$\Psi^{PI} = \sum_{\vec{\beta}} \gamma'_{\vec{\beta}} M_{\vec{\beta}}. \tag{B-15}$$

Since the basis operators $M_{\vec{\beta}}$ are orthogonal, the coefficient can be efficiently obtained,

$$\gamma'_{\vec{\beta}} = c_{\vec{\beta}} \mathrm{Tr}(M_{\vec{\beta}} \Psi^{PI}) \tag{B-16}$$

where $c_{\vec{\beta}} = \frac{i!j!k!(N-i-j-k)!}{2^N N!}$ is the normalization constant.

Second, do the basis transformation between $M_{\vec{\beta}}$ and $O_{\vec{\alpha}}$. The elements of the basis transformation matrix can be obtained by expressing $O_{\vec{\alpha}}$ on $M_{\vec{\beta}}$, that is,

$$\Omega_{\vec{\beta},\vec{\alpha}} = c_{\vec{\beta}} \mathrm{Tr}(M_{\vec{\beta}} O_{\vec{\alpha}}) \tag{B-17}$$

As a result,

$$\begin{aligned}
\Psi^{PI} &= \sum_{\vec{\alpha}} \gamma_{\vec{\alpha}} O_{\vec{\alpha}} \\
&= \sum_{\vec{\alpha},\vec{\beta}} \gamma_{\vec{\alpha}} \Omega_{\vec{\beta},\vec{\alpha}} M_{\vec{\beta}} \\
&= \sum_{\vec{\beta}} \gamma'_{\vec{\beta}} M_{\vec{\beta}}.
\end{aligned} \tag{B-18}$$

Thus, one has $\gamma'_{\vec{\beta}} = \sum_{\vec{\alpha}} \Omega_{\vec{\beta},\vec{\alpha}} \gamma_{\vec{\alpha}}$ and $\gamma_{\vec{\alpha}} = \Omega^{-1} \gamma'_{\vec{\beta}}$. Note that the inverse of the matrix Ω can be evaluated efficiently by numerical method, since the dimension of the matrix is $\binom{N+2}{2}$.

As a result, by measuring the expectation values of product operators $\langle O_{\vec{\alpha}} \rangle$, one can get the fidelity $\langle \Psi^{PI} \rangle = \sum_{\vec{\alpha}} \gamma_{\vec{\alpha}} \langle O_{\vec{\alpha}} \rangle$ with respective to any PI state Ψ^{PI}, by only post-processing the measurement results.

Moreover, as shown in Eq. (4-16) in the main part, one can choose other possible product-from basis by changing the parameters of the local operators that satisfy Eq. (4-6). Different product-from bases may show different noise tolerances in practical application. For instance, there is some basis choice, where two product operators are too “close" (even

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

though they are linearly independent), such that they return almost the same result under some measurement imperfection. Thus, we suggest the following selection method, which makes the basis operators distribute as "evenly" as possible. One chooses the coefficients in Eq. (B-12) as follows. $a_i = \tan\theta_i$ with $\theta_i = \frac{i\pi}{N+1}$, $b_j = \tan\theta_j$ with $\theta_j = \frac{j\pi}{N+1}$, and $c_k = \tan\theta_k$ with $\theta_k = \frac{k\pi}{N+1}$.

Finally, we would like to remak that the method shown above can also be applied to decompose general symmetric operators directly, which may be useful in other related problems.

B.3 Proof of Theorem. 4.4 when $b_i = 0$ or $c_i = 0$ in Eq. (4-41)

Here we give the proof of Theorem 4.4 in the case where $b_i = 0$ or $c_i = 0$ in Eq. (4-41). Remember that in the main part, we project the operator GHZ_N and O on a specific subspace in Eq. (4-38), and the projection results are respectively

$$v_{GHZ} = \frac{1}{2^N}(1, -1, 1, \cdots, (-1)^{\lfloor N/2 \rfloor}), \tag{B-19}$$

$$v_O = \sum_{i=1}^{n_A} \alpha_{i0}(b_i^N, b_i^{N-2}c_i^2, \cdots, b_i^{N-2\lfloor N/2 \rfloor}c_i^{2\lfloor N/2 \rfloor}). \tag{B-20}$$

Then we define a function $g(x)$ in Eq. (4-43) which is a summation of several exponential functions, and use the root property of it to bound the number of LMSs.

Here we consider the general case where $b_i = 0$ or $c_i = 0$. Let S denote the set of i with both b_i and c_i not equal to 0, and define $\beta_i = (c_i/b_i)^2$ only on S. Let S_b denote the set of i with $c_i = 0$, $b_i \neq 0$ and let S_c denote the set of i with $b_i = 0$, $c_i \neq 0$. Then v_O can be written as follows,

$$v_O = \sum_{i \in S} \alpha_i(1, \beta_i \cdots, \beta_i^{\lfloor N/2 \rfloor}) + (\alpha_b, 0, \cdots, 0) + (0, \cdots, 0, \alpha_c), \tag{B-21}$$

where $\alpha_i = \alpha_{i0}b_i^N$, $\alpha_b = \sum_{i \in S_b} \alpha_{i0}b_i^N$ and $\alpha_c = \sum_{i \in S_c} \alpha_{i0}b_i^{N-2\lfloor N/2 \rfloor}c_i^{2\lfloor N/2 \rfloor}$. It is clear that

$$n_A \geq |S| + |S_b| + |S_c|. \tag{B-22}$$

And we define $g(x)$ of the set S as,

$$g(x) = \sum_{i \in S} \alpha_i \beta_i^x. \tag{B-23}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Since $v_O = v_G$, $g(0) = 1 - \alpha_b$, $g(1) = -1$, $\cdots$, $g(\lfloor N/2 \rfloor) = (-1)^{\lfloor N/2 \rfloor} - \alpha_c$. Because the continuity of $g(x)$, there is at least one root of $g(x)$ in each of the intervals $(1, 2)$, $(2, 3)$, $\cdots$, $(\lfloor N/2 \rfloor - 2, \lfloor N/2 \rfloor - 1)$, which means $\lfloor N/2 \rfloor - 2$ roots in total. If $\alpha_b = 0$, there is at least another root in $(0, 1)$. Similarly, if $\alpha_c = 0$, there is at least another root in $(\lfloor N/2 \rfloor - 1, \lfloor N/2 \rfloor)$.

Therefore, the number of roots of $g(x)$ is at least

$$\begin{aligned} &\lfloor N/2 \rfloor - 2 + I(\alpha_b = 0) + I(\alpha_c = 0) \\ =&\lfloor N/2 \rfloor - I(\alpha_b \neq 0) - I(\alpha_c \neq 0) \\ \geq&\lfloor N/2 \rfloor - |S_b| - |S_c|, \end{aligned} \tag{B-24}$$

where $I(x)$ denote that function that $I(x) = 0/1$ when x is ture/false.

Then apply Lemma 4.1 to $g(x)$, we get $|S| - 1 \geq \lfloor N/2 \rfloor - |S_b| - |S_c|$. Combine this with (B-22), one has $n_A \geq \lceil \frac{N+1}{2} \rceil$.

B.4 Proof of Theorem 4.5

Here we give the proof of Theorem 4.5. As mentioned in the main part, we find a subspace where $D_{N,m}$ has zero projection, and at the same time show that one needs at least $N - 2m + 1$ LMSs to make the projection also to be zero.

As in the GHZ state case, suppose the optimal LMSs are

$$\mathcal{A} = \{A_i^{\otimes N} = (b_i \sigma_X + c_i \sigma_Y + d_i \sigma_Z)^{\otimes N} | i = 1, 2, \cdots, n_A\}. \tag{B-25}$$

The final operator constructed from $\mathcal{A}$ is denoted by O,

$$O = \sum_{i=1}^{n_A} \sum_{j=1}^{N} \alpha_{ij} \sum_{\pi} \mathbb{I}^{\otimes j} A_i^{\otimes N-j}, \tag{B-26}$$

and it is assumed that $O = D_{N,m}$.

As shown in Eqs. (4-23), (4-24) and (4-25) in the main part, $D_{N,m}$ can be decomposed as,

$$D_{N,m} = \frac{1}{\binom{N}{m}} \sum_{t=0}^{m} \Theta_t, \tag{B-27}$$

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

with

$$
\begin{aligned}
\Theta_t &= \sum_{\pi} (\frac{\mathbb{I}-\sigma_Z}{2})^{\otimes m-t} \otimes \chi_t \otimes (\frac{\mathbb{I}+\sigma_Z}{2})^{\otimes N-m-t}, \\
\chi_t &= \sum_{l=0}^{2t} \sum_{\pi} \alpha_{t,l} \sigma_X^{\otimes l} \sigma_Y^{\otimes (2t-l)}.
\end{aligned}
\tag{B-28}
$$

It is not hard to see that there are at most $2m$ times of σ_X and σ_Y in the decomposition, thus $D_{N,m}$ lies in the subspace, $\mathrm{span}\{M_{i,j,k} | 0 \le j+k \le 2m\}$, where $M_{i,j,k}$ are defined in (4-14).

For the constructed operator O, there should be some operator A_i satisfying $b_i \neq 0$ in the LMSs in Eq. (B-25), otherwise there will be no σ_X term in O. If all the operator A_i with $b_i \neq 0$ satisfy $d_i = 0$, $O \neq D_{N,m}$, since there are terms like $\sum_\pi \sigma_X^{\otimes 2t} \sigma_Z^{\otimes N-2t}$ in $D_{N,m}$.

Now consider the following subspace

$$
V_1 = \mathrm{span}\{M_{0,j,0} | 2m+1 \le j \le N\}, \tag{B-29}
$$

where $D_{N,m}$ has zero component on. For O, only the following terms could have non-zero projection on this subspace,

$$
\sum_{i=1}^{n_A} \alpha_{i0} A_i^{\otimes N}, \tag{B-30}
$$

and we write the projection on $M_{0,j,0}$ in Eq. (B-29) in the vector form as,

$$
v_O = \sum_{i=1}^{n_A} \alpha_{i0} (b_i^{2m+1} d_i^{N-2m-1}, b_i^{2m+2} d_i^{N-2m-2}, \cdots, b_i^N), \tag{B-31}
$$

where we consider $b_i \neq 0$ otherwise it contribute nothing to the summation. On account of $O = D_{N,m}$, this projection result should also be zero, i.e., $v_O = \vec{0}$.

First, we focus on the case where all $d_i \neq 0$, denote $\beta_i = b_i/d_i$. And v_O can be written as,

$$
v_O = \sum_i \alpha_i (1, \beta_i, \cdots, \beta_i^{N-2m-1})^T = \vec{0}. \tag{B-32}
$$

where α_i is the summation of all the corresponding coefficients sharing same β_i,

$$
\alpha_i = \sum_{i':\beta_{i'}=\beta_i} \alpha_{i'0} b_{i'}^{2m+1} d_{i'}^{N-2m-1}, \tag{B-33}
$$

In fact, there is at least one $\alpha_i \neq 0$. To illustrate this, let us consider another subspace,

$$
V_2 = \mathrm{span}\{M_{0,j,0} | 1 \le j \le 2m\}. \tag{B-34}
$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

It is clear that the projection of $D_{N,m}$ on V_2 is nonzero. For example, the terms like $\sum_\pi \sigma_X^{\otimes 2t}\sigma_Z^{\otimes N-2t}$ are the basis of it. In the meantime, the projection of O on V_2 is,

$$v_O' = \sum_i \alpha_i(\beta_i^{-2m}, \beta_i^{-2m+1} \cdots, \beta_i^{-1})^T. \tag{B-35}$$

Consequently, there is at least one $\alpha_i \neq 0$, otherwise $v_O' = \vec{0}$, which is in contradiction to $O = D_{N,m}$.

Denote the number of different β_i as n_β. Then Eq. (B-32) means that an $(N-2m)\times n_\beta$ Vandermonde matrix multiplies a non-zero vector $\{\alpha_i\}$. Due to the non-singularity of Vandermonde matrix, the result can be $\vec{0}$, only if $n_\beta > N-2m$. As a result, the number of measurement setting is lower bounded by $n_A \geq n_\beta > N-2m$.

For the case where there are LMSs with $d_i = 0$, denote the set of these LMSs as S, the projection in Eq. (B-31) shows

$$\sum_{i\in S} \alpha_{i0} b_j^N (0, 0, \cdots, 1)^T + \sum_{i\in[n_A]\backslash S} \alpha_{i0} b_j^{2m+1} d_i^{N-2m-1}(1, \beta_i, \cdots, \beta_i^{N-2m-1})^T = \vec{0}. \tag{B-36}$$

Denote $\sum_{i\in S}\alpha_{i0}b_j^N = \alpha'$. If $\alpha' \neq 0$, it just adding one vector in the linear combination compared with Eq. (B-32),

$$\alpha'(0, 0, \cdots, 1)^T + \sum_i \alpha_i(1, \beta_i, \cdots, \beta_i^{N-2m-1})^T = \vec{0}. \tag{B-37}$$

Similarly, based on the non-singularity of Vandermonde matrix, $n_\beta + 1 > N-2m$. Hence, $n_A \geq n_\beta + 1 > N-2m$.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Appendix C Details of Efficient detection of multipartite entanglement structure

This section contains details of Efficient detection of multipartite entanglement structure in Chapter 5. We put the proofs of Corollaries 5.1 to 5.4 in Sec. C.2 to C.5, respectively. We also discuss the tightness of each witness at the end of each corollary.

C.1 Witness entanglement structures of graph states

In this section, to illustrate the proposed entanglement structure witnesses, we apply Theorem 5.1 to several widely-used graph states, such as 1-D and 2-D cluster states and prove the results shown in Main Text. In addition, we also discuss the advantage of witnessing subsystem entanglement structures by only post-processing the measurement results, and the generalization to multi-color graph states.

C.1.1 Entanglement entropy of graph state

In this subsection, we briefly review the formula of the entanglement entropy of graph state [Hein et al. (2004)], which is helpful for the following discussions.

Any simple graph G can be uniquely determined by its symmetric adjacency matrix denoted as Γ, with $\Gamma_{i,j} = 1$ iff $(i, j) \in E$. Suppose the vertex set $V = \{N\}$ is partitioned into two complementary subsets A and $\bar{A}$, the adjacency matrix Γ can be arranged in the following form,

$$\Gamma_G = \begin{pmatrix} \Gamma_A & \Gamma_{A\bar{A}} \\ \Gamma_{A\bar{A}}^T & \Gamma_{\bar{A}} \end{pmatrix}, \tag{C-1}$$

where Γ_A, $\Gamma_{\bar{A}}$ describe the connections inside each subsystem, and the off-diagonal $\Gamma_{A\bar{A}}$ is for the ones between them.

Given a graph state $|G\rangle$ with its associated graph G, the reduced density matrix of a subsystem A is $\rho_A = \mathrm{Tr}_{\bar{A}}(|G\rangle\langle G|)$, where the partial trace is on $\bar{A}$. The explicit formula of the entanglement entropy is

$$S(\rho_A) = \mathrm{rank}(\Gamma_{A\bar{A}}) \tag{C-2}$$

where the rank is on the binary field $\mathbb{F}_2$, and $S(\rho) = -\mathrm{Tr}[\rho \log_2 \rho]$ is Von Neumann

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

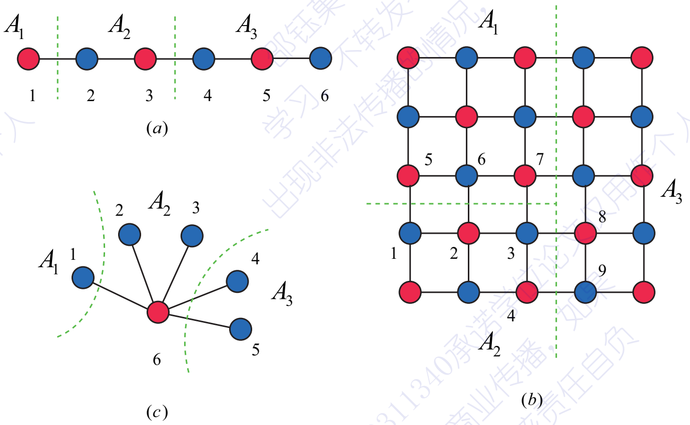


Figure C.1 Graphs of (a) 1-D cluster state, (b) 2-D cluster state, and (c) GHZ state

entropy. Note that Renyi-α entropy $S_\alpha(\rho_A)$ of any order is also suitable here, since the spectrum of ρ_A is flat for graph states.

C.1.2 Examples: 1-D and 2-D cluster states

Now we apply Theorem 5.1 to detect entanglement structures of the 1-D and 2-D cluster states. The corresponding graphs of these states are all 2-colorable, i.e., $k = 2$, thus one can realize the witnesses with only two local measurement settings.

We first detect the entanglement structures of the 1-D cluster state $|C_1\rangle$ using the two projectors P_1 and P_2 defined in Eq. (5-29) with stabilizers of $|C_1\rangle$. Consider an example of tripartition $\mathcal{P}_3 = \{A_1, A_2, A_3\}$ as shown in Fig. C.1(a), there are three ways to divide the subsystems into two sets, i.e., $\{A, \bar{A}\} = \{A_1, A_2A_3\}, \{A_2, A_1A_3\}, \{A_3, A_1A_2\}$. And the corresponding entanglement entropies are $S(\rho_{A_1}) = S(\rho_{A_3}) = 1$ and $S(\rho_{A_2}) = 2$, which is a manifest of the area law of entanglement entropy [Eisert et al. (2010)]. Thus the maximal and minimal entropy is 2 and 1. According to Theorem 5.1, the operators to witness $\mathcal{P}_3$-entanglement structure are given by,

$$\begin{aligned} W_{f,C_1}^{\mathcal{P}_3} &= \frac{5}{4}\mathbb{I} - (P_1 + P_2), \\ W_{b,C_1}^{\mathcal{P}_3} &= \frac{3}{2}\mathbb{I} - (P_1 + P_2), \end{aligned} \tag{C-3}$$

where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the graph of Fig. C.1(a). Similar analysis works for other general partitions.

Here we show how to calculate the entanglement entropy $S(\rho_{A_2})$ by using the formula in Eq. (C-2), and the entanglement entropy of other subsystems can be calculated similarly.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

The matrix $\Gamma_{A_2,\bar{A}_2}$ which describes the connections between A_2 and $\bar{A}_2 = A_1A_3$ shows,

$$\Gamma_{A_2,\bar{A}_2} = \begin{array}{c} \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \end{array}, \tag{C-4}$$

where the indexes of the row and column label the vertexes in A_2 and $\bar{A}_2$ respectively. In fact, one just need to consider following submatrix,

$$\begin{array}{c} \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cc} 1 & 4 \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array}, \tag{C-5}$$

which is obtained from $\Gamma_{A_2,\bar{A}_2}$ by deleting the last two columns, and shares the same rank of $\Gamma_{A_2,\bar{A}_2}$. Note that there is no edge between the vertexes 5, 6 in $\bar{A}_2$ and the ones in A_2. The matrix in Eq. (C-5) is an identity matrix with rank 2, thus $S(\rho_{A_2}) = 2$. Generally speaking, one only needs to consider the vertexes which are related to the edges connecting A and $\bar{A}$, when calculating the rank of the matrix $\Gamma_{A,\bar{A}}$.

Next, we consider the 2-D cluster state $|C_2\rangle$ that is defined on a 2-D square lattice. As an example, we consider a tripartition of a 5×5 lattice as shown in Fig. C.1(b). Similar as the 1-D cluster state case, the corresponding entanglement entropies are $S(\rho_{A_1}) = S(\rho_{A_3}) = 5$ and $S(\rho_{A_2}) = 4$. According to Theorem 5.1, the operators to witness $\mathcal{P}_3$-entanglement structure are given by,

$$\begin{aligned} W_{f,C_2}^{\mathcal{P}_3} &= \frac{33}{32}\mathbb{I} - (P_1 + P_2), \\ W_{b,C_2}^{\mathcal{P}_3} &= \frac{17}{16}\mathbb{I} - (P_1 + P_2), \end{aligned} \tag{C-6}$$

where the two projectors P_1 and P_2 are defined in Eq. (5-29) with the graph of Fig. C.1(b). Similar analysis works for other general partitions.

Here we show how to calculate the entanglement entropy $S(\rho_{A_2})$ by using the formula in Eq. (C-2), and the entanglement entropy of other subsystems can be calculated similarly. As mentioned in the 1-D case, one only needs to consider the following matrix which

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

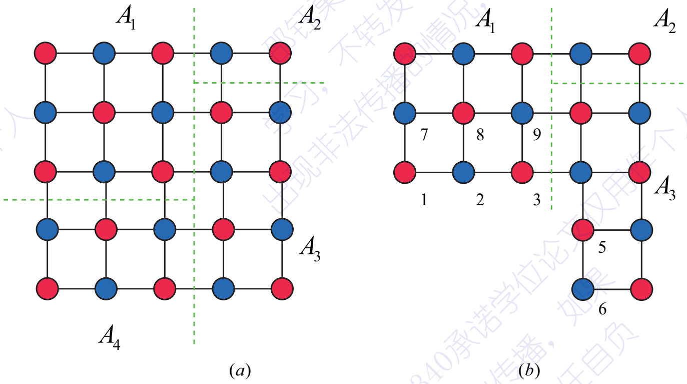


Figure C.2　Witness subsystem entanglement structures.

shares same rank with $\Gamma_{A_2,\bar{A}_2}$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \end{array} \tag{C-7}$$

which is obtained from $\Gamma_{A_2,\bar{A}_2}$ by ignoring the vertexes in the bulks of both A_2 and $\bar{A}_2$. It is clear that the rank of the matrix in Eq. (C-7) is 4, since the four row vectors are linearly independent. As a result, $S(\rho_{A_2}) = 4$.

C.1.3　Witnessing subsystem entanglement structures

As mentioned in Main Text, the witnesses in Theorem 5.1 can also be used to detect the entanglement structures of a few of subsystems, by only post-processing the original measurement results. In the following, we take the 2-D cluster state to illustrate this advantage.

As shown in Fig. C.2(a), the whole 2-D lattice is partitioned into four parts $\{A_1, A_2, A_3, A_4\}$. Suppose one only cares about the entanglement structures among subsystems A_1, A_2 and A_3, the witnesses shown in Theorem 5.1 can be applied in this scenario. To be specific, the projectors P_1 and P_2 appearing in the witnesses should be changed to P_1' and P_2', which are related to the new graph state $|G_{A_1A_2A_3}\rangle$. $G_{A_1A_2A_3}$ is the subgraph of G with edges and vertexes related to A_2 deleted, i.e., $G_{A_1A_2A_3} = G - V_{A_4}$, as shown in Fig. C.2 (b). Similar as the 2-D cluster case shown previously, now we should calculate the entanglement entropy with respect to the new graph state $|G_{A_1A_2A_3}\rangle$. It is not hard to

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

find that $S(\rho'_{A_1}) = S(\rho'_{A_3}) = 3$ and $S(\rho'_{A_2}) = 2$, where $\rho'_{A_i} = \mathrm{Tr}_{\bar{A}_i}(|G_{A_1A_2A_3}\rangle\langle G_{A_1A_2A_3}|)$ for $i = 1, 2, 3$.

As a result, according to Theorem 5.1, the operators to witness this $\mathcal{P}_3 = \{A_1, A_2, A_3\}$-entanglement structure are given by,

$$\begin{aligned} W^{\mathcal{P}_3}_{f,sub} &= \frac{9}{8}\mathbb{I} - (P'_1 + P'_2), \\ W^{\mathcal{P}_3}_{b,sub} &= \frac{5}{4}\mathbb{I} - (P'_1 + P'_2), \end{aligned} \tag{C-8}$$

where the two projectors P'_1 and P'_2 are defined in Eq. (5-29) with stabilizers of the graph state $|G_{A_1A_2A_3}\rangle$. Now the stabilizers which constitute the projectors are restricted on the subsystem $A_1A_2A_3$. For example, $S'_1 = X_1Z_2Z_7$ and $S'_2 = X_2Z_1Z_8Z_3$ in P'_1 and P'_2 in Fig. C.2 (b).

Note that the expectation values of them can be evaluated from the two original local measurement settings $\bigotimes_{i\in V_1} X_i \bigotimes_{j\in V_2} Z_j$ and $\bigotimes_{i\in V_1} Z_i \bigotimes_{j\in V_2} X_j$, which are employed to measure P_1 and P_2, respectively. Consequently, one can detect the entanglement structures of any subset of subsystems by only post-processing the measurement results, without conducting the experiment again.

C.1.4 Multi-color graph state

As shown in Main Text, the number of local measurement settings in the detection is directly related to the colorability of the corresponding graph. That is, the witnesses can be realized with k local measurements when the corresponding graph G is k-colorable. We have shown several widely-used graph states whose graphes are 2-colorable. Here we give a 3-colorable graph state and construct the entanglement structure witnesses according to Theorem 5.1.

Before that, we remark that one may reduce the chromatic number of the underlying graph by applying local complementation, which can be realized by local Clifford operation on the graph state [Hein et al. (2006); Van den Nest et al. (2004)]. To be specific, local complementation τ_i on G with respective to the vertex i is to delete edges between vertexes in the neighborhood set N_i if they are originally connected; or to add edges otherwise. The corresponding local Clifford unitary to realize this graph transformation shows,

$$U_i(G) = \exp(-i\frac{\pi}{4}X_i)\bigotimes_{j\in N_i}\exp(i\frac{\pi}{4}Z_j), \tag{C-9}$$

and one has $|\tau_i(G)\rangle = U_i(G)|G\rangle$. For example, as shown in Fig. C.3 (a), the fully

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

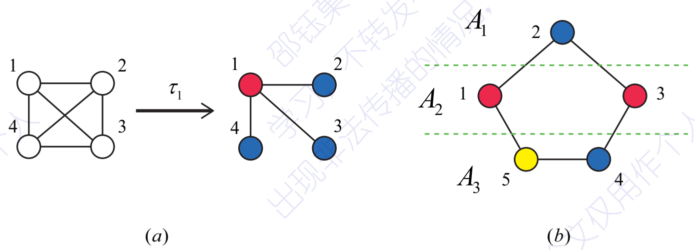


Figure C.3 (a) The local complementation on the fully connected graph which is N-colorable can transform it to the star graph which is 2-colorable. (b) Five-vertex ring graph which is 3-colorable, and the whole system is partitioned into 3 parts.

connected graph can be transformed to the star graph by local complementation, and one is N-colorable and the other is 2-colorable.

Then let us consider the five-qubit ring state $|R_5\rangle$ shown in Fig. C.3(b), with the corresponding graph being 3-colorable. Note that the optimizations in the witnesses shown in Theorem 5.1 just relate to the entanglement entropy of the graph state, not the chromatic number of it. The chromatic number decides how many local measurements that one needs to lower bound the fidelity between the separable states with the graph state, as shown in Proposition 5.2. In this case, we needs 3 local measurement settings according to the red, blue, and yellow vertexes to obtain the expectation values of the following three projectors,

$$\begin{aligned} P_1 &= \prod_{red\ i} \frac{S_i + \mathbb{I}}{2}, \\ P_2 &= \prod_{blue\ i} \frac{S_i + \mathbb{I}}{2}, \\ P_3 &= \prod_{yellow\ i} \frac{S_i + \mathbb{I}}{2}. \end{aligned} \tag{C-10}$$

On the other hand, the entanglement entropies of the subsystems show $S(\rho_{A_1}) = 1$ and $S(\rho_{A_2}) = S(\rho_{A_3}) = 2$. According to Theorem 5.1, the operators to witness $\mathcal{P}_3$-entanglement structure are given by,

$$\begin{aligned} W_{f,R_5}^{\mathcal{P}_3} &= \frac{9}{4}\mathbb{I} - (P_1 + P_2 + P_3), \\ W_{b,R_5}^{\mathcal{P}_3} &= \frac{5}{2}\mathbb{I} - (P_1 + P_2 + P_3), \end{aligned} \tag{C-11}$$

where the two projectors P_1, P_2 and P_3 are defined in Eq. (C-10) with stabilizers of the ring state $|R_5\rangle$.

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

C.2 Proof of Corollary 5.1

Proof. The genuine entanglement witness $W_b^{\mathcal{P}_N}$ in Eq. (5-21) is obtained from Eq. (5-19) in Theorem 5.1, by considering the N-partition $\mathcal{P}_N$. Thus, we need to find the solution of $\max_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$, or equivalently, $\min_{\{A,\bar{A}\}} S(\rho_A)$ of the N-partite graph state $|G\rangle$. Here we show that $\min_{\{A,\bar{A}\}} S(\rho_A) = 1$. Since $|G\rangle$ is an entangled pure state, $S(\rho_A) > 0$ for any A. Because the entanglement spectrum is flat for any graph state, $S(\rho_A)$ is at least 1 with spectrum $\{\frac{1}{2}, \frac{1}{2}\}$. We can choose any single qubit as A such that $S(\rho_A) = 1$ and finish the proof. ■

In the following, we show that the witness $W_b^{\mathcal{P}_N}$ is tight (or optimal), in the sense that there exists a bi-separable state ρ_b that saturates $\mathrm{Tr}(\rho_b W_b^{\mathcal{P}_N}) = 0$. For simplicity, we consider the case where the underlying graph is $k = 2$-colorable. For general k case, the tightness can be proved similarly. As $k = 2$, the witness in Eq. (5-21) becomes,

$$W_b^{\mathcal{P}_N} = \frac{3}{2}\mathbb{I} - (P_1 + P_2), \tag{C-12}$$

which is suitable for 1-D and 2-D cluster states and the GHZ state shown in Fig. C.1, and the projectors P_1 and P_2 are defined in Eq. (5-29).

To show the tightness, we give a specific bi-separable state such that $\mathrm{Tr}(\rho_b W_b^{\mathcal{P}_N}) = 0$, or equivalently $\langle P_1 + P_2\rangle = \frac{3}{2}$. P_1 and P_2 can be written explicitly as a summation of stabilizers in the form $K_{\vec{p}} = S_1^{p_1} S_2^{p_2} \cdots S_N^{p_N}$, with $\vec{p} = (p_1, p_2 \cdots p_N)$ a binary vector. To be specific, P_1 and P_2 contains all the stabilizers generated by the independent stabilizers S_i of the red and blue vertexes respectively,

$$\begin{aligned} P_1 &= \sum_{red\ \vec{p}} \frac{K_{\vec{p}}}{2^{n_r}}, \\ P_2 &= \sum_{blue\ \vec{q}} \frac{K_{\vec{q}}}{2^{n_b}}, \end{aligned} \tag{C-13}$$

where n_r and n_b denote the number of red and blue vertexes, respectively with $n_r + n_b = N$; $\vec{p}$ denote red type vector whose $p_i = 0$ for all blue i; $\vec{q}$ denote blue type vector whose $q_{i'} = 0$ for all red i'.

Now suppose the first vertex is red, we choose $|\Psi_b\rangle = |0\rangle_1 \otimes |G_{\{2,3,\cdots,N\}}\rangle$, where the first qubit is set as $|0\rangle$ and the remaining qubits hold a graph state $|G_{\{2,3,\cdots,N\}}\rangle$. The corresponding graph $G_{\{2,3,\cdots,N\}}$ is obtained from the original graph G via deleting the vertex 1 and the edges connected to it. First, considering the stabilizer $K_{\vec{p}}$ in the projector

P_1. If $K_{\vec{p}}$ does not contain S_1, one has $\langle K_{\vec{p}}\rangle = 1$, since it is still a stabilizer of the state $|G_{\{2,3,\cdots,N\}}\rangle$, when restricted on the qubits $\{2,\cdots,N\}$; otherwise $\langle K_{\vec{p}}\rangle = 0$, since S_1 contains a Pauli X_1 on the first qubit and $\langle 0| X |0\rangle = 0$. As a result, we have $\langle P_1\rangle = \frac{1}{2}$, because there is one half of $K_{\vec{p}}$ containing S_1. Then, considering the stabilizer $K_{\vec{q}}$ in the projector P_2. $\langle K_{\vec{q}}\rangle = 1$ for any $K_{\vec{q}}$ in P_2, since $K_{\vec{q}}$ contains a Pauli Z_1 or $\mathbb{I}_1$ on the first qubit with $\langle 0| Z(\mathbb{I}) |0\rangle = 1$, and the remaining part of it is also a stabilizer of the state $|G_{\{2,3,\cdots,N\}}\rangle$. As a result, one has $\langle P_2\rangle = 1$ and hence $\langle P_1 + P_2\rangle = \frac{3}{2}$.

C.3 Proof of Corollary 5.2

As mentioned in Main Text, Corollary 5.2 is obtained from Eq. (5-18) in Theorem 5.1 by taking all the subsystems just containing one qubit, i.e., an N-partition $\mathcal{P}_N$. To prove it, one need to find the solution of the optimization problem about entanglement entropy, say, $\min_{\{A,\bar{A}\}} 2^{-S(\rho_A)}$, where A is a subsystem and $S(\rho_A) = \mathrm{Tr}_{\bar{A}}(|C\rangle\langle C|)$. Equivalently, one should find the optimization $\max_{\{A,\bar{A}\}} S(\rho_A)$, denoted as S_{max} for simplicity. In the following subsections, we prove Corollary 5.2 for 1-D and 2-D cluster states, by showing that $S_{max} = \lfloor \frac{N}{2} \rfloor$, respectively.

C.3.1 Proof of Corollary 5.2 of 1-D cluster state

Proof. Here, we show that $S_{max} = \lfloor \frac{N}{2} \rfloor$ for the 1-D cluster state. First, note the entanglement entropy should be no more than the qubit number in the subsystem, thus one has $S(\rho_A) \leq |A|$ and $S(\rho_{\bar{A}}) \leq |\bar{A}|$. On account of $S(\rho_A) = S(\rho_{\bar{A}})$, one further has $S(\rho_A) \leq \min\{|A|, |\bar{A}|\}$. As a result, $S_{max} \leq \lfloor \frac{N}{2} \rfloor$.

Then, we choose the system A composed of all the qubits on the odd sites to saturate this bound. One can calculate the corresponding entanglement entropy with the formula given in Eq. (C-2). Here, we evaluate $S(\rho_A)$ with another equivalent method by distilling EPR pairs between A and $\bar{A}$ with local unitary [Briegel et al. (2001); Markham et al. (2007)], which is more intuitional and beneficial to other proofs in Supplemental Material. Since local unitary does not change the entanglement entropy, one can properly find the value of it by counting the final number of EPR pairs.

As shown in Fig. C.4, we divide the system into two parts according to the odd/even position of the qubits (or red/blue according to Fig. C.1). First, apply "local" unitary Controlled-Z operation $CZ^{\{1,3\}}$ on qubits 1 and 3, where locality is in the sense that one considers A and $\bar{A}$ as two subsystems. Second, apply local complementation on qubit 1, which can be realized by local Clifford unitary [Hein et al. (2006); Van den Nest et al. (2004)]. Local complementation τ_i on G with respective to the vertex i is to add edges between the vertexes in the neighborhood set N_i under module 2. As a result, the edge $\{2,3\}$ is deleted. Third, apply $CZ^{\{1,3\}}$ again and there is a EPR pair appearing between qubits 1, 2. Here we call the two-qubit graph state $\frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)$ EPR pair without confusion. Iterating this process, one finally can distill $\lfloor \frac{N}{2} \rfloor$ EPR pairs. Consequently, one has $S(\rho_{odd}) = \lfloor \frac{N}{2} \rfloor$. ■

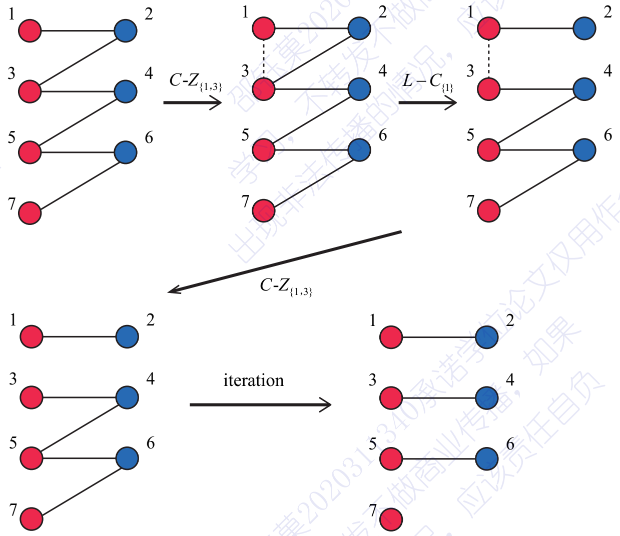


Figure C.4　An illustration of distilling EPR pairs from 1-D cluster state by local unitary.

C.3.2　Proof of Corollary 5.2 of 2-D cluster state

Proof. Here, we show that $S_{max} = \lfloor \frac{N}{2} \rfloor$ for 2-D cluster state. One has $S_{max} \leq \lfloor \frac{N}{2} \rfloor$ as in the 1-D case, since the entanglement entropy can not be larger than the number of qubit in the subsystems. In the following, we give examples of subsystem A to saturate this bound. The chosen A depends on the even/odd property of the total number of qubits.

First, let us consider the even-qubit case, i.e., the qubit number $N = n \times n$ where n is even. We select all the odd columns to constitute the subsystem A, as shown in Fig. C.5. Then one can prove that $S(\rho_A) = \frac{N}{2}$ by distilling EPR pairs as in the 1-D case. To be specific, one first applies CZ operations inside both subsystems A and $\bar{A}$, such that the quantum state becomes n independent 1-D cluster state each with n qubits. Then by distilling EPR for each 1-D cluster state, finally one can obtain totally $n \times \frac{n}{2} = \frac{N}{2}$ EPR pairs, thus $S(\rho_A) = \frac{N}{2}$.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

For the odd-qubit case, $N = n \times n$ with n being odd. The previous choosing style can not make $S(\rho_A) = \lfloor \frac{N}{2} \rfloor$. Here we show a modified one. The first $n - 1$ columns belong to A and $\bar{A}$ in succession as before. For the qubits in the final column, we successively distribute the qubits to A and $\bar{A}$. Then as in the even-qubit case, one applies CZ operations inside both subsystems and distill EPR pairs for several 1-D cluster states, as shown in Fig. C.5. Finally, we also get $S(\rho_A) = \lfloor \frac{N}{2} \rfloor$. ■

We remark that Corollary 5.2 also holds for the 2-D cluster state with general rectangle lattice $n_1 \times n_2$. With loss of generality, assume that n_1 is odd and n_2 is even, one can distill $\lfloor \frac{N}{2} \rfloor$ EPR pairs by choosing A containing all the odd columns as the above proof. We further conjecture that Corollary 5.2 holds for any (such as 3-D) cluster states.

Finally, we show that the witness $W_{f,C}^{\mathcal{P}_N}$ in Corollary 5.2 is tight. We give a fully separable state $|\Psi_f\rangle = \bigotimes_{red\ i} |+\rangle_i \bigotimes_{blue\ j} |0\rangle_j$ to saturate the bound, where the red (blue) qubits are set as $|+\rangle$ ($|0\rangle$) respectively. Similar as the discussion of $W_b^{\mathcal{P}_N}$ in Sec. C.2, one has $\langle P_1 \rangle = 1$, since $\langle K_{\vec{p}} \rangle = 1$ for all $K_{\vec{p}}$ in P_1; $\langle P_2 \rangle = 2^{-\lfloor \frac{N}{2} \rfloor}$, since all $\langle K_{\vec{q}} \rangle = 0$ in P_2 except the $\mathbb{I}$. Consequently, $\langle P_1 + P_2 \rangle = 1 + 2^{-\lfloor \frac{N}{2} \rfloor}$.

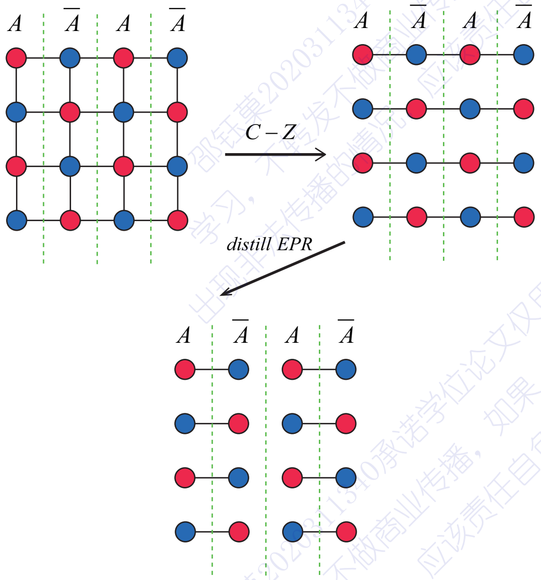


Figure C.5 Distill EPR pairs in the 4 × 4 2-D cluster state

C.4 Proof of Corollary 5.3

Before proving Corollary 5.3, we introduce the following Lemma. It gives a lower bound of $S(\rho_A)$ related to the geometric connection between A and $\bar{A}$. First, let us

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

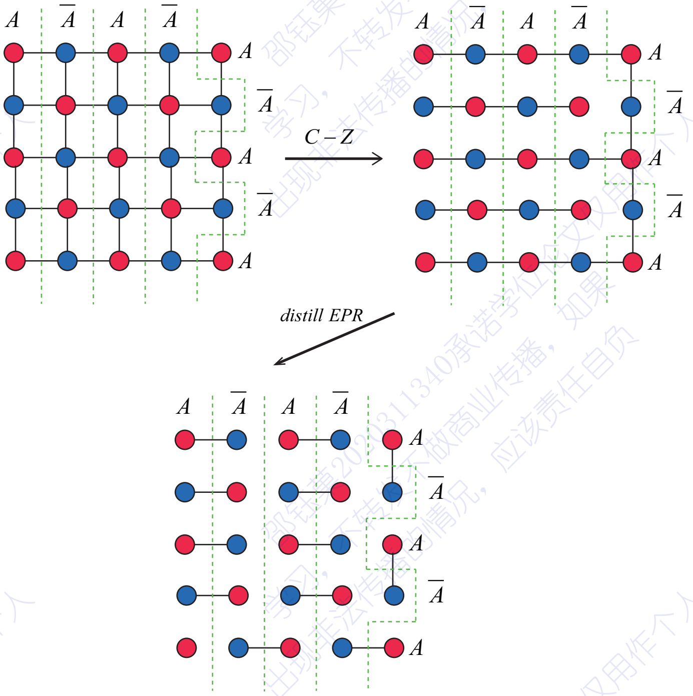


Figure C.6 Distill EPR pairs in the 5 × 5 2-D cluster state

introduce the definition of the boundary between A and $\bar{A}$ on a 1-D qubit chain. The edge $(i, i+1)$ is called a boundary, if $i \in A$, $i+1 \in \bar{A}$ or vice versa.

Lemma C.1： Given a bipartition $\{A, \bar{A}\}$ on a 1-D qubit chain, if the number of boundaries between A and $\bar{A}$ is not less than $m-1$, the entanglement entropy can be lower bounded by,

$$S(\rho_A) \geq \lfloor \frac{m}{2} \rfloor, \tag{C-14}$$

where $\rho_A = \mathrm{Tr}_{\bar{A}}(|C_1\rangle\langle C_1|)$ is the the reduced density matrix of a 1-D cluster state $|C_1\rangle$.

Note that Lemma C.1 can be seen as a manifest of the area law of entanglement entropy [Eisert et al. (2010)].

Proof. In the following, we bound the value of $S(\rho_A)$ by distilling EPR pairs between A and $\bar{A}$ with local unitary operations, similar as the proof of Corollary 5.2.

Given any bipartition $\{A, \bar{A}\}$, subsystems A and $\bar{A}$ would distribute sequentially on the chain, as shown in Fig. C.7. Two boundaries may be close to each other, such as $(i, i+1)$ and $(i+1, i+2)$. There are several boundary clusters, denoted by h_k. Inside each cluster, the boundaries distribute in sequence closely; between the clusters, the boundaries are far away from each other more than one qubit. Fig. C.7 (a) shows a 7-qubit example, where there are two boundary clusters h_1 and h_2.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

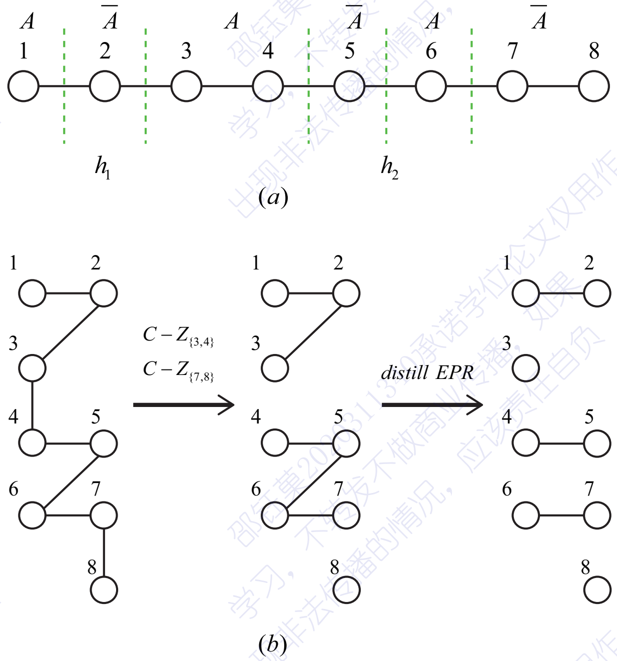


Figure C.7 (a) Given a bipartition $\{A, \bar{A}\}$, subsystems A and $\bar{A}$ distribute sequentially on the chain. In this 7-qubit example, there are two boundary clusters h_1 and h_2, with $|h_1| = 2$ and $|h_2| = 3$. (2) Distill EPR pairs between A and $\bar{A}$. First, one can apply C-Z operation inside A and $\bar{A}$ to eliminate the connection which are not relevant. Here we apply $C - Z_{\{3,4\}}$ and $C - Z_{\{7,8\}}$. Second, we distill EPR pairs between A and $\bar{A}$ as in Fig. C.4, and one can see that the distillation is conducted inside each cluster.

Via applying local unitary operations, one can distill $\lceil |h_k|/2 \rceil$ EPR pairs from each cluster, where $|h_k|$ is the number of boundaries (see Fig. C.7 (b) for detailed illustration). As a result, the entanglement entropy is bounded by,

$$S(\rho_A) = \sum_k \left\lceil \frac{|h_k|}{2} \right\rceil \geq \left\lceil \sum_k \frac{|h_k|}{2} \right\rceil \geq \left\lceil \frac{m-1}{2} \right\rceil = \left\lfloor \frac{m}{2} \right\rfloor \tag{C-15}$$

where the second inequality is because the precondition that the number of boundaries is not less than $m - 1$. ■

Then we give the proof of Corollary 5.3 as follows.

Proof. According to Theorem 5.2, one needs to prove the solution of the optimization,

$$f_1(m) \equiv \min_{\mathcal{P}_m} \max_{\{A,\bar{A}\}} S(\rho_A) = \left\lfloor \frac{m}{2} \right\rfloor \tag{C-16}$$

where the maximization takes over all possible partitions $\mathcal{P}_m$ with m subsystems, the minimization takes over all bipartitions of $\mathcal{P}_m$, and $\rho_A = \mathrm{Tr}_{\bar{A}}(|C_1\rangle\langle C_1|)$. In the following, We first show $f_1(m) \geq \lfloor \frac{m}{2} \rfloor$ and then give a specific partition to saturate the bound.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Given any m-partition $\mathcal{P}_m = \{A_i\}_{i=1,2\cdots m}$, one can always choose a bipartition $\{A, \bar{A}\}$ of $\mathcal{P}_m$, such that A and $\bar{A}$ shares at least $m-1$ boundaries. Then, with Lemma C.1 one has $f_1(m) \geq \left\lfloor \frac{m}{2} \right\rfloor$. To be specific, if A_i distribute sequentially on the qubit chain, one can choose the odd site of A_i, i.e., $A = \bigcup_{odd\ i} A_i$, and it is clear that A and $\bar{A}$ shares $m-1$ boundaries in this case. For general cases, by utilizing a fact of graph theory one can also find a proper bipartition of $\mathcal{P}_m$ as follows. Let every subsystem A_i represent a vertex i of a weighted graph, and the weight of the edge (i, j) is the number of boundaries between A_i and A_j. Since this graph is connected, one can choose a (minimum) spanning tree of this graph [Kleinberg et al. (2005)]. Then let A contains all the A_i in the odd layers of the tree, and there are $m-1$ edges between A and $\bar{A}$. As a result, the number of boundary is at least $m-1$, since there is at least one boundary for one edge.

Finally, we give a specific partition to show that $f_1(m) = \left\lfloor \frac{m}{2} \right\rfloor$. Let $A_1 = \{1\}, A_2 = \{2\}, \cdots, A_m = \{m, m+1, \cdots, N\}$, where $1, 2, \cdots N$ denote the qubits. Then choose $A = \bigcup_{odd\ i} A_i$, one can distill EPR pairs as in the proof of Lemma C.1. Now there is only one boundary cluster and one has $S(\rho_A) = \left\lfloor \frac{m}{2} \right\rfloor$. Finally, we finish the proof of $f_1(m) = \left\lfloor \frac{m}{2} \right\rfloor$ as well as Corollary 5.3. ■

At the end of this section, we show that the witnesses in Corollary 5.3 are tight, in the sense that there is an m-separable state ρ_m to saturate $\mathrm{Tr}(\rho_m W_{m,C_1}) = 0$. Here we show the $m = 4$ case, by choosing $|\Psi_m\rangle = |+\rangle_1 |0\rangle_2 |+\rangle_3 |0\rangle_4 |C_1\rangle_{\{5,6,\cdots,N\}}$, and it can be generalized to any m directly. Similar as the discussion of $W_b^{\mathcal{P}_N}$ in Sec. C.2, one can find that $\langle P_1 \rangle = 1$, $\langle P_2 \rangle = 2^{-\lfloor \frac{m}{2} \rfloor}$, and $\langle P_1 + P_2 \rangle = 1 + 2^{-\lfloor \frac{m}{2} \rfloor}$.

C.5 Proof of Corollary 5.4

Before proving Corollary 5.4, we introduce the following Lemma.

Lemma C.2: Given an m-partition $\mathcal{P}_m$ of an N-qubit system, with subsystems $\{A_i\}_{i=1}^m$ and $N \geq \frac{m(m-1)}{2}$, there always exists a bipartition of $\mathcal{P}_m$, denoted as $\{A, \bar{A}\}$, such that the qubit number in A satisfies,

$$m - 1 \leq |A| \leq N - (m-1). \tag{C-17}$$

Proof. Without loss of generality, we assume that the qubit number of each subsystem is in the increasing order $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. Since $|A_i| \geq 1$, one has $|A_m| = N - \sum_{i=1}^{m-1} \leq N - (m-1)$. Suppose $|A_m| \geq m-1$, we can directly select A_m as A. Otherwise we choose $A = A_{m-1} \bigcup A_m$, and show that $|A| = |A_{m-1}| + |A_m|$ satisfies Eq. (C-17) by contradiction.

First, suppose $|A| < m-1$, in the case of m being even, one has

$$N = \sum_{i=1}^{m} |A_i| \le \frac{m}{2}(|A_{m-1}| + |A_m|) < \frac{m(m-1)}{2}, \tag{C-18}$$

where the first inequality is because there are $\frac{m}{2}$ pair of subsystems A_{2k-1}, A_{2k} for $1 \le k \le \frac{m}{2}$, with $|A_{2k-1}| + |A_{2k}| \le |A_{m-1}| + |A_m|$. It is clear that Eq. (C-18) is contradict with the precondition $N \ge \frac{m(m-1)}{2}$. In the odd m case, one can obtain the same contradiction as Eq. (C-18),

$$N = \sum_{i=1}^{m} |A_i| \le (m-2)|A_{m-1}| + (|A_{m-1}| + |A_m|) < (m-2)\frac{m-1}{2} + (m-1) = \frac{m(m-1)}{2}, \tag{C-19}$$

where in the first inequality we apply $|A_i| \le |A_{m-1}|$ for the first $m-2$ subsystems, the second inequality is due to the fact that $|A_{m-1}| < \frac{m-1}{2}$.

Moreover, suppose $|A| > N-(m-1)$, one has $|A| = N-(m-2)$, since there is at least one qubit in each of the first $m-2$ subsystems. On account of $|A_m| < m-1$, we have

$$|A_{m-1}| > N-(m-2)-(m-1) = N-1, \tag{C-20}$$

which means that $|A_{m-1}| = N$ and it leads to a clear contradiction. ■

Then we give the proof of Corollary 5.4 as follows.

Proof. According to Theorem 5.2, similar as the 1-D case, one needs to find the solution of the optimization

$$f_2(m) \equiv \min_{\mathcal{P}_m} \max_{\{A,\bar{A}\}} S(\rho_A) \tag{C-21}$$

where the maximization takes over all possible partitions $\mathcal{P}_m$ with m subsystems, the minimization takes over all bipartitions of $\mathcal{P}_m$, and $\rho_A = \mathrm{Tr}_{\bar{A}}(|C_2\rangle\langle C_2|)$. Comparing to the 1-D case, the partition of the 2-D lattice is richer and more complex, thus here instead of finding the exact solution of $f_2(m)$, we give a reliable lower bound of it, i.e.,

$$f_2(m) \ge \gamma(m) \equiv \left\lceil \frac{-1+\sqrt{1+8(m-1)}}{2} \right\rceil. \tag{C-22}$$

Note that a lower bound of the optimization can give us a reasonable witness. We also show that this bound is tight, i.e., it exactly equals to the solution of the optimization, as $m \le 5$.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

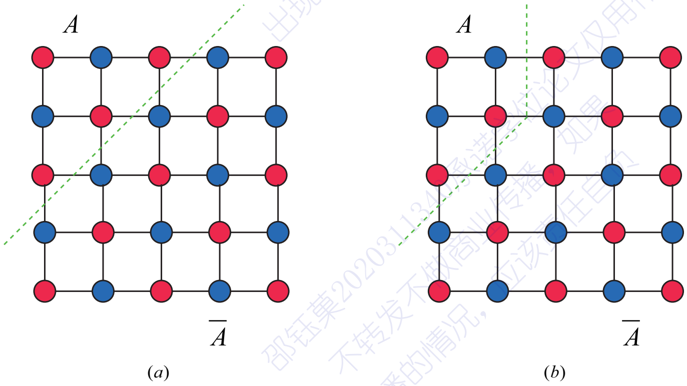
In the following, we first prove that $f_2(m) \geq \gamma(m)$ and then give explicit partitions to saturate the bound as $m \leq 5$. On account of Lemma C.2, for any m-partition $\mathcal{P}_m$, one can always find a bipartition $\{A, \bar{A}\}$ of $\mathcal{P}_m$ such that the qubit number in A satisfying $m-1 \leq |A| \leq N-(m-1)$. Without loss of generality, one can consider $m-1 \leq |A| \leq \frac{N}{2}$, otherwise we take $\bar{A}$ as A.

Generally speaking, the larger the total qubit number $|A|$ contains, the larger the entanglement entropy $S(\rho_A)$ is. For 2-D cluster state, the entanglement entropy satisfies the area law [Eisert et al. (2010)]. Given that the qubit number of A satisfies $m-1 \leq |A| \leq \frac{N}{2}$, the best way to minimize the entanglement entropy is to reduce the boundary length of it,that is, gather at the corner of the square lattice, as shown in Fig. C.8. Suppose that the subsystem A happens to be a right-angled isosceles triangle with the length of hypotenuse being d. Then the boundary length of A, $|\partial A| = d$, and it is not hard to find that $S(\rho_A) = d$. Consider $|A| = m - 1$, and we have the relation,

$$\frac{d(d+1)}{2} = m - 1. \tag{C-23}$$

By solving Eq. (C-24), one obtains $d = \frac{-1+\sqrt{1+8(m-1)}}{2}$. For general m, the shape of A is not necessarily a triangle, and we should round up the value and get,

$$S(\rho_A) \geq \left\lceil \frac{-1+\sqrt{1+8(m-1)}}{2} \right\rceil. \tag{C-24}$$



(a) (b)

Figure C.8 Minimization of the entanglement entropy $S(\rho_A)$ by reducing the boundary length $|\partial A|$. The best strategy is to gather at the corner of the 2-D lattice. (a)The subsystem A contains 6 qubits and it happens to be a triangle with $S(\rho_A) = |\partial A| = 3$. (b)The subsystem A contains 5 qubits and in this case its entropy $S(\rho_A)$ is still 3.

Consequently, for any m-partition $\mathcal{P}_m$, there exists a bipartition $\{A, \bar{A}\}$ of it, such that

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

$S(\rho_A) \geq \gamma(m)$ and hence $\max_{\{A,\bar{A}\}} S(\rho_A) \geq \gamma(m)$. As a result, one has $f_2(m) \geq \gamma(m)$.

Moreover, we give partitions to saturate this bound as $m \leq 5$. Take the $m = 5$ case for example, one can choose the first four subsystems all contain one qubits, i.e., $|A_1| = |A_2| = |A_3| = |A_4| = 1$, in a corner of the square lattice, and A_5 contains the remaining qubits, as shown in Fig. C.9. It is not hard to see that $\max_{\{A,\bar{A}\}} S(\rho_A) = \gamma(5) = 3$ for any bipartition of this $\mathcal{P}_{m=5}$. ■

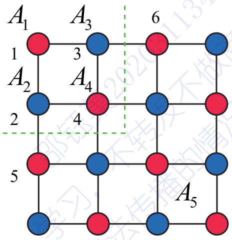


Figure C.9 Illustration of a partition that saturates the bound on entanglement entropy, i.e., $S(\rho_A) \geq \gamma(m) = 3$, in the $m = 5$ case. The first four subsystems all contain one qubits, i.e., $|A_1| = |A_2| = |A_3| = |A_4| = 1$, in the corner of the square lattice, and A_5 contains the remaining qubits. It is not hard to see that $\max_{\{A,\bar{A}\}} S(\rho_A) = 3$ for any bipartition of this $\mathcal{P}_{m=5}$.

Finally, we remark that the non-m-separability witnesses shown in Corollary 5.4 is tight or optimal as $m \leq 5$. Here we show a specific m-separable state to saturate the witness as $m = 5$. The qubit label is given in Fig. C.9, and we choose $|\Psi_m\rangle = |G_{\{1,2,3\}}\rangle \otimes |0\rangle_4 |0\rangle_5 |0\rangle_6 \otimes |G_{\{7,8,\cdots,N\}}\rangle$. Here $|G_{\{1,2,3\}}\rangle \otimes |G_{\{7,8,\cdots,N\}}\rangle$ are the graph state whose graph is obtained from the 2-D lattice by deleting the vertexes $\{4,5,6\}$ and their associated edges. Similar as the discussion of $W_b^{\mathcal{P}_N}$ in Sec. C.2, one can find that $\langle P_1\rangle = 2^{-3}$, $\langle P_2\rangle = 1$, and $\langle P_1 + P_2\rangle = 1 + 2^{-3}$.

邵钰棊2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Appendix D Details of operational interpretation of coherence in QKD

This section contains the details of operational interpretation of coherence in QKD in Chapter 6.

D.1 Quantum bit error correction

We first clarify the information reconciliation of the original protocol in Fig. 6.1, and then convert it to a quantum version, the quantum bit error correction of the virtual protocol.

In the original protocol, after the Z-basis measurement on $\rho_{AB}^{\otimes n}$, Alice and Bob get an n-bit string $\mathcal{Z}_A^n$ and $\mathcal{Z}_B^n$, respectively. Due to errors, the random variables $\mathcal{Z}_A^n$ and $\mathcal{Z}_B^n$ are not identical in general. Then, in (linear) error correction, Alice generate an error syndrome by hashing her bit string with an $nH(\mathcal{Z}_A|\mathcal{Z}_B) \times n$ random binary matrix. By consuming $nH(\mathcal{Z}_A|\mathcal{Z}_B)$ pre-shared secret bits, Alice sends the syndrome to Bob safely with the one-time-pad encryption. After obtaining the syndromes, Bob can correct the corresponding error bits.

In the virtual protocol, the quantum bit error correction is executed before the Z-basis measurement. Specifically, Alice and Bob now share $nH(\mathcal{Z}_A|\mathcal{Z}_B)$ EPR pairs. First, they use their state $\rho_{AB}^{\otimes n}$ to control the EPR pairs according to the hashing matrix separately, where the ancillary EPR pairs act as the target of the CNOT gate. Second, they measure the EPR pairs in the Z basis separately and get the measurement results $\mathcal{Z}_A^a$ and $\mathcal{Z}_B^a$, where a labels the ancilla. Then Alice sends $\mathcal{Z}_A^a$ to Bob and Bob obtains the error syndrome via bitwise binary addition $\mathcal{Z}_A^a \oplus \mathcal{Z}_B^a$. Finally, Bob locates the bit errors and applies the σ_x operation to correct them. Here, it is clear that the quantum bit error correction commutes with the Z-basis measurement. Take a simple example, where

$$H_{2\times 3} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \tag{D-1}$$

the circuit is illustrated in Fig. D.1.

邵钰棐2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

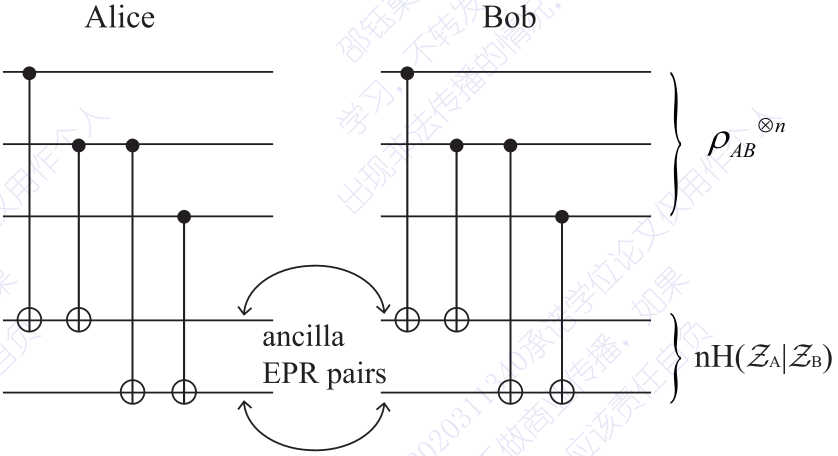


Figure D.1 The circuit for quantum bit error correction. Alice and Bob separately use their state $\rho_{AB}^{\otimes n}$ to control the EPR pairs according to a $nH(\mathcal{Z}_A|\mathcal{Z}_B) \times n$ hashing matrix with $n \to \infty$. Here for clearness we show the schematic with a 2×3 hashing matrix $H_{2\times 3}$ given in Eq. (D-1).

D.2 Analytical solution to Problem 6.1

Lemma D.1： If the four diagonal elements of the density matrix in Eq. (6-26) satisfy $m_{00}/m_{33} = m_{11}/m_{22} = \frac{\alpha}{1-\alpha}$ (or $m_{00}/m_{33} = m_{22}/m_{11}$), the minimal coherence obtained from the optimization in Problem 6.1 is $H(\alpha) - H\left(\frac{1}{2} + \sqrt{(\alpha - \frac{1}{2})^2 + (\frac{1}{2} - e_p)^2}\right)$, with the solution $\bar{a} = (1 - e_b)(1/2 - e_p)$ and $\bar{b} = e_b(1/2 - e_p)$.

Proof. Here, we only consider the case $m_{00}/m_{33} = m_{11}/m_{22}$, and the proof for the other case $\bar{m}_{00}/\bar{m}_{33} = \bar{m}_{22}/\bar{m}_{11}$ can proceed in similar way.

Due to the additivity property of coherence, we can express the coherence of $\rho(a, b)$ like Eq.(6-7) as,

$$C(\rho(a, b)) = (1 - e_b)C(\rho^+) + e_b C(\rho^-) \tag{D-2}$$

where $\rho^{+(-)} = \Pi^{+(-)}\rho(a, b)\Pi^{+(-)}/\mathrm{Tr}(\Pi^{+(-)}\rho(a, b))$. With $m_{00}/m_{33} = m_{11}/m_{22} = \frac{\alpha}{1-\alpha}$, we can explicitly write down the matrix form of $\rho^{+(-)}$ as,

$$\rho^+ = \begin{pmatrix} \alpha & a' \\ a' & 1-\alpha \end{pmatrix}, \quad \rho^- = \begin{pmatrix} \alpha & b' \\ b' & 1-\alpha \end{pmatrix}, \tag{D-3}$$

where $(1 - e_b)a' = a$ and $e_b b' = b$.

The relative entropy of coherence of the state ρ^+ is,

$$C(\rho^+) \quad = \quad S(\Delta(\rho^+)) - S(\rho^+), \tag{D-4}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播的情况，如果出现非法传播，应该责任自负

$$= H(\alpha) - H\left(\frac{1}{2} + \sqrt{(\alpha - \frac{1}{2})^2 + |a'|^2}\right),$$

where $\Delta(\cdot)$ is the dephasing operation of $\{|00\rangle, |11\rangle\}$ basis. For simplicity, we denote $g(x) = \frac{1}{2} + \sqrt{\gamma + x^2}$, where $\gamma = (\alpha - \frac{1}{2})^2$, hence

$$C(\rho^+) = H(\alpha) - H(g(|a'|)). \tag{D-5}$$

And similarly for ρ^-, we have

$$C(\rho^-) = H(\alpha) - H(g(|b'|)). \tag{D-6}$$

In fact, $g(x)$ is a monotonically increasing convex function, on account of

$$\begin{aligned} g'(x) &= \frac{x}{\sqrt{\gamma + x^2}} \geq 0, \\ g''(x) &= \frac{\gamma}{(\gamma + x^2)^{\frac{3}{2}}} > 0. \end{aligned} \tag{D-7}$$

Moreover we can show that $H\big(g(x)\big)$ is a concave function. Specifically, for two variables x_1, x_2 with probability p_1, p_2,

$$\sum_i p_i H\big(g(x_i)\big) \leq H\Big(\sum_i p_i g(x_i)\Big) \leq H\Big(g\Big(\sum_i p_i x_i\Big)\Big), \tag{D-8}$$

where the summation $i = 1, 2$. The first inequality is due to the concavity of the entropy function $H(x)$. The second inequality holds because of three facts: $g(x)$ is a convex function, i.e., $\sum_i p_i g(x_i) \geq g\Big(\sum_i p_i x_i\Big)$; $g(x)$ is larger than $\frac{1}{2}$; $H(x)$ monotonically decreases as $x \geq \frac{1}{2}$.

Then inserting Eq. (D-5) and (D-6) into Eq. (D-2), and utilizing the concavity of $H(g(x))$, we have

$$\begin{aligned} C(\rho(a,b)) &= H(\alpha) - (1 - e_b)H(g(|a'|)) - e_b H(g(|b'|)) \\ &\geq H(\alpha) - H(g((1 - e_b)|a'| + e_b|b'|)), \end{aligned} \tag{D-9}$$

where the equality holds when $|a'| = |b'|$.

Remembering that the coherence $C(\rho(a,b))$ should be minimized under the constraint $a + b = (1 - e_b)a' + e_b b' = \frac{1}{2} - e_p$, we have

$$(1 - e_b)|a'| + e_b|b'| \geq |(1 - e_b)a' + e_b b'| = |\frac{1}{2} - e_p|, \tag{D-10}$$

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

where the equality is saturated when a' and b' share the same sign. Consequently, following Eq. (D-9), we have

$$\begin{aligned} C(\rho(a,b)) &\geq H(\alpha) - H(g((1-e_b)|a'| + e_b|b'|)) \\ &\geq H(\alpha) - H(g(|\tfrac{1}{2} - e_p|)), \end{aligned} \tag{D-11}$$

where the second inequality holds since $H(g(x))$ is a monotonically decreasing function. And the inequality is saturated when $\bar{a} = (1-e_b)(1/2 - e_p)$ and $\bar{b} = e_b(1/2 - e_p)$. ■

D.3 Derivation of the key rate K in Eq. (6-73)

Here we derive the key rate for the symmetric attack scenario, where the key is generated from Z-basis bit of ρ_{AB}^{Z}. Under the symmetric assumption in Eq. (6-68), the four diagonal elements in Z-basis of ρ_{AB}^{Z} are, $2c\frac{\eta_0}{\eta_0+\eta_1}$, $2d\frac{\eta_1}{\eta_0+\eta_1}$, $2d\frac{\eta_0}{\eta_0+\eta_1}$, and $2c\frac{\eta_1}{\eta_0+\eta_1}$ respectively. And the phase error e_p' is given by Eq. (6-72). Consequently, the coherence minimization of Problem 6.1 becomes,

$$\rho(a,b) = \begin{pmatrix} 2c\frac{\eta_0}{\eta_0+\eta_1} & 0 & 0 & a \\ 0 & 2d\frac{\eta_1}{\eta_0+\eta_1} & b & 0 \\ 0 & b & 2d\frac{\eta_0}{\eta_0+\eta_1} & 0 \\ a & 0 & 0 & 2c\frac{\eta_1}{\eta_0+\eta_1} \end{pmatrix}. \tag{D-12}$$

where $a + b = \frac{1}{2} - e_p'$. It is not hard to find that this minimization satisfies the condition in Lemma D.1 with $\alpha = \frac{\eta_0}{\eta_0+\eta_1}$. Hence according to Theorem 6.2 the key rate reads,

$$\begin{aligned} K &= H(\alpha) - H\left(1/2 + \sqrt{(\alpha - \frac{1}{2})^2 + (\frac{1}{2} - e_p')^2}\right) - H(e_b) \\ &= H(\alpha) - H\left(1/2 + \sqrt{(\alpha - \frac{1}{2})^2 + \alpha(1-\alpha)(1-2e_p)^2}\right) - H(e_b), \end{aligned} \tag{D-13}$$

where Eq. (6-72) is applied in the third line to express e_p' with e_p. If we substitute x for α in the above equation, we get the key rate in Eq. (6-73) in the main part.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

D.4 Proof of Proposition 6.1

From Eq. (6-7), one has $C(\Phi(\rho_{AB})) = (1 - e_b)C(\rho^+_{AB}) + e_b C(\rho^-_{AB})$. By definition [Baumgratz et al. (2014)],

$$\begin{aligned} C(\rho^+_{AB}) &= S(\rho^{+\mathrm{diag}}_{AB}) - S(\rho^+_{AB}) \\ &= S(\rho^+_B) - S(\rho^+_{AB}), \end{aligned} \tag{D-14}$$

where $\rho^+_B = \mathrm{Tr}_B(\rho^+_{AB})$. Here in the second line we utilize the fact that $S(\rho^+_B) = S(\rho^{+\mathrm{diag}}_{AB})$, since ρ^+_{AB} is in the Π^+ subspace. Similarly, one has

$$C(\rho^-_{AB}) = S(\rho^-_B) - S(\rho^-_{AB}). \tag{D-15}$$

As a result,

$$\begin{aligned} K(\rho_{AB}) &= C(\Phi(\rho_{AB})) - H(e_b) \\ &= (1 - e_b)\Big(S(\rho^+_B) - S(\rho^+_{AB})\Big) + e_b\Big(S(\rho^-_B) - S(\rho^-_{AB})\Big) - H(e_b) \\ &= (1 - e_b)S(\rho^+_B) + e_b S(\rho^-_B) - \Big((1 - e_b)S(\rho^+_{AB}) + e_b S(\rho^-_{AB}) + H(e_b)\Big), \\ &\leq S((1 - e_b)\rho^+_B + e_b\rho^-_B) - S(\Phi(\rho_{AB})), \\ &= S\Big((1 - e_b)\mathrm{Tr}_A(\rho^+_{AB}) + e_b\mathrm{Tr}_A(\rho^-_{AB})\Big) - S(\Phi(\rho_{AB})), \\ &= S(\mathrm{Tr}_A(\Phi(\rho_{AB}))) - S(\Phi(\rho_{AB})), \end{aligned} \tag{D-16}$$

where the inequality in the fourth line is due to the concavity of entropy.

D.5 Comparison with the Devetak-Winter formula

The Devetak-Winter formula shows that the key rate of state ρ_{AB} in the i.i.d. scenario is $K_{D-W} = S(\mathcal{Z}_A|E) - H(\mathcal{Z}_A|\mathcal{Z}_B)$. This formula considers the one-way information reconciliation protocol. And in this case, the information reconciliation term $H(\mathcal{Z}_A|\mathcal{Z}_B)$ is the same to our formula. Note that our formula Eq.(6.1) can be applied to more general information reconciliation protocols, whereas the Devetak-Winter one is originally designed for one-way postprocessing. Thus, we focus on the first term $S(\mathcal{Z}_A|E)$ which is used to estimate the privacy of the sifted key on Alice's side. In fact, it can be written in the relative entropy form [Coles (2012); Coles et al. (2016)] as

$$S(\mathcal{Z}_A|E) = D(\rho_{AB}\|\Delta_{Z_A}(\rho_{AB})), \tag{D-17}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

where Δ_{Z_A} is the *partial* dephasing operation on system A, i.e., $\Delta_{Z_A}(\rho_{AB}) = \sum_{i=0,1} |i\rangle_A \langle i| \rho_{AB} |i\rangle_A \langle i|$. Here $S(\mathcal{Z}_A|E)$ equals to the amount of basis-dependent *discord* of ρ_{AB} [Modi et al. (2012)].

On the other hand, the term corresponding to privacy, $C(\Phi(\rho_{AB}))$ in our key formula in Eq. (6-2), can also be written in the relative entropy form. By definition [Baumgratz et al. (2014)], we have

$$C(\Phi(\rho_{AB})) = D(\Phi(\rho_{AB})\|\Delta_{Z_{AB}}(\Phi(\rho_{AB})). \tag{D-18}$$

Compared with Eq. (D-17) of Devetak-Winter formula, $C(\Phi(\rho_{AB}))$ quantifies the global coherence of $\Phi(\rho_{AB})$.

It is enlightening to note that using the same fine-grained parameters, one can achieve the same key rate improvement from the Devetak-Winter formula as our coherence framework. Here is the proof. As shown in Eq. (6-26), ρ_{AB} constrained by the fine-grained parameters in the BB84 protocol satisfies $\rho_{AB} = \Phi(\rho_{AB})$. Similarly, Eq. (6-39) shows that $\rho_{AB} = \Phi(\rho_{AB})$ is also satisfied for ρ_{AB} constrained by the fine-grained parameters in the six-state protocol. Therefore, for both protocols, one has

$$\begin{aligned} C(\Phi(\rho_{AB})) &= D(\Phi(\rho_{AB})\|\Delta_{Z_{AB}}(\Phi(\rho_{AB}))) \\ &= D(\Phi(\rho_{AB})\|\Delta_{Z_A}(\Phi(\rho_{AB}))) \\ &= D(\rho_{AB}\|\Delta_{Z_A}(\rho_{AB})) \\ &= S(\mathcal{Z}_A|E) \end{aligned} \tag{D-19}$$

where the second equality employs the fact that $\Delta_{Z_A}(\Phi(\cdot)) = \Delta_{Z_{AB}}(\Phi(\cdot))$ and the third equality employs $\rho_{AB} = \Phi(\rho_{AB})$.

Therefore, with the fine-grained parameters, K_{D-W} is equal to the key rate formula Eq. (6.1). This implies one can derive the same improved key rate formulas, as those in Theorem 6.2 and Theorem 6.3, from the Devetak-Winter formula with fine-grained parameters.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Appendix E Details of IFM as quantum channel discrimination

This section contains details of IFM as quantum channel discrimination in Chapter 7.

E.1 Derivation of the quantum channel $\mathcal{E}_I$ of the generic semitransparent object

In the main part, the generic semitransparent object is composed of a beam splitter and a photon detector. The quantum channel $\mathcal{E}_I$ will be built by combing the operation of the beam splitter and the photon detector in the following.

let us give the channel description of the photon detector first. The photon detector is modeled by a two-level atom with the ground state $|g\rangle$ and the exited state $|e\rangle$ respectively. And the atom staying at $|g\rangle$ interacts with the incident photon mode, denoted by $|p\rangle$. The atom can absorb the photon, transform it to the vacuum state $|v\rangle$ and become to the exited state $|e\rangle$ under the unitary U_{det}; however, the unitary U_{det} does not change the state $|v, g\rangle$, that is,

$$\begin{aligned} U_{\text{det}} |p, g\rangle &= |v, e\rangle , \\ U_{\text{det}} |v, g\rangle &= |v, g\rangle . \end{aligned} \tag{E-1}$$

Then the atom should be measured in the $|g\rangle , |e\rangle$ basis and reset to $|g\rangle$. In fact, we does not need to care about the operation of U_{det} on the other two states, say, $|p, e\rangle$ and $|v, e\rangle$, since the atom always stays at the ground state $|g\rangle$ before the interaction.

Hence, the overall operation on the photon state is:

$$\begin{aligned} \rho_{\text{out}} &= \sum_{i=g,e} \langle i| U_{\text{det}}(\rho_{\text{in}} \otimes |g\rangle \langle g|)U_{\text{det}}^{\dagger} |i\rangle , \\ &= \sum_{i=g,e} \langle i| U_{\text{det}} |g\rangle \rho_{\text{in}} \langle g| U_{\text{det}}^{\dagger} |i\rangle , \end{aligned} \tag{E-2}$$

where ρ_{in} and ρ_{out} are the input and output photon state. Following the standard quantum channel construction method [Nielsen et al. (2010)], the quantum operation in Eq. (E-2)

邵钰棠2020311340承诺学位论文仅作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

can be written down with the Kraus representation as:

$$\begin{aligned}
\rho_{\text{out}} &= \sum_{i=0,1} K_i \rho_{\text{in}} K_i^{\dagger}, \\
K_0 &= \langle g| U_{det} |g\rangle = |v\rangle \langle v|, \\
K_1 &= \langle e| U_{det} |g\rangle = |v\rangle \langle p|.
\end{aligned} \tag{E-3}$$

where K_0, K_1 are the corresponding Kraus operators and we obtain the expressions of them using Eq. (E-1).

For the scenario in the main part, there are three photon modes, i.e., $|1\rangle, |2\rangle, |3\rangle$, except the vacuum one $|v\rangle$, and only $|3\rangle$ can interact with the detector. So the channel should be slightly modified to

$$\begin{aligned}
\mathcal{E}_{det}(\cdot) &= \sum_{i=0,1} D_i (\cdot) D_i^{\dagger}, \\
D_0 &= |1\rangle \langle 1| + |2\rangle \langle 2| + |v\rangle \langle v|, \\
D_1 &= |v\rangle \langle 3|.
\end{aligned} \tag{E-4}$$

where D_0, D_1 are the corresponding Kraus operators.

On the other hand, the matrix representation of the unitary for the beam splitter U_{b} in the $|1\rangle, |2\rangle, |3\rangle, |v\rangle$ basis shows

$$U_{\text{b}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & -\sqrt{1-a^2} & 0 \\ 0 & \sqrt{1-a^2} & a & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{E-5}$$

Combing the two operations of the photon detector $\mathcal{E}_{\text{det}}$ and the beam splitter U_b, we have the combined channel being

$$\mathcal{E}_{\text{com}}(\cdot) = \sum_{i=0,1} D_i U_b (\cdot) U_b^{\dagger} D_i^{\dagger}, \tag{E-6}$$

and the corresponding Kraus operators $C_i = D_i U_b$ show

$$\begin{aligned}
C_0 &= |1\rangle \langle 1| + a\, |2\rangle \langle 2| - \sqrt{1-a^2}\, |2\rangle \langle 3| + |v\rangle \langle v|, \\
C_1 &= \sqrt{1-a^2}\, |v\rangle \langle 2| + a\, |v\rangle \langle 3|.
\end{aligned} \tag{E-7}$$

In fact, the component $|3\rangle$ is redundant as it is introduced to illustrate the intermediate process between the beam splitter and the photon detector. Remembering that the beam

邵钰棻2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

splitter and the photon detector as a whole represent the semitransparent object, thus we can treat them together as a black box and the photon state in IFM equivalently lives in the three dimensional space $\mathcal{H}_{12v} = spanned\{|1\rangle, |2\rangle, |v\rangle\}$. As a result, without altering the function of the channel that represents the semitransparent object, we can eliminate the terms in the above Kraus operator (Eq. (E-7)) that relate to the component $|3\rangle$ and get

$$\begin{aligned} A_0 &= |1\rangle\langle 1| + a|2\rangle\langle 2| + |v\rangle\langle v|, \\ A_1 &= \sqrt{1-a^2}\,|v\rangle\langle 2|, \end{aligned} \tag{E-8}$$

where we use A_0 and A_1 to denote the new Kraus operators.

Further more, actually, we can substitute the loss state $|3\rangle$ for the vacuum state $|v\rangle$ in the above Kraus operators to obtain the effective channel in the main part (Eq. (7-16)), since using which label to count the photon loss probability is equivalent here. The physical insight behind this is that the component $|3\rangle$ reflected by the beam splitter should be absorbed totally by the photon detector, i.e., dephased and transformed to the vacuum state $|v\rangle$.

E.2 Non-increasing of the generalized trace distance under quantum operation

Here, we first give the definition of the generalized trace distance as follows.

Definition E.1: The generalized trace distance for the two quantum state ρ_1 and ρ_2 shows,

$$D_q(\rho_1, \rho_2) = \|q\rho_1 - (1-q)\rho_2\|, \tag{E-9}$$

where $\|\cdots\|$ is the trace norm and $0 \le q \le 1$ is the corresponding probability factor.

Note that $D_{1/2}(\rho_1, \rho_2)$ is the original trace distance [Nielsen et al. (2010)]. Then we show the property of the generalized trace distance in the following Theorem.

Theorem E.1: suppose $\Lambda(\cdot)$ is a trace preserving quantum operation, then it is contradictive for the generalized trace distance, i.e.,

$$D_q(\rho_1, \rho_2) \ge D_q(\Lambda(\rho_1), \Lambda(\rho_2)). \tag{E-10}$$

To prove Th. E.1 conveniently, we show another equivalent definition for the generalized trace distance $D_q(\rho_1, \rho_2)$.

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Lemma E.1：

$$D_q(\rho_1, \rho_2) = \mathrm{Tr}_{max}[(P_1 - P_0)M], \tag{E-11}$$

where we use $M = q\rho_1 - (1-q)\rho_2$ for simplicity; and the maximization is over all projector pairs P_0, P_1 that satisfy $P_0 + P_1 = \mathbb{I}$.

Proof. M is a hermit matrix by definition, thus we can use unitary to diagonalize it to $UMU^\dagger$, and by separating the eigenvalues to nonnegative and negative parts we can obtain $UMU^\dagger = Q' - S'$. As a result, we can represent M as the subtraction of the two nonnegative matrices $M = U^\dagger(Q' - S')U = Q - S$, and $||M|| = ||Q - S|| = Tr(Q) + Tr(S)$. Then for any projector pair P_0, P_1,

$$\begin{aligned}
\mathrm{Tr}[(P_1 - P_0)M] &= Tr[(P_1 - P_0)(Q - S)],\\
&\leq \mathrm{Tr}[P_1 Q + P_0 S],\\
&\leq \mathrm{Tr}(Q) + \mathrm{Tr}(S),\\
&\leq ||M||.
\end{aligned} \tag{E-12}$$

We can choose P_0 and P_1 just the projectors on the two orthogonal subspace where Q and S lives respectively, then $Tr[(\Pi_1 - \Pi_0)M]$ can reach $||M||$ in this way and we finish the proof. ■

Then we prove Th. E.1 with the help of Lemma. E.1.

Proof.

$$\begin{aligned}
\|M\| &= Tr(Q) + Tr(S),\\
&= Tr[\Lambda(Q) + \Lambda(S)],\\
&\geq Tr[(P_1' - P_0')(\Lambda(Q) - \Lambda(S))],\\
&= Tr[(P_1' - P_0')\Lambda(M)],\\
&= \|\Lambda(M)\|,
\end{aligned} \tag{E-13}$$

where P_0' and P_1' are the projector pair used to reach the maixmal value $\|\Lambda(M)\|$, referring to Lemma. E.1. Then, by substituting $M = q\rho_1 - (1-q)\rho_2$, we finish the proof. ■

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

E.3 Proof of Lemma. 7.1

Here, we give the proof of Lemma. 7.1 in the main part that says

$$\|p|\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2|\| = \sqrt{(p+1)^2 - 4p|\langle\psi_1|\psi_2\rangle|^2}.$$

Proof. $|\psi_1\rangle\langle\psi_1|$ can be expressed as $\frac{1}{2}(I + \sigma_z)$ in the basis of itself. Since $|\psi_2\rangle\langle\psi_2|$ does not change if we change the global phase of it, we have $|\psi_2\rangle = \cos\frac{\gamma}{2}|\psi_1\rangle + \sin\frac{\gamma}{2}|\psi_3\rangle$ $(0 \le \gamma \le \pi/2)$, where $|\psi_3\rangle$ is the state orthogonal to $|\psi_1\rangle$. Then $|\psi_2\rangle\langle\psi_2|$ shows $\frac{1}{2}(I + \cos\gamma\sigma_z + \sin\gamma\sigma_x)$. And the trace norm $\|p|\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2|\| = \frac{1}{2}\|(p-1)I + (p - \cos\gamma)\sigma_z - \sin\gamma\sigma_x\|$. The two eigenvalues of $(p-1)\mathbb{I} + (p-\cos\gamma)\sigma_z - \sin\gamma\sigma_x$ are $(p-1) \pm \sqrt{(p-\cos\gamma)^2 + \sin^2\gamma}$. Hence $\|p|\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2|\| = \sqrt{(p-\cos\gamma)^2 + \sin^2\gamma} = \sqrt{(p+1)^2 - 4p\cos^2\frac{\gamma}{2}} = \sqrt{(p+1)^2 - 4p|\langle\psi_1|\psi_2\rangle|^2}$ ■

E.4 The effect of quantum correlation in IFM considering P_{error} and P_f

In this appendix, we will give the detailed illustration of the argument in the main part of our article that quantum correlation can not benefit the IFM process considering P_{error} and P_f respectively.

For simplicity, we substitute for the terms in Eq. (7-64) by:

$$\begin{aligned} \lambda_1 &= qTr[C^\dagger C\rho_A] + (1-q), \\ \lambda_2 &= 2\sqrt{q(1-q)}|Tr[D^\dagger C\rho_A]|. \end{aligned} \tag{E-14}$$

As a result, Eq. (7-64) becomes to a more concise form,

$$P_{\text{error}} = \frac{1}{2}(\lambda_1 - \sqrt{\lambda_1^2 - \lambda_2^2}). \tag{E-15}$$

It is not difficult to see that P_{error} monotonically decreases with the increasing of λ_1 due to the first order partial derivative on λ_1 being

$$\frac{\partial P_{\text{error}}}{\partial\lambda_1} = \frac{1}{2}(1 - \frac{\lambda_1}{\sqrt{\lambda_1^2 - \lambda_2^2}}) \le 0. \tag{E-16}$$

In the meantime, it's obvious that P_{error} decreases with the decreasing of λ_2. Consequently, increasing λ_1 and decreasing λ_2 at the same time can minimize P_{error}.

Here, with the help of Eqs. (7-57), (7-61) and (7-62), we present the expressions for

邵钰菓2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

$Tr[C^\dagger C\rho_A]$, $Tr[D^\dagger C\rho_A]$ in the definitions of λ_1 and λ_2 explicitly as

$$\begin{aligned} Tr[C^\dagger C\rho_A] &= (\frac{1-a}{2})^{2N}[f_1^2(1+k_1^2)+f_2^2+2f_1(f_2r_z-f_1k_1r_x)], \\ Tr[D^\dagger C\rho_A] &= (\frac{1-a}{2})^{N}[f_1k_1-f_1r_x+if_2r_y]. \end{aligned} \tag{E-17}$$

The above equations shows that for a fixed r_x, we can always increase λ_1 and decrease λ_2 (i.e., decrease P_{error}) by changing $r_y=0$ and $r_z=\sqrt{1-r_x^2}$. In other words, the minimum of P_{error} should be reached by pure state $\rho_A=|\varphi_A\rangle\langle\varphi_A|$ of photon A part. Thus, entangled photon input state can not enhance the performance for P_{error} in all k_1 regime, compared with single photon input state.

Moreover, we consider the effect of quantum correlation to IFM process, with a more effective criteria $P_f=P_{\text{loss}}+P_{\text{error}}$, which describing all the failure probability in IFM process. Owing to Th. 7.1, P_f also shows the following concave property like P_{error},

$$P_f \geq p_iP_f^i. \tag{E-18}$$

That is to say, the minimum of P_f should be reached by the pure state and the quantum correlation here means entanglement. With the help of Eqs. (7-56), (7-64) and (E-14) , we have P_f being

$$P_f = 1-\frac{1}{2}(\lambda_1+\sqrt{\lambda_1^2-\lambda_2^2}). \tag{E-19}$$

P_f also decreases with the increasing of λ_1 and decreasing of λ_2. Consequently, just like the aforementioned reason for P_{error}, we can also argue that entanglement can not enhance the performance of IFM considering P_f.

E.5 Derivation of Eq. (7-67)

Here, we give the derivation of $(P_{\text{loss}})_{min}^{N\to\infty}$ in Eq. (7-67), which is the asymptotic behaviour of $Eq.$ (7-58) as $N\to 0$.

First, utilizing the same approximation technique used in $Eq.$ (7-65) in the main part, we get

$$\begin{aligned} &(\frac{1-a}{2})^N(\Sigma_2-\Sigma_1)=O(a^N)\to 0, \\ &(\frac{1-a}{2})^N\Sigma_1 \simeq (\frac{1-a}{2})^N\Sigma_2=\frac{1}{2}-\frac{1+a}{1-a}\frac{\pi^2}{16N}+O(\frac{1}{N^3}). \end{aligned} \tag{E-20}$$

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

Then, let us consider the asymptotic behavior of $Eq.$ (7-58), the minimum of P_{loss}. By applying $Eq.$ (7-52), (7-54) and the definitions of k_1, k_2 (Eq. (7-50)), we have

$$\begin{aligned}
&(\frac{1-a}{2})^{2N}(f_1+\sqrt{f_2^2+f_1^2k_1^2})^2,\\
\simeq&(\frac{1-a}{2})^{2N}(f_1+f_2+\frac{f_1^2}{2f_2}k_1^2)^2,\\
=&(\frac{1-a}{2})^{2N}(\frac{\Sigma_1}{\sqrt{1-k_1^2}}+\Sigma_2+\frac{\Sigma_1^2}{2\Sigma_2}\frac{k_1^2}{1-k_1^2})^2,\\
\simeq&(\frac{1-a}{2})^{2N}[\Sigma_1(1+\frac{k_1^2}{2})+\Sigma_2+\frac{\Sigma_1^2}{2\Sigma_2}k_1^2(1+k_1^2)]^2,\\
\simeq&(\frac{1-a}{2})^{2N}[(\Sigma_1+\Sigma_2)+\frac{k_1^2}{2}\Sigma_1(1+\frac{\Sigma_1}{\Sigma_2})]^2,\\
\simeq&[1-\frac{1+a}{1-a}\frac{\pi^2}{8N}+(\frac{1+a}{1-a})^2\frac{\pi^2}{8N^2}+O(\frac{1}{N^3})]^2,\\
\simeq&1-\frac{1+a}{1-a}\frac{\pi^2}{4N}+O(\frac{1}{N^2}).
\end{aligned}\tag{E-21}$$

where in the next-to-last row, we employ the equalities in Eq. (E-20). So the asymptotic expression of $Eq.$ (7-58) is

$$(P_{\text{loss}})_{min}^{N\to\infty}\simeq q[\frac{1+a}{1-a}\frac{\pi^2}{4N}-O(\frac{1}{N^2})].$$

just as Eq. (7-67) describes in the main part.

邵钰棠2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负

个人简历、在学期间发表的学术论文与研究成果

个人简历

1992 年 8 月 27 日出生于陕西省商洛市。

2010 年 9 月考入浙江大学信息与电子工程学系，2014 年 7 月本科毕业并获得工学学士学位。

2014 年 9 月免试进入清华大学交叉信息研究院攻读物理学位至今。

发表的学术论文

[1] You Zhou, Qi Zhao, Xiao Yuan and Xiongfeng Ma, Polynomial measure of coherence, New Journal of Physics 19 123033 (Dec 2017); (SCI 收录，Accession Number: WOS:000418158900003, impact number 3.579)

[2] You Zhou, Man-Hong Yung, Interaction-free measurement as quantum channel discrimination, Physical Review A.96.062129 (Dec 2017); (SCI 收录，Accession Number: WOS:000418614300002, impact number 2.909)

[3] You Zhou, Chenghao Guo, Xiongfeng Ma, Decomposition of a symmetric multipartite observable, Physical Review A.99.052324 (May 2019); (SCI 收录，Accession Number: WOS:000468202500003, impact number 2.909)

Arxiv preprints

[4] You Zhou, Qi Zhao, Xiao Yuan, Xiongfeng Ma, Efficient detection of multipartite entanglement structure, arXiv:1904.05001

[5] Jiajun Ma, You Zhou, Xiao Yuan, Xiongfeng Ma, Operational interpretation of coherence in quantum key distribution, arXiv:1810.03267(Accepted by Phys. Rev. A (2019) 共同第一作者);

邵钰蕖2020311340承诺学位论文仅用作个人学习，不转发不做商业传播，如果出现非法传播的情况，应该责任自负