

量子糾纏態與量子資訊處理

Entanglement and Quantum Information Processing

研究生：李哲明

Student : Che-Ming Li

指導教授：褚德三

Advisor : Der-San Chuu

國立交通大學

電子物理研究所

博士論文

A Thesis

Submitted to Institute of Electrophysics

College of Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

in

Electrophysics

February 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年二月

Entanglement and Quantum Information Processing



Che-Ming Li

March 3, 2008

量子糾纏態與量子資訊處理

研究生：李哲明

指導教授：褚德三

國立交通大學
電子物理研究所

摘要

本論文提出量子糾纏與量子資訊處理的理論與實驗研究成果。我們引進且利用系統性的方法分析量子多體糾纏態的關連結構並偵測隱含於多體多維物理系統中的量子關連，我們亦提出了嶄新的量子方案以實現量子糾纏態的製造、純化、量子糾錯及量子搜尋演算法；這些理論方法與結果有助於了解量子力學的基本特徵並開發量子訊息領域中的相關應用。

在實驗工作方面，我們發展並開發了用於實現單向量子計算的二光子四量子位元糾纏源。利用高亮度糾纏源所產生的二光子量子態在偏振與空間自由度上的糾纏特性，我們實現了高效率的量子搜尋演算法，此實驗結果顯示二光子超糾纏態可作為快速且精確的光學量子計算之基礎。

ENTANGLEMENT AND QUANTUM INFORMATION PROCESSING

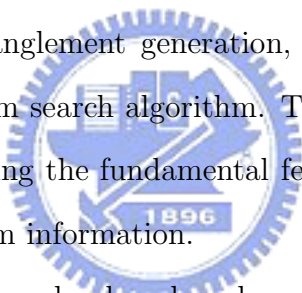
Student: Che-Ming Li

Advisor: Der-San Chuu

Department of Electrophysics
National Chiao-Tung University

Abstract

The present thesis shows the result of theoretical and experimental study on the physics of entanglement and quantum information processing. We propose a systematic approach to analyze the correlation structures of multipartite entanglement and detect genuine quantum correlations inherent in multipartite multi-level systems. In addition, we introduce novel proposals for entanglement generation, entanglement purification, quantum error corrections, and quantum search algorithm. These theoretical methods and results are both significant for studying the fundamental feature of quantum mechanics and for exploiting the field of quantum information.

The logo of National Chiao-Tung University is a circular emblem. It features a central design with a book and a torch, symbolizing knowledge and enlightenment. The year '1896' is inscribed at the bottom of the emblem. The entire logo is rendered in a light blue color and is positioned behind the abstract text.

The experimental work has developed and exploited a source of two-photon four quantum-bit entanglement to realize one-way quantum computing. With the bright source which produces a two-photon state entangled both in polarization and spatial modes, we implemented a highly efficient quantum search algorithm. The experimental result demonstrates that such hyperentangled states could serve as a building block of rapid and precise optical quantum computation.

誌謝

我感謝指導老師褚德三教授在我的博士生研究階段的指導與支持，得以將此論文完成。於褚教授在物理與研究工作的鼓勵及引領下，增進了專業的知識，並培養了寶貴的科學研究基本態度；我也要感謝褚教授對本論所提出的意見與評論，使本論文趨於完整、充實。

我感謝在海德堡大學物理研究所的指導老師 Pan Jian-Wei 教授，引領我進入實驗光學量子資訊的領域，讓我學習到重要的實驗技術與知識，於此獲得實驗與理論相印證之可貴的經驗，亦因此打開了科學研究之視野，也增進了研究的深度與廣度。

我要感謝在大學階段就帶領我進入量子資訊領域的黃吉川教授。黃教授深遠的科學研究目標，我因而幸運受益在此研究道路上持續前行，也因受黃教授的科學研究態度的影響，讓我在重要的科研初步就一直保有熱情至今日。

我也要感謝王國雄教授在碩士班階段的指導，在研究主題上的協助與相關行政事物的熱情幫忙，我因而可以進入下一個重要的研究階段，除此之外，我也學習到許多做事的態度與待人的道理。

我對於曾經一同在研究工作上努力的夥伴們表達我由衷的謝意。我感謝謝金源教授在許多研究課題上的指導，藉由每次深入的討論，培養出重要的解決問題之獨到技巧與方法，也藉此更正了許多錯誤的觀念，進而增進科學研究的興趣與正確的態度；我感謝陳岳男教授引領我討論許多重要的物理研究主題，與在研究工作上的關心、協助與鼓勵，我因此能持續探索有趣的科學問題；我感謝徐立義教授在許多研究課題上對我的啟發，讓我在相互討論中成長；我感謝蘇正耀教授在其所開的課程中教導我量子資訊的基本知識，進而對重要主題有深入的了解與啟發；我感謝 Chen Kai 博士在海德堡的實驗研究裡幫助我釐清許多重要問題，也因重要的實驗瓶頸的突破，使我獲益許多，更是一位絕佳的實驗夥伴；我感謝 Zhang Qiang 博士在海德堡的實驗室耐心地教導我基礎的光學實驗技術，也藉由在實驗問題的討論裡，更正了許多量子力學中的重要觀念；我感謝 Alexander Goebel 熱心地以啟發性的方法帶領我在基礎光學實驗室學習基本的實驗技巧；我也要感謝參與多體糾纏與量子計算實驗的夥伴：Chen Yu-Ao 博士，Chen Shuai 博士，Alois Mair 博士，Yuan Zhen-Sheng 博士，協助我克服許多實驗瓶頸與問題。我要感謝 Tobias Brandes 教授在糾纏態偵測上給予的重要意見，我也要感謝林秀豪教授與羅志偉教授在研究條件量測引致糾纏問題的時期給予的慷慨協助與討論。

我要謝謝研究室裡的夥伴林高進博士、邱裕煌、廖英彥博士、院繼祖、陳光胤、王律堯博士、趙國勝博士的勉勵與照顧，重要地，我要感謝簡騰瑞教授一路上的協助與幫忙，從大學部、碩士班以至博士班的友情支持。

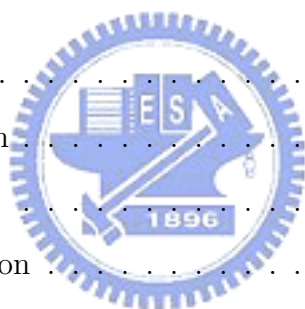
最後，我感激我親愛的父親、母親、哥哥、大嫂、姊姊與姊夫，以及敬愛的義父義母，沒有您們的支持我無法完成這系列的研究工作。也謝謝許多教過我的老師與幫助過我的朋友們。

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 1 |
| 1.1 | Entanglement, EPR paradox, and Bell's theorem | 1 |
| 1.2 | Entanglement and quantum information processing | 3 |
| 1.3 | Entanglement detections, purifications, and quantum error corrections | 6 |
| 1.4 | Experimental generations of quantum entanglement | 8 |
| 1.5 | Outline of the Thesis | 9 |
| 2 | Entanglement and correlation conditions | 12 |
| 2.1 | Introduction | 12 |
| 2.2 | Correlation condition and entanglement detection | 14 |
| 2.3 | Quantum correlations imbedded in entangled states | 21 |
| 2.3.1 | Correlation structures of many-qubit GHZ states | 21 |
| 2.3.2 | Correlation conditions for bipartite arbitrary-dimensional Bell states | 24 |
| 2.4 | Correlators embedded in Bell inequalities | 29 |
| 2.4.1 | Bell inequalities for many qubits | 29 |
| 2.4.2 | Bell inequalities for two qudits | 31 |
| 2.5 | Correlators imbedded in entanglement witness operators | 39 |
| 2.5.1 | Detections of genuine many-qubit GHZ states | 40 |
| 2.5.2 | Inequalities based on the geometry of spin vectors | 41 |
| 2.5.3 | Detecting entangled qudits with two local measurement settings | 46 |
| 2.5.4 | Witnesses composed of the kernels of Bell inequalities for qudits | 53 |

| | | |
|----------|--|------------|
| 2.6 | Conclusion | 55 |
| 3 | Correlation conditions in the stabilizer formalism | 57 |
| 3.1 | Introduction | 57 |
| 3.2 | Stabilizer formalism | 58 |
| 3.3 | Entanglement witnesses for stabilizer states | 63 |
| 3.4 | Correlator-based Bell inequalities for many-qubit graph states | 64 |
| 4 | Entanglement detection via the condition of quantum correlation | 66 |
| 4.1 | Method | 66 |
| 4.2 | Generalized GHZ states | 67 |
| 4.3 | Four-qubit singlet state | 72 |
| 4.4 | Three-qubit W state | 75 |
| 4.5 | Conclusion | 77 |
| 5 | Phase-dependent criterion for many-qudit entanglement | 78 |
| 5.1 | Motivation | 78 |
| 5.2 | Basic idea | 79 |
| 5.3 | Many-qudit Bell inequalities | 81 |
| 5.4 | Entanglement witnesses for many-qudit entangled states | 84 |
| 5.5 | Conclusion and outlook | 88 |
| 6 | Entanglement purification | 89 |
| 6.1 | Background and motivation | 89 |
| 6.2 | Basic idea of entanglement purification | 90 |
| 6.3 | Entanglement purification with a two-map protocol | 95 |
| 6.4 | Conclusion | 101 |
| 7 | Quantum error-correcting codes and entanglement purification | 103 |
| 7.1 | Introduction | 103 |

| | | |
|-----------|--|------------|
| 7.2 | The 5-EPR-pair single-error-correcting code | 105 |
| 7.3 | Analytical technique for simplification of the encoder-decoder circuit for a perfect five-qubit error correction | 110 |
| 7.3.1 | Theory | 110 |
| 7.3.2 | A systematic scenario example | 114 |
| 7.4 | The encoder-decoder circuit for a perfect five-qubit error correction | 121 |
| 7.5 | Conclusion | 125 |
| 8 | Generation of many-qubit entanglement via conditional measurements on cavity photons | 127 |
| 8.1 | Introduction | 127 |
| 8.2 | Bell states generation | 129 |
| 8.3 | Multi-qubit W state | 131 |
| 8.4 | Quantum teleportation | 135 |
| 9 | Quantum search algorithm | 137 |
| 9.1 | Quantum search problem | 137 |
| 9.2 | Quantum searching with certainty | 138 |
| 9.3 | An improved phase error tolerance in quantum search algorithm | 146 |
| 9.4 | On a family of quantum search algorithms robust against phase imperfections | 152 |
| 9.5 | Hamiltonian and measuring time for analog quantum search | 158 |
| 10 | Experimental generation of hyperentangled photons and experimental realization of one-way quantum computing | 168 |
| 10.1 | Introduction | 168 |
| 10.2 | Photon source for polarization entanglement | 169 |
| 10.3 | Experimental generation of two-photon four-qubit hyperentangled states | 171 |



CONTENTS

| | |
|--|------------|
| 10.4 Experimental demonstration of quantum search algorithm with an one-way quantum computer | 175 |
| 10.4.1 One-way quantum computation | 175 |
| 10.4.2 Experimental realization of one-way quantum search | 178 |
| 10.5 Conclusion | 179 |
| 11 Summary and Outlook | 180 |
| 11.1 Summary | 180 |
| 11.2 Outlook | 182 |
| A Tightness of Bell inequalities | 188 |
| B Entanglement witnesses of stabilizer states | 190 |
| C Entanglement witnesses of entangled qudits | 191 |



List of Figures

| | | |
|-----|--|-----|
| 6.1 | The standard purification LOCC operations including the local controlled-NOT operation, single qubit measurement, and local unitary operation in each party. Note that the classical communication is not shown in this figure. | 91 |
| 6.2 | The variations of the yield and the comparing purity (in the inserted diagram) at ten times of the recurrence method. | 97 |
| 6.3 | The variations of the yield and the comparing purity (in the inserted diagram) at five times of the recurrence method. | 98 |
| 6.4 | The variations of the improved yields $Y'_{5, TM1}$ and $Y'_{5, Ox}$ and the comparing ratio ($Y'_{5, TM1}/Y'_{5, Ox}$) (in the inserted diagram). | 100 |
| 7.1 | The 1-EPP with notations used in the context. Alice performs U_1 and m and then sends her classical result (v_A) to Bob. Bob performs U_2 and m , and then combines his own result (v_B) and Alice's to control a final operation $U_3^{(i)}$. | 106 |
| 7.2 | The three quantum gate arrays performed in the stage of row operations: (a) for $\mathbf{M}_1 \rightarrow \mathbf{M}'_1$; (b) for $\mathbf{M}'_1 \rightarrow \mathbf{M}''_1$; and (c) for $\mathbf{M}''_1 \rightarrow \mathbf{1}$. | 118 |
| 7.3 | The gate array for the transformation $\mathbf{M}_1 \rightarrow \mathbf{1}$. The basic unitary operations are performed in the order from left to right, while if they are performed from right to left, then the inverse transformation $\mathbf{M}_1 \rightarrow \mathbf{1}$ is accomplished. | 120 |

7.4 The perfect five-qubit error correction. (a) The initial tensor product state is encoded to an entangled state $|\phi_E\rangle$. (b) After suffering from the single-qubit error, the state $E_r^{(i)}|\phi_E\rangle$ is then decoded, resulting in the final tensor product state $(U_3^{(i)}|\phi\rangle)|a'b'c'd'\rangle$. Here, $\mathbf{P} = HQ$, $\mathbf{P}^+ = QH$. (c) The encoder circuit from (a) is rewritten in terms of the gate primitives of an ion-trap quantum computer. 122

8.1 (a) The quantum devices with three dot-like quantum wells embedded in a microcavity which is constructed by a ZnTe medium and two Au mirrors. This device can be prepared by the MBE, the e-beam lithography, and the conventional semiconductor processing. (b) Initial state preparation for W state generation. (c) Evolution of the QWs and cavity field for a specific time period. (d) Detection of cavity field for determining the number of the cavity photon. Procedures (b)-(d) are repeated until finishing the entanglement generation. 128

8.2 The variations of fidelity $F_{N,n}$ and the purification yield $Y_{N,n}$ (in the inserted diagram) for cases $n = 3(\square)$, $6(\nabla)$, and $9(\triangle)$, and for two different kinds of initial states: $\rho = p\mathbf{1} + (1 - np)|L_0\rangle\langle L_0|$ (dash) and $|\psi_0\rangle$ (solid), in which the evolution time of each case, $\tau_3 = \pi/(\sqrt{10}\gamma)$, $\tau_6 = \pi/(\sqrt{22}\gamma)$, and $\tau_9 = \pi/(4\sqrt{2}\gamma)$ has been set. 132

9.1 Variations of $\phi(\theta)$ (solid) and $f(\theta)$ (broken), for $\alpha + u = 0$, $\beta_0 = 10^{-4}$, and $\beta = 10^{-4}$ (1), 10^{-2} (2), 0.5 (3) and 0.7 (4), respectively. The cross marks denote the special case of Høyer [166], while the entire circles correspond to the optimal choices of ϕ_{op} and θ_{op} for $\alpha + u = 0$, $\beta_0 = 10^{-4}$ and $\beta = 0.7$. The solid straight line 1 corresponds the case $\phi = \theta$, while the solid curve 2 is only approximately close to the former. 144

LIST OF FIGURES

9.2 Variations of $\phi(\theta)$ (solid) and $f(\theta)$ (broken), for $\alpha + u = 0.1$, $\beta_0 = 0.1$, and $\beta = 10^{-4}$ (1), 10^{-2} (2), 0.5 (3) and 0.7 (4), respectively. The cross marks denote the special case of Høye [166]. The solid curves 1 and 2 are very close, and both of them are only approximately close to the line $\phi = \theta$. . . 145

9.3 Variations of exact vaule of $P_{\max}(n)$ (cross marks), $16\beta^2 \sin^2(\frac{\theta}{2})/(\delta^2+16\beta^2 \sin^2(\frac{\theta}{2}))$ (solid), and $4\beta^2/(\delta^2+4\beta^2)$ (dash) for $\theta = \pi$, $\delta = 0.01$ where $\beta = \sin^{-1}(2^{-n/2})$.150

9.4 Variations of exact vaule of $P_{\max}(n)$ (cross marks), $16\beta^2 \sin^2(\frac{\theta}{2})/(\delta^2+16\beta^2 \sin^2(\frac{\theta}{2}))$ (solid), and $4\beta^2/(\delta^2+4\beta^2)$ (dash) for $\theta = \pi$, $\delta = 0.001$ where $\beta = \sin^{-1}(2^{-n/2})$.151

9.5 The variation of $\bar{p}(\beta)$ for cases of Bae-Kwon(solid), Farhi-Gutmann(solid), and Fenner(broken) at the specific measuring times, $t_{1,BK} = t_{1,FG} = \pi/(2E_o)$ and $t_{1,F} = (\pi - 2\beta)/(2E_o)$ 164

9.6 Variations of $t_1(\phi - u)$ (broken) and $E_o(\phi - u)$ (solid), for $\beta = 0.085$ (1), $\beta = 0.031$ (2), and $\beta = 0.0055$ (3); 166

10.1 Polarization photon source with two-crystal geometry BBO crystals 170

10.2 Polarization photons emitted from the first BBO crystal 171

10.3 Polarization photons emitted from the second BBO crystal 172

10.4 Schematic of experimental setup. 173

10.5 Quantum circuit for realization of quantum search algorithm. 176

10.6 Box cluster state. 177

10.7 Quantum circuit involved an action of oracle for quantum search. 177

10.8 Quantum circuit composed of four local operations for the step 3 in one way realization. 178

10.9 A successful identification probability of $(96.1 \pm 0.2)\%$ is achieved deterministically with feed-forward, while it is $(24.9 \pm 0.4)\%$ without feed-forward. This depicts that our source of cluster state is ideally suited for such a sort of algorithm's implementation. 179

Chapter 1

Introduction

1.1 Entanglement, EPR paradox, and Bell's theorem

Entanglement is one of fundamental pillars in the field of quantum information [1–4]. The remarkable properties of entanglement go essentially beyond the classical correlation constrained by two plausible assumptions, namely *locality* and *realism* (local realism) [5, 6]. The assumption of realism states that physical properties of objects have definite values which exist independently of their observation, and the one of locality says that in a causally disconnected manner a measurement of a system does not influence the result of measurement of another system at spacelike separation. Local realism is the essence of the view of Einstein, Podolsky, and Rosen (EPR) [7] on *elements of reality*. EPR considered that any element of reality *must* be described by any *complete* physical theory, and by local realism that was *sufficient* for the reality of a physical quantity, they showed that quantum mechanics is incomplete. The criterion of EPR is applied to a composite quantum system comprised of two distant particles with a wave function of the form [8]: $\Psi = \delta(x_2 - x_1 - x_0)\delta(p_1 + p_2)$, where δ denotes a modified delta function, that is normalizable and possesses an arbitrary high-narrow peak, and x_0 is a large distance that is much larger than the range of interaction between particles 1 and 2. From the description of the wave function Ψ , one knows that the total momentum of the system is

close to zero and the relative distance of the particles is close to x_0 . If one measures x_2 , one then can predict with certainty the value of x_1 without having any actual influence on particle 1. Then, according to the criterion of EPR, x_1 corresponds to an element of physical reality. Furthermore, if one measures p_2 , one can predict with certainty the value of p_1 without having any actual influence on particle 1. Therefore, according to the criterion of EPR, p_1 corresponds to an element of physical reality. However, Heisenberg uncertainty principle precludes one from knowing position and momentum simultaneously. Thus EPR considered that quantum mechanics was an incomplete theory.

After EPR's article, Bohr published a response [9] where he gave *the principle of complementarity* and argued that the two particles in the situation considered by EPR are always parts of one quantum system and the measurement performed on the first system determines the possible predictions that can be made for the second particle. In addition to Bohr's reply, Schrödinger [10] claimed that, since the composed system is describe by a single wave function, the two remote particles can influence each other nonlocally. In 1951 Bohm [11] introduced spin-entangled systems and gave a simpler example of the dilemma of EPR. The model of Bohm has become the most studied one for the so-called EPR paradox.

The EPR paradox remained a philosophical discussion until Bell [5] in 1964 introduce *quantitative criteria* for the existence of any local-realistic theory. Bell derived correlation inequalities to show that there is an upper limit to the correlation predicted by local-realistic theories whereas the upper bound can be violated by correlations imbedded in entangled states. The inequalities advocated by Bell are experimental testable. Experiments with entangled pairs have confirmed correlations predicted by quantum mechanics and then show Einstein locality are incompatible with quantum correlations as the proof given in Bell's theorem [12].

By the inspiration of Bell's theorem, the so-called *Bell inequalities* [5, 13–16] for two-level systems have been proposed to experimentally invalidate the point of view of EPR and to show that quantum mechanics is *not* locally realistic. Furthermore, while

entanglement for quantum two-level systems (qubits) is still under intensive study, entangled quantum multi-level systems (qudits) attract much attention for their nonlocal characters [17–21] and advantages in quantum information processing [22–24]. It has been shown that entangled qudit pair can maximally violate the Clauser-Horne-Shimony-Holt (CHSH) inequality [13] and the corresponding violation continues to survive in the limit of infinite dimension [25]. Using the method of linear programming to give necessary and sufficient conditions [26], numerical calculations have demonstrated that contradiction between local realism and quantum mechanics increases with the dimension. Latter, this contradiction has been confirm analytically in [17, 27]. Collins *et al.* [17] have reformulated Bell inequalities to construct a large family of multi-level inequalities in terms of a novel constraint for local-realistic theories called Collins-Gisin-Linden-Massar-Popescu (CGLMP) inequality. Recently, Son, Lee, and Kim (SLK) [18] presented generic Bell inequalities and their variants for arbitrary high-dimensional systems through the generalized Greenberger, Horne and Zeilinger (GHZ) nonlocality [28].

1.2 Entanglement and quantum information processing

For the aspect of quantum information processing, the nonlocal features of quantum correlations enable people to perform high-security and novel quantum communication [29, 30]. Moreover, it promotes a novel model of universal quantum computation [31–33]. Quantum communication could be consider as the first application of quantum mechanics, that is based on entanglement, no-cloning theorem, and quantum superposition. Quantum communication involves transmissions of quantum states form one place to another. In 1984, the first *quantum-cryptography protocol* has been proposed by Bennett and Brassard [34]. The essence of their scheme is the fact that unknown quantum states cannot be cloned. In 1991, the first application of quantum non-locality is introduced by Ekert [29]. In the protocol of Ekert, maximally entangled pairs are utilized for transmission of quantum

key and the corresponding security is guaranteed by the distinct features of entanglement cooperating with Bell's theorem. These novel encryption schemes provide a fundamental improvements compared to conventional ones. In 1993, *quantum teleportation* was exposed by Bennett *et al.* [30] in a momentous article entitled "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels" . With share maximally entangled pairs together with two classical bits of communication as specified in their protocol, unknown quantum states can be transferred from one place to another without any intermediate location. Quantum teleportation is also central to a number of quantum computation protocols [35, 36]. In addition to the above quantum protocols, *super dense coding* [37] and *quantum secret sharing* [38] are based on resources of entangled states for quantum information processing. The former illustrates that two bits of information can be transmitted from sender to receiver by sending only a single qubit. Quantum secret sharing does not only give a procedure required for the goal of secret sharing but also provides a way to detect the presence of an eavesdropper. Many-qubit entanglement are necessary for performing some specific types of protocol of quantum secret sharing.

Experimental demonstrations of single-qubit teleportation have been implemented with different physical systems [39–43] . Recently, teleportation of two-qubit composed systems has been experimentally realized with photonic qubits successfully [44]. As for quantum secret sharing, in Re. [45] four-party secret sharing with four-photon singlet states has been experimentally preformed. On the other hand, in order to achieve the aim of long-distance entanglement-based communication, up to now experiments have demonstrated over distances of up to 144 km using polarization-entangled photons via free-space links through the atmosphere. In Re. [46], the violation of CHSH-type [13] Bell inequality shows the distinct features of entanglement observed 144 km apart and then the Ekert protocol for quantum key distribution has been demonstrated successfully. However, to dissolve the problems about limitation communication distance further, quantum relays [47] and quantum memories [48, 49], i.e., quantum repeaters, are needed.

Entanglement is also a resource for universal quantum computing. *One-way quantum computation* [31–33] is performed with a certain multipartite entangled source, a *cluster state* [31], and local measurements on the constituents, and then it is also called *measurement-based quantum computation*. Before the model of one-way quantum computation is introduced, a quantum computer including the mathematical model and the corresponding experimental realizations is designed for logic circuit [50] of universal quantum gates [51] that require highly controlled interactions between selected qubits. It has been proven that one-way quantum computer can simulate any quantum logic circuit [32]. Three experiments have created four-photon cluster states and then demonstrated quantum one-way computation by performing *quantum search algorithm* [52–54]. Quantum mechanical algorithms involves utilization of quantum effects and have become very popular in the field of computation science because they can speed up a computation over classical algorithms. Famous examples include Deutsch-Josza algorithm [55], the factorizing algorithm discovered by Shor [56], and the quantum search algorithm well-developed by Grover [57, 58]. If there is an unsorted database containing N items, and out of which only one marked item satisfies a given condition, then using Grover’s algorithm one will find the object in $O(\sqrt{N})$ quantum mechanical steps instead of $O(N)$ classical steps. It has been shown that Grover’s original algorithm is optimal [59–61]. Through four-photon cluster states, Deutsch-Josza quantum algorithm [55], that is a quantum method to identify whether a given function is *constant* or *balanced*, has also been experimentally realized in the one-way approach [62]. Besides, the compiled version of Shor’s quantum factoring algorithm has been demonstrated by using photonic qubits [63].

In addition to qubits for quantum information protocols discussed above, qudits are very useful for several different kinds of quantum communication tasks. It has been shown that quantum key distribution with higher alphabets is more secure than that based on qubits [64–66]. The coin-flipping and the Byzantine agreement problems can be solved by making use of qutrits (quantum three-level systems) [67]. Entangled qutrits can be used to solve two-party communication complexity problem [68]. N -party N -level supersinglet

states can help to solve the problems which have no solution using classical method: N -strangers, secret sharing, and liar detection problems [69].

1.3 Entanglement detections, purifications, and quantum error corrections

Quantum communication protocols for tasks such as quantum key distributions [29], quantum teleportation [30], and quantum super dense coding [37] rely on the transmission of maximally entangled qubit pairs over quantum channels between a sender (Alice) and a receiver (Bob). The quantum channel, however, is always noisy due to the interaction with the environment and even possibly the measurement controlled by an eavesdropper. Therefore, the pairs shared by Alice and Bob are no longer of the desired pure ones to begin with a quantum processing. The resource in the noisy channel then can be viewed as a mixed state, or equivalently, an ensemble of pure states with definite random probabilities. The fidelity of the pure states in the ensemble are random so should be unknown to Alice and Bob. Accordingly, first, Alice and Bob need to find efficient experimental methods to detect whether a experimental output is indeed entangled. Then, they could take an action of entanglement purification to regain, at least asymptotically, the desired maximally entangled pure state if the mixed state is distillable. This aim can be achieved by Alice and Bob, using consecutive local operations and classical communications (LOCC). Above processes are also necessary for many-party protocols of quantum communication, e.g., experimental achievement of open-destination teleportation [43]. In addition to the importance of entanglement detections for quantum communication, detecting genuine many-qubit correlations of multipartite entanglement is also crucial for performing faithful measurement-based quantum computation [31–33].

Since Bell inequalities can be consider as a means to feature quantum correlations in the corresponding violations, it is natural to think that Bell inequalities are useful for entanglement detections. However, there are two difficulties in utilizing Bell inequalities

for entanglement detections. One involves experimental difficulty and another is about limits of their intrinsic utilities. First, for detecting N -qubit entangled states, the number of local measurement settings (see the definition in the second chapter) required increases with exponentially with N [14–16]. Second, Bell inequalities cannot always detect an entangled state with some specific characters of quantum correlation, e.g., detections of genuine multipartite entanglement [70]. To resolve these problems, *entanglement witnesses* are introduced to detect entanglement [71]. Entanglement witness operators rely on an use of the whole or partial knowledge of an entangled state to be created, which are designed for distinguishing entangled states from separable ones. Furthermore, entanglement witnesses can be designed for detecting genuine multipartite entanglement [70], and some witnesses for truly multipartite entanglement require fewer local measurement settings [72, 73] when used in experiments.

The first entanglement purification protocol (the IBM protocol) was developed by Bennett *et al.* [74, 75] in achieving a faithful quantum teleportation. Soon later, an improved protocol entitled “Quantum Privacy Amplification” (QPA, or the Oxford protocol) was addressed by Deutsch *et al.* [76] in consideration of the security of a quantum cryptography over noisy channels. Both the IBM and Oxford protocols are capable of purifying a desired maximally entangled pure state from every distillable mixed state whose components are not learned by Alice and Bob initially.

It is worth noting that Bennett *et al.* [74] have presented the equivalence between the entanglement purification protocol based on one-way classical communication, that is different from the IBM protocol with two-way classical communication, and the five-qubit *quantum error-correcting code* [77, 78]. Quantum states can be encoded into qubits through quantum error-correcting codes [79, 80]. With an introduction of redundancy, the encoded data can tolerate little errors which are due to decoherence in some individual qubits. Then, quantum error-correcting codes play a crucial role in scalable quantum computation and communication to preserve the gain in computational time and in security.

The experimental purification of entangled qubits of IBM protocol has been demonstrated by using entangled-photon source [81]. In addition to the IBM and Oxford protocols, further extensions cover purifications of many-qubit W [82] and graph states [83] and multi-level GHZ states [84].

1.4 Experimental generations of quantum entanglement

For the aspect of generating entanglement in real physical systems, many different architectures and schemes have been proposed. An entanglement can be generated in atom- [85–87] and ion-trap systems [88], superconducting charge [89, 90] and flux [91] qubit systems. However, in order to perform quantum information processing, in addition to entanglement generations there are several criteria for measuring how good physical systems are. To realize quantum computation, the requirements of the physical systems involve scalability, isolation, initialization, measurement, and controllably interactions for universal quantum gates [92]. To achieve quantum communication, the physical systems carrying information are expected to transmit between remote places [93, 94]. According to these reasons, optical quantum systems [36, 93–96] are important candidates for quantum information processing and then become leading approaches over the past few years. Many experimental achievements of tasks of quantum information processing are attained with optical quantum systems.

Polarization-entangled photons emitted by the process of spontaneous parametric down-conversion (SPDC) [97, 98] in a nonlinear crystal has been widely utilized to analyze quantum correlation and to experimentally demonstrate quantum computation and quantum communication, e.g., the experimental realizations of the quantum protocol mentioned above [39–41, 43–46, 52–54, 62, 63, 81], entanglement of six photons in graph states [99], and test of non-local realism [100]. These experiments are designed to process information encoded in qubits.

Recently, due to the advantages and distinct characteristics of qudits as mentioned above, many researches have paid attention to generations of hyperentanglement. Orbital angular momentum entangled photons generated from the SPDC process have been experimentally realized and provide a resource to study quantum correlation inherent in multilevel systems [20]. Using this kind of entangled source, violation of three-level Bell inequalities has been experimentally confirmed and quantum key distribution with qutrits has also been demonstrated [23]. In addition to the polarization and orbital angular momentum of photons, utilizing accessible degrees of freedom including path modes [54, 101, 102], energy time, time bin [103–105], and every degree of freedom [106], one can produce hyperentangled photon sources. Since a hyperentangled state is in a larger Hilbert space, this feature can be used to perform 100% efficient complete Bell-state analysis with only linear elements [107], to purify entanglement [101], and to realize all versus nothing test of quantum mechanics [102]. An experimental CGLMP test for energy-time entangled qutrits has been reported in Re. [105]. The experimental scheme for deterministic and efficient quantum communication based on hyperentanglement has also been proposed [108]. In particular, experimental realization of one-way quantum computing with two-photon four-qubit hyperentangled states has been reported in Re. [54].

1.5 Outline of the Thesis

We have proposed several novel ideas and proposals for quantum information processing and experimentally demonstrated one important element of quantum computation during the time of my Ph. D. studies. Our research mainly concentrates on entanglement detection, on entanglement generation, on entanglement purification, on quantum error corrections, on quantum search algorithm, and on the experimental creation of four-qubit hyperentangled states and realization of one-way quantum computation. We investigate into several key subjects involved in almost the whole process of quantum information processing. We start with a study into the properties of correlations inherent in multipartite

entangled states and then provide a new insight into entanglement detections including Bell inequalities, entanglement witness operators, and the connections between them. We improve the purification protocols of entanglement and then design a new efficient one. Furthermore, we give an analytic and systematic way to construct quantum circuits for both entanglement purification and quantum error corrections. For entanglement generation, we propose a scheme for generating a many-qubit entangled state with translational symmetry. We also analyze the quantum search algorithm in detail and experimentally perform a quantum search by one-way realization successfully. A summary is given as follows.

Chapter 2 Quantum correlations imbedded in many-qubit and two-qudit entangled states are described by novel criteria of correlation for dependent systems. Correlation structures of Bell inequalities and entanglement witness operators are in terms of correlation criteria proposed. Several robust and efficient Bell inequalities and entanglement witnesses are also introduced.

Chapter 3 We apply the correlation criteria to the stabilizer formalism and discuss the entanglement of stabilizer states in a new point of view. Entanglement witnesses for stabilizer-entangled states that required only two local measurement settings when used in experiments are given.

Chapter 4 Entanglement witnesses for detecting several different kinds of many-qubit entangled states that are useful for quantum information processing are proposed.

Chapter 5 General correlation criteria for many-qudit entanglement are introduced. We reveal the essential elements of the GHZ paradoxes and the generic Bell inequalities for many qudits are comprised of the criteria introduced. Several witnesses for multipartite entangled qudits are proposed.

Chapter 6 Standard entanglement purification protocols based on hybrid maps are proposed to purify any distillable state to a desired maximally entangled pure state.

Chapter 7 An analytical method to simplify the encoder-decoder circuit for a perfect five-qubit quantum error correcting code that is converted from its equivalent one-way entanglement purification protocol is introduced.

Chapter 8 We study how dot-like single quantum well excitons, which are coupled to single-mode cavity photon, evolve into maximally entangled state as a series of conditional measurements are taken on the cavity field state.

Chapter 9 Detailed analyses of the constructions of quantum search algorithm are presented in this chapter. We focus on the accuracy and noise tolerance of the quantum algorithm.

Chapter 10 We experimentally develop a two-photon cluster state source entangled both in polarization and spatial modes. We also utilize the created hyperentangled qubit source to give a experimental demonstration of one-way quantum computation. A quantum search task is performed in an one-way realization.

Chapter 11 We summarize the main results in the thesis and give an outlook.

Chapter 2

Entanglement and correlation conditions

2.1 Introduction



Bell inequalities are results about local realism, and then violations of which by entangled states can be considered as a means to feature the distinct properties of quantum correlations. In this situation, three main questions arise: (i) Is there a necessary condition of quantum correlation associated with some entangled state in the kernels of Bell inequalities? While Bell inequalities are based on the local realistic theories, we wonder whether their kernels can provide conditions of correlation for entangled states. (ii) What is the connection between the correlation structures of Bell inequalities for qubits and the ones for qudits? Can it be utilized to analyze the correlation properties of both entangled qudits and many-qubit entanglement? (iii) What is the connection between the correlation structures of Bell inequalities and entanglement witnesses? Can the kernels of Bell inequalities be used to construct entanglement witnesses for qudits?

The goal of this chapter is threefold. First, we introduce necessary conditions of correlation for many-qubit and two-qudit entanglement. Second, we reveal that the Bell inequalities for many qubits introduced by Clauser-Horne-Shimony-Holt (CHSH) [13],

Mermin [14], and Seevinck-Svetlichny [15], and the Collins-Gisin-Linden-Massar-Popescu (CGLMP) [17] and Son-Lee-Kim (SLK) [18] inequalities for bipartite arbitrarily high-dimensional systems are composed of the correlation conditions proposed. The general correlation functions of the CHSH inequality proposed by Fu [109] are also shown to consist of conditions of correlation. Bell inequalities based on correlation criteria for qudits are introduced. In addition, we show that the Durkin-Simon inequalities [110] for many-qubit entanglement can be rephrased in terms of correlation criteria. Third, we use the criteria to construct the first entanglement witness operator for detecting a two-qudit Bell state. In particular, this witness needs only two local measurement settings (see below) when used in experiments and is very robust against noise, independent of the number of levels. Further, two novel and robust witnesses for qudits are proposed. The conditions of correlations for Bell inequalities are also utilized to construct witness operators for qudits. In short, the condition presented is common among Bell inequalities for qudits and many qubits. The constructions introduced show connections between Bell inequalities and entanglement witnesses.

This chapter is organized as follows. We start in Sec. 2.2 by revisiting the scenario of a many-party Bell-type experiment for identifying the correlations between outcomes of measurements. Then we present the basic idea of the condition of correlation and introduce the dependence criterion for many-qubit and two-qudit correlations. Since many-qubit GHZ and two-qudit Bell states are very useful for quantum information processing and under intensive study in entanglement physics, in Sec. 2.3 we proposed different kinds of correlation conditions to analyze their correlation characters. In Sec. 2.4, we show the criteria of correlations introduced in Sec. 2.3 are the kernels of the Bell inequalities that have been presented. We also introduce Bell inequalities based on the conditions of quantum correlations for qudits. In Sec. 2.5 we give a novel entanglement witness operator for detecting states close to a two-qudit Bell state. We also consider entanglement detections of two given multilevel entangled states. In addition, we give witness operators for N -qubit GHZ states and analyze the structure of the inequalities based on the geometry of

spin vectors by the conditions proposed. Then a conclusion follows. Finally, in Appendix A we give a proof to show the tightness of the Bell inequalities for qudits proposed in Sec. 2.4.

2.2 Correlation condition and entanglement detection

In a N -party Bell-type experiment, measurements on each spatially-separated particle are assumed to be performed with two distinct results (d distinct results for d -level Bell-type experiments) from two different observables. In each run of the experiment, each party chooses one observable for a simultaneous measurement on the particle in parallel. Let us denote the local measurement setting by $M = (V_1, V_2, \dots, V_N)$, where V_i represents the observable chosen by the i th party. After measurements, a set of results, (v_1, v_2, \dots, v_N) , where $v_i \in \{0, 1\}$ ($v_i \in \{0, 1, \dots, d-1\}$ for d -level Bell-type experiments), is acquired. If sufficient runs of such measurements have been made under the chosen local measurement setting, the correlation between experimental outcomes can be revealed through analytical analyses of experimental records. In analogy, experiments for bipartite multilevel systems work in the same way as mentioned above.

For quantum mechanical representation, we introduce an operator of the form

$$\hat{V}_i = \sum_{v_i=0}^{d-1} (-1)^{v_i} \hat{v}_i, \quad (2.1)$$

where $\hat{v}_i = |v_i\rangle_{V_i} \langle v_i|$ and $\{|v_i\rangle_{V_i}\}$ is a complete set of orthonormal basis vectors for the observable \hat{V}_i . Each N -product operator of the form $\hat{V}^\pm = \pm \bigotimes_{i=1}^N \hat{V}_i$ can be represented explicitly by

$$\hat{V}^\pm = \hat{C}_0^\pm + \hat{C}_1^\pm, \quad (2.2)$$

where

$$\hat{C}_0^+ = (\hat{\mathbf{0}}_m - \hat{\mathbf{1}}_m) \otimes \hat{\mathbf{0}}_{\bar{m}}, \hat{C}_1^+ = (\hat{\mathbf{1}}_m - \hat{\mathbf{0}}_m) \otimes \hat{\mathbf{1}}_{\bar{m}}, \quad (2.3)$$

$$\hat{C}_0^- = (\hat{\mathbf{0}}_m - \hat{\mathbf{1}}_m) \otimes \hat{\mathbf{1}}_{\bar{m}}, \hat{C}_1^- = (\hat{\mathbf{1}}_m - \hat{\mathbf{0}}_m) \otimes \hat{\mathbf{0}}_{\bar{m}}, \quad (2.4)$$

and

$$\begin{aligned} \hat{\mathbf{0}}_m &= \sum_{v_1, \dots, v_m} \bigotimes_{i=1}^m \hat{v}_i \text{ for } \sum_{i=1}^m v_i \doteq 0, \\ \hat{\mathbf{1}}_m &= \sum_{v_1, \dots, v_m} \bigotimes_{i=1}^m \hat{v}_i \text{ for } \sum_{i=1}^m v_i \doteq 1, \\ \hat{\mathbf{0}}_{\bar{m}} &= \sum_{v_{m+1}, \dots, v_N} \bigotimes_{i=m+1}^N \hat{v}_i \text{ for } \sum_{i=m+1}^N v_i \doteq 0, \\ \hat{\mathbf{1}}_{\bar{m}} &= \sum_{v_{m+1}, \dots, v_N} \bigotimes_{i=m+1}^N \hat{v}_i \text{ for } \sum_{i=m+1}^N v_i \doteq 1, \end{aligned} \quad (2.5)$$

and \doteq denotes equality modulus two. Expectation values of \hat{V}^\pm for some physical states, denoted by $\langle \hat{V}^\pm \rangle$, are typically called N -point correlation functions. Here we will give a new insight into $\langle \hat{V}^\pm \rangle$ via their elements \hat{C}_0^\pm and \hat{C}_1^\pm . Determining the expectation values of \hat{C}_0^\pm and \hat{C}_1^\pm can provide information about correlation between the subsystems composed of the first m qubits and the rest of the system.

Theorem 1. If measured outcomes show that expectation values of operators satisfy $\langle \hat{C}_0^\pm \rangle > 0$ and $\langle \hat{C}_1^\pm \rangle > 0$, or, $\langle \hat{C}_0^\pm \rangle < 0$ and $\langle \hat{C}_1^\pm \rangle < 0$, the outcomes of measurements performed on the subsystem of the first m qubits are correlated with the ones performed on the subsystem of the last $N - m$ qubits [111].

Proof. If the subsystems are *independent*, we have the following relations

$$\langle \hat{C}_0^+ \rangle = (\langle \hat{\mathbf{0}}_m \rangle - \langle \hat{\mathbf{1}}_m \rangle) \langle \hat{\mathbf{0}}_{\bar{m}} \rangle, \langle \hat{C}_1^+ \rangle = (\langle \hat{\mathbf{1}}_m \rangle - \langle \hat{\mathbf{0}}_m \rangle) \langle \hat{\mathbf{1}}_{\bar{m}} \rangle, \quad (2.6)$$

and

$$\langle \hat{C}_0^- \rangle = (\langle \hat{\mathbf{0}}_m \rangle - \langle \hat{\mathbf{1}}_m \rangle) \langle \hat{\mathbf{1}}_{\bar{m}} \rangle, \langle \hat{C}_1^- \rangle = (\langle \hat{\mathbf{1}}_m \rangle - \langle \hat{\mathbf{0}}_m \rangle) \langle \hat{\mathbf{0}}_{\bar{m}} \rangle. \quad (2.7)$$

Since $\langle \hat{\mathbf{0}}_m \rangle + \langle \hat{\mathbf{1}}_m \rangle = 1$, $\langle \hat{\mathbf{0}}_{\bar{m}} \rangle \geq 0$, and $\langle \hat{\mathbf{1}}_{\bar{m}} \rangle \geq 0$ for any physical systems, it turns out that $\langle \hat{C}_0^+ \rangle \langle \hat{C}_1^+ \rangle \leq 0$ and $\langle \hat{C}_0^- \rangle \langle \hat{C}_1^- \rangle \leq 0$. Thus a contradiction reveals the dependency of one subsystem on another one. \square

Then $\langle \hat{V}^\pm \rangle$ is not just a N -point correlation function but a general one composed of $\langle \hat{C}_{0,1}^\pm \rangle$ that gives n_c conditions of dependence for correlations between any two subsystems with m qubits and $N - m$ ones, where

$$n_c = \sum_{k=1}^{\lfloor N/2 \rfloor} f(N, k) \frac{N!}{k!(N-k)!}, \quad (2.8)$$

$f(N, k) = 2^{-\delta[k, \lfloor N/2 \rfloor]}$ for even N , $\delta[\cdot]$ denotes Kronecker delta symbol, and $f(N, k) = 1$ for odd one. Take $N = 3$ for example. A correlation function $\langle \hat{V}_1 \hat{V}_2 \hat{V}_3 \rangle$ involves three conditions, i.e., $n_c = 3$, to describe correlations between subsystems including the following classifications, $\{[1, 2, 3]\}$: $[1|2, 3]$, $[2|1, 3]$, and $[3|1, 2]$, where $[i|j, k]$ denotes the correlation between the i th qubit and the subsystem composed of the j th and k th ones. For N qubits, we use the denotation $\{[1, 2, \dots, N]\}$ or $\{[\mathbf{m}, \bar{\mathbf{m}}]\}$ to represent n_c different kinds of partitions for correlation, and we sometimes use the notations $\hat{C}_{0[\mathbf{m}, \bar{\mathbf{m}}]}^\pm$ and $\hat{C}_{1[\mathbf{m}, \bar{\mathbf{m}}]}^\pm$ emphasizing the correlations between two specific subsystems denoted by \mathbf{m} and $\bar{\mathbf{m}}$ respectively.

By the same idea of constructing $\hat{C}_{0,1}^\pm$ for qubits, we introduce the following sets of operators for two-qudit correlations:

$$\hat{C}_k^{(q)} = [\hat{k} - T(\hat{k})] \otimes U(\hat{k}), \quad (2.9)$$

for $k = 0, 1, \dots, d - 1$ and $q = 1, \dots, \gamma_d$, where T and U are injective maps such that $T(\hat{k}) \mapsto \hat{k}'$, $U(\hat{k}) \mapsto \hat{k}''$, and $k' \neq k$, and each set $\{T(\hat{k})\}$ composed of $T(\hat{k})$'s is numbered by q . Take $d = 3$ for example, we have two sets of $\{T(\hat{k})\}$ and hence the sets of operators

$\{\hat{C}_k^{(q)}\}$ could be

$$\begin{aligned} \{\hat{C}_0^{(1)} = (\hat{0} - \hat{1})\hat{0}, \hat{C}_1^{(1)} = (\hat{1} - \hat{2})\hat{1}, \hat{C}_2^{(1)} = (\hat{2} - \hat{0})\hat{2}\}, \\ \{\hat{C}_0^{(2)} = (\hat{0} - \hat{2})\hat{0}, \hat{C}_1^{(2)} = (\hat{1} - \hat{0})\hat{1}, \hat{C}_2^{(2)} = (\hat{2} - \hat{1})\hat{2}\}. \end{aligned}$$

where $U(\hat{k}) = \hat{k}$ is used in this example. For $d = 2$, we get the sets of operators for qubits introduced above: $\hat{C}_0^{(1)} = \hat{C}_0^+$ and $\hat{C}_1^{(1)} = \hat{C}_1^+$ for $U(\hat{k}) = \hat{k}$, or $\hat{C}_0^{(1)} = \hat{C}_0^-$ and $\hat{C}_1^{(1)} = \hat{C}_1^-$ for $U(\hat{k}) = \hat{k}''$ and $k'' \neq k$. Then it is clear that the number of sets $\{\hat{C}_k^{(q)}\}$ depends on the number of $\{T(\hat{k})\}$. For general d , we have γ_d sets of $\{\hat{C}_k^{(q)}\}$, where $\gamma_2 = 1$, $\gamma_3 = 2$, $\gamma_4 = 9$, $\gamma_5 = 44$, $\gamma_6 = 285$, and

$$\gamma_d = (d-2) \prod_{v=3}^{d-1} v + (d-1)\gamma_{d-2}, \quad (2.10)$$

for $d \geq 7$. The correlation between outcomes of measurements performed on two remote qudits can be revealed by the help of the following theorem.

Theorem 2. If measured outcomes show each expectation value $\langle \hat{C}_k^{(q)} \rangle$ in the q th set $\{\langle \hat{C}_k^{(q)} \rangle\}$ is positive or each one is negative, the outcomes of measurements performed on the first qudit are correlated with the ones performed on the second qudit [112].

Proof. If the subsystems are independent, one can recast $\langle \hat{C}_k^{(q)} \rangle$ as

$$\langle \hat{C}_k^{(q)} \rangle = (\langle \hat{k} \rangle - \langle T(\hat{k}) \rangle) \langle U(\hat{k}) \rangle, \quad (2.11)$$

Since $\sum_k \langle \hat{k} \rangle = \sum_k \langle T(\hat{k}) \rangle = 1$ and $\langle U(\hat{k}) \rangle \geq 0$, $\langle \hat{C}_k^{(q)} \rangle > 0$ for all k 's is impossible for independent subsystems. Then a contradiction indicates the dependency of the first qudit on the second one. \square

With the above two theorems, one can feature a many-qubit or two-qudit entangled state in sets of correlation conditions proposed under different local measurement settings. These conditions can be considered as necessary ones for the entangled state under

study. We call the expectation values $\langle \hat{C}_k^{(q)} \rangle$ and $\langle \hat{C}_{0,1}^\pm \rangle$ *correlators* due to their utilities for correlations. We give three concrete examples to illustrate how correlators work for analyzations of the correlation structures of given states and the basic idea of entanglement detections based on correlators:

(a) A two-qubit pure entangled state in the following representation:

$$|\phi\rangle = \sin(\xi) |00\rangle + \cos(\xi) |11\rangle, \quad (2.12)$$

for $0 < \xi < \pi/4$, where $|v_1 v_2\rangle = |v_1\rangle \otimes |v_2\rangle$ and $|v_i\rangle$ is the eigenstate of Pauli-operator σ_z with eigenvalue $(-1)^{v_i}$, can be described by correlators that correspond to the operators $\hat{C}_{0Z} = \hat{C}_0^+ = (\hat{0} - \hat{1})\hat{0}$ and $\hat{C}_{1Z} = \hat{C}_1^+ = (\hat{1} - \hat{0})\hat{1}$. By a direct calculation, one obtains the correlators $\langle \hat{C}_{0Z} \rangle = \sin^2(\xi)$ and $\langle \hat{C}_{1Z} \rangle = \cos^2(\xi)$ for the state $|\phi\rangle$, which reveals the correlation properties when observed in the local measurement setting $M_z = (Z, Z)$ where $Z = \sigma_z$. The state $|\phi\rangle$ can also be shown in another representation, e.g.,

$$|\phi\rangle = a(|00\rangle_X + |11\rangle_X) + b(|01\rangle_X + |10\rangle_X), \quad (2.13)$$

where $a = [\cos(\theta) + \sin(\theta)]/2$, $b = [\cos(\theta) - \sin(\theta)]/2$, and $|v_i\rangle_X$ is an eigenstate of Pauli-operator σ_x with an eigenvalue $(-1)^{v_i}$. This representation provides the information of probability distribution for $\{|v_1 v_2\rangle_X\}$ when measured in the setting $M_x = (X, X)$ where $X = \sigma_x$. From which, one can construct correlators, and the characters of correlation can be described by $\langle \hat{C}_{0X} \rangle = \langle \hat{C}_{1X} \rangle = \sin(2\xi)/2$ where $\hat{C}_{0X} = \hat{C}_0^+ = (\hat{0} - \hat{1})\hat{0}$ and $\hat{C}_{1X} = \hat{C}_1^+ = (\hat{1} - \hat{0})\hat{1}$.

(b) The probability distribution for $|\phi\rangle$ when measured with the setting M_z is the same as the one of the following mixture of product states:

$$\rho_\phi = \sin^2(\xi) |00\rangle \langle 00| + \cos^2(\xi) |11\rangle \langle 11|. \quad (2.14)$$

Then we have the correlators $\langle \hat{C}_{0Z} \rangle_{\rho_\phi} = \sin^2(\xi)$ and $\langle \hat{C}_{1Z} \rangle_{\rho_\phi} = \cos^2(\xi)$ and know outcomes

of measurements for these particles are dependent. When the state ρ_ϕ is represented in the basis $\{|v_1 v_2\rangle_X\}$, the probability for observing an element in $\{|v_1 v_2\rangle_{XX}\}$ of ρ_ϕ is $1/4$, which implies that these two particles are independent. This fact can be shown by the correlators $\langle \hat{C}_{0X} \rangle = \langle \hat{C}_{1X} \rangle = 0$.

From the above examples, one has $\sum_{l=X,Z} \sum_{k=0}^1 \langle \hat{C}_{kl} \rangle > \sum_{l=X,Z} \sum_{k=0}^1 \langle \hat{C}_{kl} \rangle_{\rho_\phi}$. From which, it is worth noting that determining a sum of correlators associated with two different local measurement settings can help us to distinguish the entangled state $|\phi\rangle$ from the separable state ρ_ϕ . This idea and approach can be applied to detections of truly many-qubit entanglement and bipartite entangled qudits. For any many-qubit system composed of two independent parts, outcomes of measurements should satisfy

$$\left| \sum_k \langle \hat{C}_{k[\mathbf{m}, \bar{\mathbf{m}}]}^\pm \rangle \right| = |(\langle \hat{\mathbf{0}}_m \rangle - \langle \hat{\mathbf{1}}_m \rangle)(\langle \hat{\mathbf{0}}_{\bar{m}} \rangle - \langle \hat{\mathbf{1}}_{\bar{m}} \rangle)| \leq 1 \quad (2.15)$$

for any measurement settings chosen. Whereas, for some specific entangled states, one can feature properties of entanglement to be created in $|\sum_k \langle \hat{C}_{k[\mathbf{m}, \bar{\mathbf{m}}]}^\pm \rangle| = 1$ for several local measurement settings chosen and consider which as necessary conditions for the entangled state. Furthermore, we could give all conditions of correlations $[\mathbf{m}, \bar{\mathbf{m}}]$ associated with any two subsystems of the many-qubit entangled state under study. Thus we can use these conditions of genuine many-qubit entanglement to rule out biseparable correlations. For two independent qudits observed under any measurement settings, a sum of correlators should follow the criteria

$$\left| \sum_k \langle \hat{C}_k^{(q)} \rangle \right| \leq \sum_k |(\langle \hat{k} \rangle - \langle T(\hat{k}) \rangle)|^2 \sum_{k'} |(\langle U(\hat{k}') \rangle)|^2 \leq 1. \quad (2.16)$$

Then entanglement conditions $|\sum_k \langle \hat{C}_k^{(q)} \rangle| = 1$ for all local measurement settings considered can be very useful to detect entangled qudit pairs. Using the idea introduced above can promote constructions of many-qubit and two-qudit entanglement witness operators that require only two local measurement settings. Even though the conditions

$|\sum_k \langle \hat{C}_{k[\mathbf{m}, \bar{\mathbf{m}}]}^\pm \rangle| = 1$ and $|\sum_k \langle \hat{C}_k^{(q)} \rangle| = 1$ cannot be satisfied by all entangled states considered, the above approach still can be applied to entanglement detections if more local measurement settings are used. See the case discussed in the second subsection of Sec. 2.5.

(c) The state vector of a two-qubit singlet state is represented by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (2.17)$$

If $\hat{V}_1 \in \{\hat{V}_1^{(1)} = Z, \hat{V}_1^{(2)} = X\}$ and $\hat{V}_2 \in \{\hat{V}_2^{(1)} = -(Z + X)/\sqrt{2}, \hat{V}_2^{(2)} = (Z - X)/\sqrt{2}\}$, we have four different local measurement settings $M = (\hat{V}_1, \hat{V}_2)$ to give four sets of correlators. The operators of correlators are as follows: $\hat{C}_0^{(rt)} = \hat{C}_0^+ = (\hat{0} - \hat{1})\hat{0}$, $\hat{C}_1^{(rt)} = \hat{C}_1^+ = (\hat{1} - \hat{0})\hat{1}$ for $(rt) \in \{(11), (21), (22)\}$ and $\hat{C}_0^{(12)} = \hat{C}_0^- = (\hat{0} - \hat{1})\hat{1}$, $\hat{C}_1^{(12)} = \hat{C}_1^- = (\hat{1} - \hat{0})\hat{0}$, where the superscripts (rt) mean an observable $\hat{V}_1^{(r)}$ and another one $\hat{V}_2^{(t)}$ are chosen for measurements. The correlators can be easily calculated, and then we have $\langle \hat{C}_0^{(rt)} \rangle = \langle \hat{C}_1^{(rt)} \rangle = 1/2\sqrt{2}$. When collecting all of the correlator operators proposed above, one gets

$$\begin{aligned}
 B &= \sum_{r,t=1}^2 \sum_{k=0}^1 \hat{C}_k^{(rt)} \\
 &= \hat{V}_1^{(1)}\hat{V}_2^{(1)} + \hat{V}_2^{(2)}\hat{V}_2^{(2)} + \hat{V}_1^{(2)}\hat{V}_2^{(1)} - \hat{V}_1^{(1)}\hat{V}_2^{(2)}.
 \end{aligned} \quad (2.18)$$

Local-realistic theories predict that $B \leq 2$, which is called the CHSH inequality [13], whereas the entangled state $|\psi\rangle$ predicted by quantum mechanics provides a violation by $\sum_{rt} \langle \hat{C}^{(rt)} \rangle = 2\sqrt{2}$. It is remarkable that the kernel of the CHSH inequality [13] is composed of necessary conditions of the state $|\psi\rangle$ in terms of the correlators $(\langle \hat{C}_0^{(rt)} \rangle, \langle \hat{C}_1^{(rt)} \rangle)$.

In what follows, we will use correlators to analyze the most studied many-qubit and two-qudit entangled states: the N -qubit GHZ state [113] and the two-qudit Bell state. The correlators proposed are necessary for states to be the entanglement under study and play important roles in identifying quantum correlations including ruling out biseparable correlations and ones predicted by local-realistic theories.

2.3 Quantum correlations imbedded in entangled states

2.3.1 Correlation structures of many-qubit GHZ states

The three-qubit GHZ state is first discussed in the GHZ argument [113] which provides important insights into tripartite entanglement. Entanglement embedded in a three-qubit GHZ state has been shown very useful to investigate both noncontextual variables and Bell-EPR theorems [114]. In addition to the three-qubit GHZ state, the generalized N -qubit GHZ states have attracted much attentions. Many Bell inequalities for many qubits [14–16] have been shown to be violated by N -qubit GHZ states. Furthermore, six-atom [85] and six-photon [99] GHZ states have been demonstrated experimentally.

In this subsection, we utilize three different types of correlators to specify the features of N -qubit correlation of a N -qubit GHZ state which is of the state vector:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \quad (2.19)$$

The classification of correlator depends on which kind a local measurement setting is chosen and how many settings are used in Bell-type experiments. These correlators will be utilized to subsequent investigations on entanglement detections.

Specification 1. Firstly, we introduce alternative dichotomous observable for qubits by

$$\hat{V}_k \in \{X, Y\}, \hat{V}_N \in \left\{ \frac{Y+X}{\sqrt{2}}, \frac{Y-X}{\sqrt{2}} \right\}, \quad (2.20)$$

for $k = 1, 2, \dots, N-1$, where Y denotes the Pauli-operator σ_y . Since each party has two choices to perform measurements, there are 2^N possible sets of local measurement settings.

Then we give the following operators of correlators

$$\hat{C}_{0l} = \gamma_l \hat{C}_0^+, \hat{C}_{1l} = \gamma_l \hat{C}_1^+, \quad (2.21)$$

for $l = 1, 2, \dots, 2^N$, where l is used to number 2^N different measurement settings and γ_l

are constants.

By a direct calculation, we have the correlators

$$\langle \hat{C}_{0l} \rangle = \langle \hat{C}_{1l} \rangle = \frac{\gamma_l (-1)^{n_2(n_2+1)/2}}{2\sqrt{2}}, \quad (2.22)$$

where n_2 denotes the number of $\hat{V}_k = Y$ and $\hat{V}_N = (Y - X)/\sqrt{2}$ chosen in a setting numbered l . If we assign $\gamma_l = (-1)^{n_2(n_2+1)/2}$, then each correlator has the same sign and becomes $\langle \hat{C}_{0l} \rangle = \langle \hat{C}_{1l} \rangle = 1/2\sqrt{2}$.

Specification 2. The observable of each particle designed for measurement is given by

$$\hat{V}_k \in \{X, Y\}, \quad (2.23)$$

for $k = 1, 2, \dots, N$. Although there are 2^N possible settings of local measurements, we focus only on settings in which there are even number of Y 's chosen for measurements. For odd N and $2n$ Y 's where n is odd, we introduce correlator operators of the form

$$\hat{C}_{0l} = \hat{C}_0^-, \hat{C}_{1l} = \hat{C}_1^-, \quad (2.24)$$

for $l = 1, 2, \dots, 2^{N-1} - 1$. For even N and $2n$ Y 's where n is even, the operators of correlators are given by

$$\hat{C}_{0l} = \hat{C}_0^+, \hat{C}_{1l} = \hat{C}_1^+, \quad (2.25)$$

for $l = 1, 2, \dots, 2^{N-1}$. For a N -qubit GHZ state, the correlators proposed are all the same:

$$\langle \hat{C}_{0l} \rangle = \langle \hat{C}_{1l} \rangle = \frac{1}{2}. \quad (2.26)$$

Specification 3. In this specification, we use only two local measurement settings to

feature correlation structure in correlators:

$$M_z = \{Z, Z, \dots, Z\}, M_x = \{X, X, \dots, X\}. \quad (2.27)$$

When a N -qubit GHZ state is measured under the setting M_z , correlations between some subsystem composed of m qubits and the rest can be described by correlators corresponding to the operators:

$$\hat{C}_{0Z[\mathbf{m}, \bar{\mathbf{m}}]} = (\mathbf{0}_{\mathbf{m}Z} - \mathbf{1}_{\mathbf{m}Z})\mathbf{0}_{\bar{\mathbf{m}}Z}, \hat{C}_{1Z[\mathbf{m}, \bar{\mathbf{m}}]} = (\mathbf{1}_{\mathbf{m}Z} - \mathbf{0}_{\mathbf{m}Z})\mathbf{1}_{\bar{\mathbf{m}}Z}, \quad (2.28)$$

where $\mathbf{0}_{\mathbf{m}(\bar{\mathbf{m}})Z} = \bigotimes_{i \in \mathbf{m}(\bar{\mathbf{m}})} \hat{v}_i$ for all $v_i = 0$, $\mathbf{1}_{\mathbf{m}(\bar{\mathbf{m}})Z} = \bigotimes_{i \in \mathbf{m}(\bar{\mathbf{m}})} \hat{v}_i$ for all $v_i = 1$, and \mathbf{m} and $\bar{\mathbf{m}}$ denote the subsystems comprised of m and $N - m$ qubits respectively. For instance, to detect three-qubit GHZ state the correlator operators have the explicit representations:

$$\hat{C}_{0Z[i,pq]} = (\hat{0}_i - \hat{1}_i)\hat{0}_p\hat{0}_q, \hat{C}_{1Z[i,pq]} = (\hat{1}_i - \hat{0}_i)\hat{1}_p\hat{1}_q,$$

where the set of subscripts (ipq) is used to number qubits. For each set of correlator, we have

$$\langle \hat{C}_{0Z[\mathbf{m}, \bar{\mathbf{m}}]} \rangle = \langle \hat{C}_{1Z[\mathbf{m}, \bar{\mathbf{m}}]} \rangle = \frac{1}{2}. \quad (2.29)$$

For the sets of correlators constructed under the setting M_x , their constructions are similar to the ones of $(\hat{C}_{0Z[\mathbf{m}, \bar{\mathbf{m}}]}, \hat{C}_{1Z[\mathbf{m}, \bar{\mathbf{m}}]})$ and represented by

$$\hat{C}_{0X[\mathbf{m}, \bar{\mathbf{m}}]} = \hat{C}_{0[\mathbf{m}, \bar{\mathbf{m}}]}^+, \hat{C}_{1X[\mathbf{m}, \bar{\mathbf{m}}]} = \hat{C}_{1[\mathbf{m}, \bar{\mathbf{m}}]}^+. \quad (2.30)$$

where the operators $\hat{C}_{0[\mathbf{m}, \bar{\mathbf{m}}]}^+$ and $\hat{C}_{1[\mathbf{m}, \bar{\mathbf{m}}]}^+$ are of the forms as Eq. (2.3). Take three-qubit operators of correlators for example, they are of the forms:

$$\hat{C}_{0X[i,pq]} = (\hat{0}_i - \hat{1}_i)(\hat{0}_p\hat{0}_q + \hat{1}_p\hat{1}_q), \hat{C}_{1X[i,pq]} = (\hat{1}_i - \hat{0}_i)(\hat{0}_p\hat{1}_q + \hat{1}_p\hat{0}_q).$$

The correlators corresponding to the above operators can be easily calculated and given by

$$\langle \hat{C}_{0X[m,\bar{m}]} \rangle = \langle \hat{C}_{1X[m,\bar{m}]} \rangle = \frac{1}{2}. \quad (2.31)$$

2.3.2 Correlation conditions for bipartite arbitrary-dimensional Bell states

We proceed to introduce correlators to study the correlation structure of a bipartite arbitrary-dimensional Bell state:

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} |v\rangle \otimes |v\rangle. \quad (2.32)$$

The constructions of correlators are based on the basic idea shown in the introduction and mainly in the second theorem. The generalized Bell state plays an important role both in violations of Bell inequalities for two qudits [17, 18] and in quantum communication protocols [24]. Experiments have demonstrated generalized Bell states for $d = 3$ successfully and even used for further applications [23].

Specification 1. The correlator operators presented in this specification can be formulated by the following general form

$$\hat{C}_k^{(rt)}(v_1^{(r)}, v_1'^{(r)}, v_2^{(t)}) = (\hat{v}_1^{(r)} - \hat{v}_1'^{(r)}) \otimes \hat{v}_2^{(t)}, \quad (2.33)$$

where the superscripts, (rt) , (r) , and (t) , mean that the measurement $\hat{V}_1^{(r)}$ numbered r and the one $\hat{V}_2^{(t)}$ numbered t have been selected from two choices by each party. Four

designations of $(v_1^{(r)}, v_1'^{(r)}, v_2^{(t)})$ associated four local measurement settings are given by

$$\begin{aligned}
 (v_1^{(1)} \doteq -k, v_1'^{(1)} \doteq 1 - k, v_2^{(2)} = k), \\
 (v_1^{(2)} \doteq d - k - 1, v_1'^{(2)} \doteq -k, v_2^{(1)} = k), \\
 (v_1^{(h)} \doteq -k, v_1'^{(h)} \doteq d - k - 1, v_2^{(h)} = k),
 \end{aligned} \tag{2.34}$$

for $h = 1, 2$ and $k = 0, 1, \dots, d-1$, where \doteq denotes equality modulo d . The set of operators $\{\hat{C}_k^{(rt)}\}$ is a special case of the general one $\{\hat{C}_k^{(q)}\}$ discussed in the second theorem, and for each measurement setting $\{\hat{C}_k^{(rt)}\}$ involves one set of correlation condition rather than γ_d conditions for $\{\hat{C}_k^{(q)}\}$.

To evaluate the correlators concretely, we choose specific sets of complete orthonormal basis $\{|v_j^{(h)}\rangle_{V_j^{(h)}}\}$ for projectors $\{\hat{v}_j^{(h)} = |v_j^{(h)}\rangle_{V_j^{(h)}}\langle v_j^{(h)}|\}$ and operators $\{\hat{V}_j^{(h)}\}$, where

$$|v_j^{(h)}\rangle_{V_j^{(h)}} = \frac{1}{d} \sum_{v=0}^{d-1} \exp[i\frac{2\pi v}{d}(v_j^{(h)} + n_j^{(h)})] |v\rangle, \tag{2.35}$$

and $n_j^{(h)}$ are local parameters that manifest observable $\hat{V}_j^{(h)}$. For a set of local parameters given by

$$n_1^{(1)} = 0, n_2^{(1)} = 1/4, n_1^{(2)} = 1/2, n_2^{(2)} = -1/4, \tag{2.36}$$

the joint probabilities for obtaining a set of measured outcome $(v_1^{(r)}, v_2^{(t)})$ for the state $|\Psi\rangle$ is [17]

$$\langle \hat{v}_1^{(r)} \otimes \hat{v}_2^{(t)} \rangle = \frac{1}{2d^3 \sin^2[\frac{\pi}{d}(v^{(rt)} + n^{(rt)})]}, \tag{2.37}$$

where $v^{(rt)} = v_1^{(r)} + v_2^{(t)}$ and $n^{(rt)} = n_1^{(r)} + n_2^{(t)}$. Therefore, the correlators $\langle \hat{C}_k^{(rt)} \rangle$ can be calculated analytically, and then we arrive at

$$\langle \hat{C}_k^{(rt)} \rangle = \frac{1}{2d^3} [\csc^2(\frac{\pi}{4d}) - \csc^2(\frac{3\pi}{4d})]. \tag{2.38}$$

Since $\langle \hat{C}_k^{(rt)} \rangle > 0$ for all k 's with any finite value of d , we ensure that outcomes of measurements performed on particles of a state $|\Psi\rangle$ are dependent under four different local measurement settings.

Specification 2. We can generalize the designations $(v_1^{(r)}, v_1'^{(r)}, v_2^{(t)})$ introduced in the above specification to more general cases. The correlator operators are given by

$$\hat{C}_{k\alpha}^{(rt)} = (\hat{v}_1^{(r)} - \hat{v}_1'^{(r)}) \otimes \hat{v}_2^{(t)}. \quad (2.39)$$

We propose the following designation as the kernel of the second specification of correlation:

$$\begin{aligned} (v_1^{(1)} \doteq k - \alpha, v_1'^{(1)} \doteq k + \alpha + 1, v_2^{(2)} = k), \\ (v_1^{(2)} \doteq k - \alpha - 1, v_1'^{(2)} \doteq k + \alpha, v_2^{(1)} = k), \\ (v_1^{(h)} \doteq k + \alpha, v_1'^{(h)} \doteq k - \alpha - 1, v_2^{(h)} = k), \end{aligned} \quad (2.40)$$

for $h = 1, 2, k = 0, 1, \dots, d - 1$, and $\alpha = 0, \dots, \lfloor d/2 - 1 \rfloor$.

The sets of projectors $\{\hat{v}_j^{(h)} = |v_j^{(h)}\rangle_{V_j^{(h)} V_j^{(h)}} \langle v_j^{(h)}|\}$ for the first qudit and the second one are defined by two specific sets of complete orthonormal basis $\{|v_j^{(h)}\rangle_{V_j^{(h)}}\}$, where

$$\begin{aligned} |v_1^{(h)}\rangle_{V_1^{(h)}} &= \frac{1}{d} \sum_{v=0}^{d-1} \exp[i \frac{2\pi v}{d} (v_1^{(h)} + n_1^{(h)})] |v\rangle, \\ |v_2^{(h)}\rangle_{V_2^{(h)}} &= \frac{1}{d} \sum_{v=0}^{d-1} \exp[i \frac{2\pi v}{d} (-v_2^{(h)} + n_2^{(h)})] |v\rangle, \end{aligned} \quad (2.41)$$

and the set of local parameters $\{n_j^{(h)}\}$ chosen is the same as the one used in the first specification. We have the correlators

$$\langle \hat{C}_{k\alpha}^{(rt)} \rangle = \frac{1}{2d^3} \left\{ \csc^2 \left[\frac{(1 + 4\alpha)\pi}{4d} \right] - \csc^2 \left[\frac{(3 + 4\alpha)\pi}{4d} \right] \right\}, \quad (2.42)$$

which are positive for all k 's and α 's considered. For a given α , we have one necessary

condition of the generalized Bell state. Thus one can feature the quantum correlations embedded in the bipartite d -level Bell state in $4\lfloor d/2 \rfloor$ sets of correlators and hence have $4\lfloor d/2 \rfloor$ necessary conditions.

Specification 3. There is a specific relation between the projector $\hat{v}_1^{(r)}$ and $\hat{v}_1'^{(r)}$ via the variable α introduced in the second specification. Then it is natural to consider a generalization about sets of correlators containing two variables. For this motivation, we introduce correlators of the form

$$\hat{C}_{k\eta\mu}^{(rt)} = (\hat{v}_1^{(r)} - v_1'^{(r)}) \otimes \hat{v}_2^{(t)}, \quad (2.43)$$

where

$$(v_1^{(r)} \doteq \eta - k, v_1'^{(r)} \doteq \mu - k, v_2^{(t)} = k), \quad (2.44)$$

for $k = 0, 1, \dots, d-1$, and η and μ are introduced variables. Let the projectors $\{\hat{v}_j^{(h)}\}$ are the same as the one introduced in the first specification, refer to Eq. (2.35) and definitions before which. Then the probability for getting a set of result $(v_1^{(r)}, v_2^{(t)})$ is

$$\langle \hat{v}_1^{(r)} \otimes \hat{v}_1^{(r)} \rangle = \frac{1 \sin^2[\pi(v^{(rt)} + n^{(rt)})]}{d^3 \sin^2[\frac{\pi}{d}(v^{(rt)} + n^{(rt)})]}. \quad (2.45)$$

From which we have the correlators:

$$\langle \hat{C}_{k\eta\mu}^{(rt)} \rangle = \langle \hat{\eta} \otimes \hat{\theta} \rangle - \langle \hat{\mu} \otimes \hat{\theta} \rangle, \quad (2.46)$$

for all k 's, and for each local measurement setting chosen, all of the correlators $\langle \hat{C}_{k\eta\mu}^{(rt)} \rangle$ satisfy either of the conditions:

$$\langle \hat{C}_{k\eta\mu}^{(rt)} \rangle > 0, \text{ for } k = 0, 1, \dots, d-1, \quad (2.47)$$

$$\langle \hat{C}_{k\eta\mu}^{(rt)} \rangle < 0, \text{ for } k = 0, 1, \dots, d-1, \quad (2.48)$$

i.e., the criteria of dependence.

Specification 4. In the previous three specifications, we use four local measurement settings to investigate correlations. Whereas we will give correlators under two measurement settings in this specification. For the first setting, our operators of correlators are of the form:

$$\hat{C}_k^{(q)} = [\hat{k} - T(\hat{k})] \otimes \hat{k}, \quad (2.49)$$

for $k = 0, 1, \dots, d-1$ and $q = 1, \dots, \gamma_d$, where $\hat{k} = |k\rangle \langle k|$. The above formulation of $\{\hat{C}_k^{(q)}\}$ follows the same definition as the one introduced in the second theorem, and note that we have applied $U(\hat{k}) = \hat{k}$ to the present specification.

For the second measurement setting, we choose a specific complete set of orthonormal basis vectors $\{|v_j\rangle_{F_j}\}$ where

$$|v_j\rangle_{F_j} = \frac{1}{d} \sum_{v=0}^{d-1} \exp(-i\frac{2\pi v}{d}v_j) |v\rangle, \quad (2.50)$$

to represent correlator operators, and then we give the following operators of correlators

$$\hat{C}_{kF}^{(q)} = [\hat{k} - T(\hat{k})] \otimes \hat{v}_2, \quad (2.51)$$

for $k = 0, 1, \dots, d-1$ and $q = 1, \dots, \gamma_d$, where $\hat{v}_j = |v_j\rangle_{F_j} \langle v_j|$ and $v_2 + k \doteq 0$. By a direct calculation, one has the correlators

$$\langle \hat{C}_k^{(q)} \rangle = \langle \hat{C}_{kF}^{(q)} \rangle = \frac{1}{d}, \quad (2.52)$$

for all k 's and q 's, which satisfies the condition of dependence.

2.4 Correlators embedded in Bell inequalities

Entanglement manifests itself via correlations in different directions of measurements. In the previous section, we feature quantum correlations of the genuine many-qubit GHZ states and the two-qudit Bell state in the correlators under different local measurement settings. These correlators can be considered as necessary conditions of the states under study. In addition to the CHSH inequality discussed in Sec. 2.2, further, we will reveal that four Bell inequalities that have been presented are composed of correlators.

2.4.1 Bell inequalities for many qubits

Seevinck-Svetlichny inequality

In the first specification for the N -qubit GHZ state, we give 2^N sets of correlators corresponding 2^N local measurement settings to describe the correlation structure of a GHZ state. It is worth noting that each set of correlator $(\hat{C}_{0l}, \hat{C}_{1l})$ provides information about correlations between any two subsystems of the N -qubit state and give n_c sets of necessary conditions of a generalized GHZ state. Each correlator has the same value whatever a partition is chosen, i.e., $\langle \hat{C}_{0l[\mathbf{m}, \bar{\mathbf{m}}]} \rangle = \langle \hat{C}_{1l[\mathbf{m}, \bar{\mathbf{m}}]} \rangle = \frac{1}{2\sqrt{2}}$, for $l = 1, \dots, 2^N$ and for all different partitions involved in $\{[\mathbf{m}, \bar{\mathbf{m}}]\}$, which describes the properties of *genuine* multipartite entanglement. A N -qubit genuine multipartite entanglement cannot be created without participation of *all* of the N particles. It is an interesting question whether one can use these correlators associated characters of many-qubit correlation to rule out correlations predicted by local-realistic theories.

Using a linear combination of the correlators

$$C_{\Phi_1} = \sum_l \langle \hat{C}_{0l} \rangle + \langle \hat{C}_{1l} \rangle \quad (2.53)$$

could be a means of the identification of a N -qubit GHZ state, which helps to approach the question mentioned above. Recently, Seevinck and Svetlichny [15] introduce a new

type of hidden variable theory by studying *partial separability*. The hypothesis of partial separability says that each subsystem of a N -particle decaying ensemble forms extended systems which are uncorrelated to each other [15]. Then, for a subsystem with m particles which is uncorrelated with the one with $N - m$ elements, the hypothesis of partial separability can be represented through a factorizable expression for joint probability given by

$$\begin{aligned} P(v_1, v_2, \dots, v_N) \\ = \int p(v_1, v_2, \dots, v_m | \lambda) q(v_{m+1}, v_{m+2}, \dots, v_N | \lambda) d\rho(\lambda), \end{aligned}$$

where p and q are probabilities conditioned to the hidden variable λ with probability measure $d\rho$.

For systems constrained by the hypothesis of partial separability, Seevinck and Svetlichny [15] have proved that local realistic theories predict C_{Φ_1} by $C_{\Phi_1,LR} \leq 2^{N-1}$, which is smaller than $2^{N-1/2}$ that a truly N -qubit GHZ state can achieve. In addition, they also showed that for any N -particle systems with the partition $[k' | k : 1, \dots, N; k \neq k']$, i.e. biseparable, the sum of correlators gives the bound $C_{\Phi_1} \leq 2^{N-1}$. Thus from their results, we realize that the many-particle correlations of a N -qubit GHZ state and C_{Φ_1} cannot be mimicked by biseparable states and cannot be reproduced by systems governed by the hypothesis of partial separability.

Mermin inequality

A linear combination of correlator operators proposed in the second specification for a N -qubit GHZ state, $\hat{C}_{\Phi_2} = \sum_l \hat{C}_{0l} + \hat{C}_{1l}$, can be rephrased in the following form:

$$\hat{C}_{\Phi_2} = \frac{1}{2} \left[\bigotimes_{k=1}^N (X_k + iY_k) + \bigotimes_{k=1}^N (X_k - iY_k) \right], \quad (2.54)$$

where $\{X_k, Y_k\}$ denotes the set of observable $\{X, Y\}$ for the k th particle. It is remarkable that \hat{C}_{Φ_2} is an alternative form of the operator introduced by Mermin [14] for Bell

inequality. For a N -qubit GHZ state, quantum correlations provide $C_{\Phi_2} = \langle \hat{C}_{\Phi_2} \rangle = 2^{N-1}$. Mermin showed that correlations predicted by quantum mechanics are stronger than the ones predicted by local-realistic theories by the following inequalities [14]: $C_{\Phi_2,LR} \leq 2^{N/2}$, for even N , and $C_{\Phi_2,LR} \leq 2^{(N-1)/2}$, for odd N .

A N -qubit GHZ state is the eigenstate of \hat{C}_{Φ_2} with the maximum eigenvalue 2^{N-1} . Then a N -qubit GHZ state gives a maximal violation of the Mermin inequality. In addition to this fact, through the correlators proposed, we gain an insight into the structure of \hat{C}_{Φ_2} . In particular, by an analytical analysis of the elements of \hat{C}_{Φ_2} , one can realize that the correlation conditions that are necessary for states to be a N -qubit GHZ state are embedded in \hat{C}_{Φ_2} . From which, we could know how property of quantum correlations manifests itself via correlations in different measurement settings in a concrete way.

2.4.2 Bell inequalities for two qudits

Correlator-based Bell inequalities

We combine all of the correlator operators introduced in the first specification for the state $|\Psi\rangle$,

$$\hat{C}_{\Psi_1}^{(d)} = \sum_{r,t,k} \hat{C}_k^{(rt)}, \quad (2.55)$$

and use its expectation value $C_{\Psi_1}^{(d)} = \langle \hat{C}_{\Psi_1}^{(d)} \rangle$ to be a single identification of the correlation properties of entangled qudits. Then it is interesting to investigate what is the maximal values of $C_{\Psi_1}^{(d)}$ that can be provided by classical correlations under local-realistic theories.

The expectation value $C_{\Psi_1}^{(d)}$ for any physical systems can be represented as:

$$\begin{aligned}
 C_{\Psi_1}^{(d)} = & P(v_1^{(1)} + v_2^{(1)} \doteq 0) - P(v_1^{(1)} + v_2^{(1)} \doteq -1) \\
 & + P(v_1^{(1)} + v_2^{(2)} \doteq 0) - P(v_1^{(1)} + v_2^{(2)} \doteq 1) \\
 & + P(v_1^{(2)} + v_2^{(2)} \doteq 0) - P(v_1^{(2)} + v_2^{(2)} \doteq -1) \\
 & + P(v_1^{(2)} + v_2^{(1)} \doteq -1) - P(v_1^{(2)} + v_2^{(1)} \doteq 0),
 \end{aligned} \tag{2.56}$$

where $P(\cdot)$ denotes a joint probability for getting a set of result $(v_1^{(r)}, v_2^{(t)})$ which satisfies a condition shown in the bracket. In order to have a compact form of $C_{\Psi_1}^{(d)}$ for a convenient discussion, we define the following variables:

$$\begin{aligned}
 \chi_{11} &= v_1^{(1)} + v_2^{(1)} + \dot{d}_{11}, \\
 \chi_{12} &= -v_1^{(1)} - v_2^{(2)} + \dot{d}_{12}, \\
 \chi_{22} &= v_1^{(2)} + v_2^{(2)} + \dot{d}_{22}, \\
 \chi_{21} &= -v_1^{(2)} - v_2^{(1)} - 1 + \dot{d}_{21},
 \end{aligned} \tag{2.57}$$


where \dot{d}_{rt} denotes a multiple of d and $\chi_{rt} \in \{-1, 0\}$ for $r, t = 1, 2$. In particular, the sum of the variables satisfies the constrain:

$$\sum_{r,t=1}^2 \chi_{rt} \doteq -1. \tag{2.58}$$

With the defined variables, $C_{\Psi_1}^{(d)}$ is written as

$$C_{\Psi_1}^{(d)} = \sum_{r,t=1}^2 P(\chi_{rt} = 0) - P(\chi_{rt} = -1). \tag{2.59}$$

Next, we proceed to consider the extreme values of $C_{\Psi_1}^{(d)}$ under the local-realistic theories. The all possible sets of $(\chi_{11}, \chi_{12}, \chi_{22}, \chi_{21})$ which fulfill the constraint of the sum of the variables are as the following: (i) three of the variables are 0 and the rest is -1 . (ii) all of the variables are -1 . The first class can be applied to arbitrary d , whereas the

second one is only applicable for $d = 3$. Thus, we have $C_{\Psi_1, \text{LR}}^{(d)} = 2$ for the class (i) and $C_{\Psi_1, \text{LR}}^{(3)} = -4$ for (ii), which mean that for all the generators of the convex polytope for $C_{\Psi_1, \text{LR}}^{(d)}$ the value of $C_{\Psi_1, \text{LR}}^{(d)}$ is equal or less than 2. Therefore, in the regime governed by local-realistic theories, the value of $C_{\Psi_1, \text{LR}}^{(d)}$ is bounded by 2, i.e., $C_{\Psi_1, \text{LR}}^{(d)} \leq 2$.

For a generalized Bell state, the summation of all of the correlators can be calculated analytically and we have

$$\langle \hat{C}_{\Psi_1}^{(d)} \rangle = \frac{1}{2d^2} [\csc^2(\frac{\pi}{4d}) - \csc^2(\frac{3\pi}{4d})]. \quad (2.60)$$

which is an increasing function of d . For example, if $d = 3$, one has $\langle \hat{C}_{\Psi_1}^{(3)} \rangle \simeq 2.87293$, and in the limit of large d , we obtain, $\lim_{d \rightarrow \infty} \langle \hat{C}_{\Psi_1}^{(d)} \rangle = (16/3\pi)^2 \simeq 2.88202$. From the above results, we realize that $\langle \hat{C}_{\Psi_1}^{(d)} \rangle > C_{\Psi_1, \text{LR}}^{(d)}$. Therefore, the quantum correlations are stronger than the ones predicted by the local-realistic theories. With this fact, the derived kernel $C_{\Psi_1}^{(d)}$ can be utilized to tell quantum correlations from classical ones.

From a geometric point of view, we have examined our Bell-type inequality by the work of Masanes about *tightness* of Bell inequalities [115]. The result shows that the inequality is non-tight, i.e., it is not an optimal detector of non-local-realistic correlation. The detailed proof and discussions are given in Appendix A.

We proceed to consider another Bell inequality which consists of only the sets of correlators $C_{k\alpha}^{(rt)} = \langle \hat{C}_{k\alpha}^{(rt)} \rangle$ for $\alpha = 0$ presented in the second specification for the generalized Bell states. The kernel of our Bell inequality is of the form

$$\begin{aligned} C_{\Psi_2}^{(d)} &= \sum_{r,t,k} C_{k0}^{(rt)} \\ &= P(v_2^{(1)} - v_1^{(1)} \doteq 0) - P(v_2^{(1)} - v_1^{(1)} \doteq 1) \\ &\quad + P(v_2^{(2)} - v_1^{(1)} \doteq 0) - P(v_2^{(2)} - v_1^{(1)} \doteq -1) \\ &\quad + P(v_2^{(2)} - v_1^{(2)} \doteq 0) - P(v_2^{(2)} - v_1^{(2)} \doteq 1) \\ &\quad + P(v_2^{(1)} - v_1^{(2)} \doteq 1) - P(v_2^{(1)} - v_1^{(2)} \doteq 0). \end{aligned} \quad (2.61)$$

Using the following substitutions,

$$\begin{aligned}
 \chi_{11} &= v_1^{(1)} - v_2^{(1)} + \dot{d}_{11}, \\
 \chi_{12} &= -v_1^{(1)} + v_2^{(2)} + \dot{d}_{12}, \\
 \chi_{22} &= v_1^{(2)} - v_2^{(2)} + \dot{d}_{22}, \\
 \chi_{21} &= -v_1^{(2)} + v_2^{(1)} - 1 + \dot{d}_{21},
 \end{aligned} \tag{2.62}$$

$C_{\Psi_2}^{\prime(d)}$ is expressed by

$$C_{\Psi_2}^{\prime(d)} = \sum_{r,t=1}^2 P(\chi_{rt} = 0) - P(\chi_{rt} = -1), \tag{2.63}$$

with the constraint $\sum_{r,t=1}^2 \chi_{rt} \doteq -1$. Then, by the same method as the approach for determining the extreme values of $C_{\Psi_{1,LR}}^{(d)}$, one has $C_{\Psi_{2,LR}}^{\prime(d)} \leq 2$. Whereas, for a generalized Bell state, the expectation values of $\hat{C}_{\Psi_2}^{\prime(d)}$ are $\langle \hat{C}_{\Psi_2}^{\prime(d)} \rangle = [\csc^2(\frac{\pi}{4d}) - \csc^2(\frac{3\pi}{4d})]/(2d^2)$ and are greater than the local-realistic upper bound for arbitrary d .

The above Bell inequality is non-tight. The proof for showing its tightness is similar to the one for $C_{\Psi_{1,LR}}^{(d)} \leq 2$, refer to Appendix A. In addition, although the values of maximal quantum violation are slightly smaller than the CGLMP inequalities [17], the total number of joint probabilities required by each of the presented correlation functions $C_{k0}^{\prime(rt)}$ is only $2d$, which is much smaller than that in Fu's general correlation function [109], which is about $O(d^2)$ (refer to the following discussions). Moreover, the factors for violations of Bell inequalities are larger than the ones for SLK inequalities [18] for $d > 2$ (see below). Another feature of the sum of all correlators is its robustness to noise. If a generalized Bell state is suffered from white noise and turns into a mixed one, say ρ , with a noise fraction p_{noise} , the value of $\langle \hat{C}_{\Psi_2}^{\prime(d)} \rangle$ for the state ρ becomes $\langle \hat{C}_{\Psi_2}^{\prime(d)} \rangle_{\rho} = (1 - p_{\text{noise}}) \langle \hat{C}_{\Psi_2}^{\prime(d)} \rangle$. If the criterion, $\langle \hat{C}_{\Psi_2}^{\prime(d)} \rangle_{\rho} > 2$, i.e., $p_{\text{noise}} < 1 - 2/\langle \hat{C}_{\Psi_2}^{\prime(d)} \rangle$, is imposed on the system, one ensures that the mixed state still exhibits quantum correlations in outcomes of measurements. For instance, to maintain the quantum correlation for the limit of large d , the system

must have $p_{\text{noise}} < 0.30604$.

CGLMP inequality

In the second specification of the state $|\Psi\rangle$, we have proposed $4\lfloor d/2 \rfloor$ sets of correlators to describe the structure of correlation. We use a linear combination of all of these correlators to detect quantum correlations. Since each correlator is a function of α , a combination of correlator operators could be of the form:

$$\hat{C}_{\Psi_2}^{(d)} = \sum_{\alpha, r, t, k} f(\alpha) \hat{C}_{k\alpha}^{(rt)}, \quad (2.64)$$

where $f(\alpha)$ denotes a coefficient of combination which is function of α . If we let $f(\alpha)$ be

$$f(\alpha) = 1 - \frac{2\alpha}{d-1}, \quad (2.65)$$

the summation of all of the correlators $C_{k\alpha}^{(rt)}$ becomes the kernel of the CGLMP inequality [17]:

$$C_{\Psi_2}^{(d)} = C_{\Psi_2}'^{(d)} + \sum_{\alpha=1}^{\lfloor d/2-1 \rfloor} \sum_{r,t=1}^2 \sum_{k=0}^{d-1} \left(1 - \frac{2\alpha}{d-1}\right) C_{k\alpha}^{(rt)}, \quad (2.66)$$

where $C_{\Psi_2}'^{(d)}$ is the kernel of correlator-based Bell inequality defined by Eq. (2.61). Especially, note that for $d = 2, 3$ the CGLMP inequalities are the correlator-based Bell inequalities. The local realistic constraint proposed by Collins *et al.* [17] specifies that correlations have to satisfy the condition: $C_{\Psi_2, \text{LR}}^{(d)} \leq 2$. On the other hand, by Eq. (2.42), quantum correlations of a generalized Bell state gives a violation of the CGLMP inequality for arbitrary high-dimensional systems. Thus, through the related discussions in the second specification for $|\Psi\rangle$, we realize that the CGLMP inequality is composed of correlators for correlations.

It is worth representing Eq. (2.66) in the following form:

$$C_{\Psi_2}^{(d)} = C^{(11)} + C^{(12)} - C^{(21)} + C^{(22)}, \quad (2.67)$$

where

$$C^{(rt)} = \sum_{\alpha=0}^{\lfloor d/2-1 \rfloor} \sum_{k=0}^{d-1} \varepsilon_{rt} \left(1 - \frac{2\alpha}{d-1}\right) C_{k\alpha}^{(rt)}, \quad (2.68)$$

$\varepsilon_{11} = \varepsilon_{22} = \varepsilon_{12} = 1$, and $\varepsilon_{21} = -1$. The representation of $C_{\Psi_2}^{(d)}$ in Eq. (2.67) takes the same simple form as the kernel of the CHSH inequality [13], and the linear combinations of correlators, $C^{(rt)}$, are just the general correlation functions of the CHSH inequality for arbitrarily high-dimensional systems introduced by Fu [109]. Each $C^{(rt)}$ provides $\lfloor d/2 \rfloor$ sets of correlators for identifying correlations and then consists of $2d\lfloor d/2 \rfloor$ joint probabilities.



SLK inequality

Following a way similar to the one for constructing the kernel of the CGLMP inequality, we take a linear combination of the operators of correlators proposed in the third specification for the generalized Bell state and give an operator of the form

$$\hat{C}_{\Psi_3}^{(d)} = \sum_{\eta, \mu, r, t, k} f^{(rt)}(\eta, \mu) \hat{C}_{k\eta\mu}^{(rt)}, \quad (2.69)$$

where $f^{(rt)}(\eta, \mu)$ is a coefficient of combination and depends on a local measurement chosen and a set of variables (η, μ) . Let us give a concrete example to show above formulation by the following summation of correlators:

$$\sum_{\eta=0}^{d-1} g^{(rt)}(\eta) \sum_{k=0}^{d-1} P(v_1 \doteq \eta - k, v_2 = k), \quad (2.70)$$

where

$$g^{(rt)}(\eta) = \frac{1}{4} \sin[2(\nu + \eta + \nu_{rt})\pi] \{ \cot[(\nu + \eta + \nu_{rt})\pi/d] - \cot[(\nu + \eta + \nu_{rt})\pi] \}, \quad (2.71)$$

for $\nu + \eta + \nu_{rt} \neq 0$, ν , and ν_{rt} are constants, and

$$g^{(rt)}(\eta) = \frac{1}{2}(d-1), \quad (2.72)$$

for $\nu + \eta + \nu_{rt} = 0$. It is worth noting that [116]

$$\sum_{\eta=0}^{d-1} g^{(rt)}(\eta) = 0, \quad (2.73)$$

for $\nu + \nu_{rt} \neq 0$, which indicates that the sum of positive $g^{(rt)}(\eta)$'s and negative ones is zero and implies that one can always have the following relation:

$$\begin{aligned} & \sum_{\eta=0}^{d-1} g^{(rt)}(\eta) \sum_{k=0}^{d-1} P(v_1^{(r)} \doteq \eta - k, v_2^{(t)} \doteq k) \\ &= \sum_{\eta, \mu, k} f^{(rt)}(\eta, \mu) \left[P(v_1^{(r)} \doteq \eta - k, v_2^{(t)} \doteq k) - P(v_1^{(r)} \doteq \mu - k, v_2^{(t)} \doteq k) \right]. \end{aligned} \quad (2.74)$$

If we choose the same measurement settings as the ones mentioned in the third specification and let $n_{1,2}^{(1)} = 0$, $n_{1,2}^{(2)} = 1/2$ (refer to Eqs. (2.35) and (2.45)), $\nu = \nu_{11} = 0$, $\nu_{22} = 1$, and $\nu_{12} = \nu_{21} = 1/2$, one obtains $\sum_{\eta=1}^{d-1} g(\eta)^{(hh)} = (1-d)/2$ and $g(0)^{(hh)} = (d-1)/2$ for $h = 1, 2$. Thus, one arrives at the exact forms of $f^{(rt)}(\eta, \mu)$ for $r = t = h$ that are given by $f^{(hh)}(0, \mu) = 1/2$. Furthermore, with Eq. (2.71) we have $g(\eta)^{(12)} = g(\eta)^{(21)} = 0$, which means that there are only two local measurement settings involved in the kernel. Thus $\langle \hat{C}_{\Psi_3}^{(d)} \rangle = C_{\Psi_3}^{(d)}$ is of the following explicit form:

$$C_{\Psi_3}^{(d)} = \frac{1}{2} \sum_{h=1}^2 \sum_{\mu=1}^{d-1} \sum_{k=0}^{d-1} \left[P(v_1^{(h)} \doteq -k, v_2^{(h)} \doteq k) - P(v_1^{(h)} \doteq \mu - k, v_2^{(h)} \doteq k) \right]. \quad (2.75)$$

For a generalized Bell state, the values of correlators $\langle \hat{C}_{k\eta\mu}^{(hh)} \rangle = P(v_1^{(h)} \doteq -k, v_2^{(h)} = k) - P(v_1^{(h)} \doteq \mu - k, v_2^{(h)} = k)$ strictly satisfy the criteria (2.47) by the facts $\langle \hat{C}_{k\eta\mu}^{(hh)} \rangle = 1/d$ for all parameters considered.

In the operator representation, $C_{\Psi_3}^{(d)}$ can be represented in the form

$$\hat{C}_{\Psi_3}^{(d)} = \frac{1}{4} \sum_{n=1}^{d-1} \bigotimes_{j=1}^N (\hat{V}_j^{(1)} + \omega^{n/2} \hat{V}_j^{(2)}) + \text{H.c.}, \quad (2.76)$$

where $\hat{V}^{(h)} = \sum_{v=0}^{d-1} \omega^v \hat{v}^{(h)}$ and $\omega = \exp(i2\pi/d)$. Furthermore, in the next section we will show $\hat{C}_{\Psi_3}^{(d)}$ can be used to construct entanglement witness operators to detect states close to $|\Psi\rangle$.

One also can utilize $\hat{C}_{\Psi_3}^{(d)}$ to detect a state under a local unitary transformation of one of the qudits of $|\Psi\rangle$. For example, the state $|\Psi_\nu\rangle = (I \otimes \hat{S}_\nu) |\Psi\rangle$, where \hat{S}_ν is a phase shift operator such that $\hat{S}_\nu |v\rangle = \omega^{\nu v} |v\rangle$, is detected by the following operator:

$$\begin{aligned} \hat{C}_{\Psi_{3\nu}}^{(d)} &= (I \otimes \hat{S}_\nu) \hat{C}_{\Psi_3}^{(d)} (I \otimes \hat{S}_\nu^\dagger) \\ &= \frac{1}{4} \sum_{n=1}^{d-1} \omega^{\nu n} \bigotimes_{j=1}^N (\hat{V}_j^{(1)} + \omega^{n/2} \hat{V}_j^{(2)}) + \text{H.c.} \end{aligned} \quad (2.77)$$

Furthermore, if $\nu = 1/4$ is chosen and other parameters involved in $g^{(rt)}(\eta)$ are set as the previous ones, the expectation value $\langle \hat{C}_{\Psi_{3\nu}}^{(d)} \rangle = C_{\Psi_{3\nu}}^{(d)}$ can be represented in terms of correlators:

$$\begin{aligned} C_{\Psi_{3\nu}}^{(d)} &= \sum_{\mu=1}^{d-1} \sum_{k=0}^{d-1} g^{(11)}(\mu) [P(v_1^{(1)} \doteq -k, v_2^{(1)} = k) - P(v_1^{(1)} \doteq \mu - k, v_2^{(1)} = k)] \\ &\quad + \sum_{r,t=1}^2 \sum_{\mu=0}^{d-2} \sum_{k=0}^{d-1} g^{(rt)}(\mu) [P(v_1^{(r)} \doteq d-1-k, v_2^{(t)} = k) \\ &\quad - P(v_1^{(r)} \doteq \mu - k, v_2^{(t)} = k)], \end{aligned} \quad (2.78)$$

where in the last line the summation of local measurement setting does not include

$(r, t) = (1, 1)$. Since $g^{(rt)}(\mu) \neq 0$ for all r 's and t 's, four measurement settings are required for realizing $\hat{C}_{\Psi_{3\nu}}^{(d)}$. For generalized GHZ states, the sum of correlators is $C_{\Psi_3}^{(d)} = C_{\Psi_{3\nu}}^{(d)} = d - 1$. Son *et al.* [18] have shown that local-realistic theories predict the value of $C_{\Psi_{3\nu}}^{(d)}$ by

$$C_{\Psi_{3\nu},\text{LR}}^{(d)} \leq \frac{1}{4} \left[3 \cot\left(\frac{\pi}{4d}\right) - \cot\left(\frac{\pi}{3d}\right) \right] - 1, \quad (2.79)$$

for arbitrarily high-dimensional systems, which is called the SLK inequality. The SLK inequality is shown to be violated by the generalized Bell state by a factor:

$$\lim_{d \rightarrow \infty} \frac{C_{\Psi_3}^{(d)}}{C_{\Psi_{3\nu},\text{LR}}^{(d)}} = \frac{3\pi}{8} \simeq 1.1781, \quad (2.80)$$

for large limit of d , which is smaller than the ones for the CGLMP [17] ($\simeq 1.4849$) and the correlator-based ($\simeq 1.4410$) Bell inequalities.

2.5 Correlators imbedded in entanglement witness operators

Using partial or complete knowledge of a state to be created is an usual way to construct an entanglement witness operator for identifying an experimental output state. Choice of correlation criteria used to feature entanglement affects the effort for realizing identifications of quantum correlations. Thereby, how to feature the state under study in criteria that can describe the central part of correlation properties of entanglement and can be realized efficiently is a crucial task. In what follows, we will show the correlation conditions in terms of correlators are useful for performing entanglement detections. Since operators of correlators are locally measurable, these witnesses can be performed with Bell-type experiments and require only two local measurement settings. Furthermore, we reveal known inequalities of entanglement are composed of correlators.

2.5.1 Detections of genuine many-qubit GHZ states

Since correlators proposed in the third specification for the many-qubit GHZ state consists of conditions of many-qubit correlations, we use them to detect genuine multipartite entanglement. Since we know that

$$\sum_{k=0}^1 \langle \hat{C}_{kZ[\mathbf{m}|\bar{\mathbf{m}}]} \rangle = \sum_{k=0}^1 \langle \hat{C}_{kX[\mathbf{m}|\bar{\mathbf{m}}]} \rangle = 1$$

from the previous results, the strategy of entanglement detection follows the basic idea shown in the examples (a), (b), and related discussions in Sec. 2.2. The central part of our witness is a linear combination of correlator operators:

$$\begin{aligned} \hat{C}_\Phi &= c_z \sum_{\{\mathbf{m}|\bar{\mathbf{m}}\}} (\hat{C}_{0Z[\mathbf{m}|\bar{\mathbf{m}}]} + \hat{C}_{1Z[\mathbf{m}|\bar{\mathbf{m}}]}) \\ &\quad + c_x \sum_{\{\mathbf{m}|\bar{\mathbf{m}}\}} (\hat{C}_{0X[\mathbf{m}|\bar{\mathbf{m}}]} + \hat{C}_{1X[\mathbf{m}|\bar{\mathbf{m}}]}) \\ &= c_z [2^{N-1}(\hat{0}^{\otimes N} + \hat{1}^{\otimes N}) - \mathbf{1}] + c_x (2^{N-1} - 1)X^{\otimes N}, \end{aligned} \quad (2.81)$$

where c_z and c_x are constants, and $\mathbf{1}$ denotes an identity matrix with 2^N dimensions.

From which, we give the following entanglement witness operator

$$\mathcal{W}_\Phi = \alpha_\Phi \mathbf{1} - \hat{C}_\Phi, \quad (2.82)$$

where α_Φ is some constant. With a well choice of (c_z, c_x, α_Φ) , if $\text{Tr}(\mathcal{W}_\Phi \rho) < 0$ for some experimental output state ρ , the state ρ is identified as a truly multipartite entanglement close to a N -qubit GHZ state.

To determine whether an operator \mathcal{W}_Φ is a witness, firstly we compare \mathcal{W}_Φ with a project-based witness operator of the form:

$$\mathcal{W}_\Phi^p = \alpha_\Phi^p \mathbf{1} - |\Phi\rangle \langle \Phi|, \quad (2.83)$$

where $\alpha_{\Phi}^p = \max_{|\chi\rangle \in B} |\langle \chi | \Phi \rangle|^2$, and B denotes the set of biseparable states. The overlap α_{Ψ}^p can be determined through the general method proposed by Bourennane *et al.* [70], and thereby $\alpha_{\Phi}^p = 1/2$ is obtained. If measured outcomes show that $\text{Tr}(\mathcal{W}_{\Phi}^p \rho) < 0$, the state ρ is identified as an entanglement close to $|\Phi\rangle$. Thus we have to show if the state ρ satisfies $\text{Tr}(\mathcal{W}_{\Phi} \rho) < 0$, it also satisfies $\text{Tr}(\mathcal{W}_{\Phi}^p \rho) < 0$, i.e., $\mathcal{W}_{\Phi} - \gamma_{\Phi} \mathcal{W}_{\Phi}^p \geq 0$ where γ_{Φ} is some positive constant [72]. Second, we concern the robustness of an operator which satisfies the above condition. The robustness to noise can be determined by the noise tolerance: $p_{\text{noise}} < \delta_{\text{noise}}$, is such that $|\Phi\rangle$ suffered from white noise with a noise fraction p_{noise} is identified as a truly multipartite entanglement. When taking above two points into consideration, we have ($c_z = 2, c_x = 2^{N-1}, \alpha_{\Phi} = 3c_z c_x / 2 - c_z - c_x$) and $\gamma_{\Phi} = c_z c_x$ for achieving a noise tolerance $\delta_{\Phi} = (3 - 4/2^N)^{-1}$.

We find that the witnesses \mathcal{W}_{Φ} proposed possess the same structures of the one given by Ref. [72] based on the stabilizer formalism [117], which means that one could investigate the stabilizer entanglement witnesses [72] via concrete and analytical conditions of correlations based on correlators.

2.5.2 Inequalities based on the geometry of spin vectors

Before investigating the structure of inequalities of entanglement proposed by Dukin and Simon [110], we will discuss the multi-qubit entangled states involved in the violations of the inequalities. First, let us investigate the correlation structure of a two-qubit entanglement imbedded in the eigenstate of dot product of two spins:

$$\begin{aligned} \hat{D}^{(2)} &= \mathbf{S}_1 \cdot \mathbf{S}_2, \\ &= X_1 \otimes X_2 + Y_1 \otimes Y_2 + Z_1 \otimes Z_2, \end{aligned} \quad (2.84)$$

where $\mathbf{S}_k = \{X_k, Y_k, Z_k\}$. In the following the symbol of tensor product will be omitted from the equations for simplicity. We focus on the eigenstate with the extreme (means *maximal* or *minimal*) eigenvalue of $\hat{D}^{(2)}$, i.e., the singlet state $|D_2\rangle = |\psi\rangle$. Since

$\hat{D}_l^{(2)} |D_2\rangle = -|D_2\rangle$, where $\hat{D}_1^{(2)} = X_1X_2$, $\hat{D}_2^{(2)} = Y_1Y_2$, and $\hat{D}_3^{(2)} = Z_1Z_2$, each $\hat{D}_l^{(2)}$ contributes equally towards the minimal eigenvalue of $\hat{D}^{(2)}$ which is -3 . For the state $|D_2\rangle$ with the operators $\hat{D}_l^{(2)} = \hat{C}_0^+ + \hat{C}_1^+$, we have the correlators $\langle \hat{C}_0^+ \rangle = \langle \hat{C}_1^+ \rangle = -1/2$ that satisfy the condition of dependence, and we are convinced that the qubits of the singlet state are *dependent* on each other.

We give another example by considering the structure of the entangled pair with the form:

$$|Q_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + i|10\rangle), \quad (2.85)$$

which is also the eigenvector with the maximal eigenvalue of the z -direction component of the cross product between two spins:

$$\begin{aligned} \hat{Q}_{2z} &= (\mathbf{S}_2 \times \mathbf{S}_1)_z \\ &= Y_1X_2 - X_1Y_2. \end{aligned} \quad (2.86)$$

It is clear that $\hat{Q}_{2z,1} = Y_1X_2$ and $\hat{Q}_{2z,2} = -X_1Y_2$ are comprised of correlator operators. The necessary conditions of quantum correlation of $|Q_2\rangle$ are specified by $\langle \hat{C}_0^+ \rangle = \langle \hat{C}_1^+ \rangle = 1/2$ for $\hat{Q}_{2z,1} = \hat{C}_0^+ + \hat{C}_1^+$ and $\langle \hat{C}_0^- \rangle = \langle \hat{C}_1^- \rangle = 1/2$ for $\hat{Q}_{2z,2} = \hat{C}_0^- + \hat{C}_1^-$, which proves the above statement.

For three-qubit cases, first, we consider an entanglement of the eigenstate with extreme eigenvalues of the following operator composed of cross and dot product of spins:

$$\begin{aligned} \hat{D}^{(3)} &= \mathbf{S}_3 \cdot (\mathbf{S}_2 \times \mathbf{S}_1) \\ &= Z_1Y_2X_3 - Y_1Z_2X_3 + X_1Z_2Y_3 - Z_1X_2Y_3 + Y_1X_2Z_3 - X_1Y_2Z_3. \end{aligned} \quad (2.87)$$

We denote every element of $\hat{D}^{(3)}$ by $\hat{D}_l^{(3)}$ for $l = 1, 2, \dots, 6$ according to the order shown in the above equation, e.g. $\hat{D}_1^{(3)} = Z_1Y_2X_3$, $\hat{D}_2^{(3)} = -Y_1Z_2X_3$ *et al.*. The state represented

by the following form

$$|D_3\rangle = \frac{1}{\sqrt{3}}(|011\rangle - e^{-i\pi/3}|110\rangle - e^{i\pi/3}|101\rangle), \quad (2.88)$$

is the eigenstate with the maximum eigenvalue $2\sqrt{3}$ of $\hat{D}^{(3)}$ and gives $\langle \hat{D}_l^{(3)} \rangle = 1/\sqrt{3}$ for all l 's.

We can utilize $\hat{D}_l^{(3)}$ to describe the characters of entanglement of the state $|D_3\rangle$ by the first theorem. Every operator belonging to $\{\hat{D}_l^{(3)} : l = 1, \dots, 6\}$ possesses three types of detections of quantum correlation according to the partitions of the system $\{[1, 2, 3]\}$. Let us take $\hat{D}_1^{(3)}$ for example, for the state $|D_3\rangle$, we have the following correlators with positive values to show the dependence of qubits:

$$\begin{aligned} \langle \hat{C}_{0[1|2,3]}^+ \rangle &= (\sqrt{3} - 1)/6, \langle \hat{C}_{1[1|2,3]}^+ \rangle = (\sqrt{3} + 1)/6, \\ \langle \hat{C}_{0[2|1,3]}^+ \rangle &= \langle \hat{C}_{1[2|1,3]}^+ \rangle = 1/2\sqrt{3}, \\ \langle \hat{C}_{0[3|1,2]}^+ \rangle &= \langle \hat{C}_{1[3|1,2]}^+ \rangle = 1/2\sqrt{3}. \end{aligned}$$

Moreover, for $\hat{D}_2^{(3)} = -Y_1 Z_2 X_3$, we have

$$\begin{aligned} \langle \hat{C}_{0[1|2,3]}^- \rangle &= \langle \hat{C}_{1[1|2,3]}^- \rangle = 1/2\sqrt{3}, \\ \langle \hat{C}_{0[2|1,3]}^- \rangle &= (\sqrt{3} - 1)/6, \langle \hat{C}_{1[2|1,3]}^- \rangle = (\sqrt{3} + 1)/6, \\ \langle \hat{C}_{0[3|1,2]}^- \rangle &= \langle \hat{C}_{1[3|1,2]}^- \rangle = 1/2\sqrt{3}, \end{aligned}$$

which also show the character of dependent qubits. We have shown that the other four sets of correlators also fulfill the condition of correlation. Hence we could consider the criteria involved in the correlators of $\{\hat{D}_l^{(3)} : l = 1, \dots, 6\}$ as the necessary conditions for the state $|D_3\rangle$ and specify the structure of quantum correlation under six settings of local measurements. Therefore we reveal that the observable $\hat{D}^{(3)} = \sum_{l=1}^6 \hat{D}_l^{(3)}$ consists of the conditions of multipartite entanglement for its eigenstate $|D_3\rangle$ through the conditions of quantum correlations introduced.

Let us proceed with another three-qubit entangled state of the form:

$$|Q_3\rangle = \frac{1}{2}(|011\rangle - |101\rangle - \sqrt{2}|110\rangle), \quad (2.89)$$

which is the eigenstate of the z -component of cross product of three spins:

$$\begin{aligned} \hat{Q}_{3z} &= [\mathbf{S}_3 \times (\mathbf{S}_2 \times \mathbf{S}_1)]_z, \\ &= X_1 Z_2 X_3 - Z_1 X_2 X_3 - Z_1 Y_2 Y_3 + Y_1 Z_2 Y_3, \end{aligned} \quad (2.90)$$

corresponding to the maximal eigenvalue $2\sqrt{2}$. The structure of the state $|Q_3\rangle$ can be specified by the correlators involved in the operators $\hat{Q}_{3z,1} = X_1 Z_2 X_3$, $\hat{Q}_{3z,2} = -Z_1 X_2 X_3$, $\hat{Q}_{3z,3} = -Z_1 Y_2 Y_3$, and $\hat{Q}_{3z,4} = Y_1 Z_2 Y_3$. For example, $\hat{Q}_{3z,1}$ contains the necessary conditions of $|D_3\rangle$ due to the fact that

$$\begin{aligned} \langle \hat{C}_{0[1|2,3]} \rangle &= \langle \hat{C}_{1[1|2,3]} \rangle = 1/2\sqrt{2}, \\ \langle \hat{C}_{0[2|1,3]} \rangle &= (\sqrt{2} - 1)/4, \langle \hat{C}_{1[2|1,3]} \rangle = (\sqrt{2} + 1)/4, \\ \langle \hat{C}_{0[3|1,2]} \rangle &= \langle \hat{C}_{1[3|1,2]} \rangle = 1/2\sqrt{2}, \end{aligned}$$

and for $\hat{Q}_{3z,2} = -Z_1 X_2 X_3$ we can obtain more necessary ones by the following correlators:

$$\begin{aligned} \langle \hat{C}_{0[1|2,3]} \rangle &= (\sqrt{2} - 1)/4, \langle \hat{C}_{1[1|2,3]} \rangle = (\sqrt{2} + 1)/4, \\ \langle \hat{C}_{0[2|1,3]} \rangle &= \langle \hat{C}_{1[2|1,3]} \rangle = 1/2\sqrt{2}, \\ \langle \hat{C}_{0[3|1,2]} \rangle &= \langle \hat{C}_{1[3|1,2]} \rangle = 1/2\sqrt{2}. \end{aligned}$$

Therefore, \hat{Q}_{3z} is a linear combination of the operators which can be utilized to feature the state $|Q_3\rangle$.

The N -qubit entangled state $|D_N\rangle$ can be derived from the following observable:

$$\hat{D}^{(N)} = \mathbf{S}_N \cdot \mathbf{Q}_{N-1}, \quad (2.91)$$

where

$$\mathbf{Q}_{N-1} = \mathbf{S}_{N-1} \times \dots (\mathbf{S}_2 \times \mathbf{S}_1), \quad (2.92)$$

and $|D_N\rangle$ is the eigenstate of $\hat{D}^{(N)}$ with the extreme eigenvalue. From the cases which have been considered for $N = 2, \dots, 11$, we find that $\hat{D}^{(N)}$ consists of correlator operators for the state $|D_N\rangle$ and every pair of correlators satisfies the proposed condition of correlation. Furthermore, through the numerical results we know that the correlation between subsystems of qubits for all classifications $\{[1, 2, \dots, N]\}$ can be shown through the operators $\hat{D}_i^{(N)}$ which constitutes the operator $\hat{D}^{(N)} = \sum_i \hat{D}_i^{(N)}$ and details the N -qubit dependence in n_c ways (see Eq. (2.8)). Therefore, we have a complete information of the structures of $\hat{D}^{(N)}$ and $|D_N\rangle$ including the relation between them, and thereby one can view the spin observable $\hat{D}^{(N)}$ as a means of identification of truly multi-qubit quantum correlations embedded in the state $|D_N\rangle$. It is interesting to investigate the difference between *fully separable states* and $|D_N\rangle$ through $\hat{D}^{(N)}$. For fully separable states, Durkin and Simon [110] have shown that $|\langle \hat{D}^{(N)} \rangle_{\text{FS}}| \leq 1$. Whereas $|D_N\rangle$ for $N = 2, \dots, 11$ provide maximal violation of the above dot-type inequalities.

In addition to dot-type inequalities, \mathbf{Q}_N gives the cross-type inequalities by $\|\mathbf{Q}_N\|_{\text{FS}} \leq 1$ for fully separable states. Maximum values of $\|\mathbf{Q}_N\|$ and also the maximal violation of the inequality could be found by determining the maximum eigenvalues of the components of \mathbf{Q}_N e.g. \hat{Q}_{Nz} . Our numerical results show that the genuine multi-qubit correlation of the state $|Q_N\rangle$ for $N = 2, \dots, 11$ can be described by the proposed condition of correlation imbedded in the operators \hat{Q}_{Nz} , and the sum of all of the correlators is greater than one and violates the upper bound of the cross-type inequality for fully separable states.

2.5.3 Detecting entangled qudits with two local measurement settings

Two-qudit Bell state

It is an important and interesting question whether one can construct an entanglement witness operator to detect a truly many-qudit entanglement without using much experimental effort. Instead of investigating this subject, we will show one can detect multi-level entanglement for states in the proximity of a d -level Bell state with two local measurement settings, which is preliminary to the previous question.

We use the correlators introduced in the fourth specification of $|\Psi\rangle$ to construct an entanglement witness operator with a highly robustness, and with the fact that

$$\sum_{k=0}^{d-1} \langle \hat{C}_k^{(q)} \rangle = \sum_{k=0}^{d-1} \langle \hat{C}_{kF}^{(q)} \rangle = 1,$$

the basic idea relies on the strategy introduced in examples (a), (b), and related discussions in Sec. 2.2. The kernel of our witness is of the form:

$$\hat{C}_{\Psi_4} = \hat{C} + \hat{C}_F, \quad (2.93)$$

where

$$\begin{aligned} \hat{C} &= \sum_{q=1}^{\gamma_d} \sum_{k=0}^{d-1} \hat{C}_k^{(q)} \\ &= \sum_{k=0}^{d-1} \gamma_d \left(\hat{k} - \frac{1}{d-1} \sum_{k'=0, k' \neq k}^{d-1} \hat{k}' \right) \otimes \hat{k}, \end{aligned} \quad (2.94)$$

$$\begin{aligned} \hat{C}_F &= \sum_{q=1}^{\gamma_d} \sum_{k=0}^{d-1} \hat{C}_{kF}^{(q)} \\ &= \sum_{k=0}^{d-1} \gamma_d \left(\hat{k} - \frac{1}{d-1} \sum_{k'=0, k' \neq k}^{d-1} \hat{k}' \right) \otimes \hat{k}. \end{aligned} \quad (2.95)$$

Note that the representation of the projector \hat{k} 's in \hat{C} is different from the one in \hat{C}_F .

Then our witness operator is

$$\mathcal{W}_{\Psi_4} = \alpha_{\Psi_4} \mathbf{1} - \hat{C}_{\Psi_4}, \quad (2.96)$$

where $\alpha_{\Psi_4} = \gamma_d$ and $\mathbf{1}$ denotes an identify operator with d^2 dimensions. If a state ρ shows $\text{Tr}(\mathcal{W}_{\Psi_4}\rho) < 0$, ρ is identified as an entanglement close to the state $|\Psi\rangle$. Especially, the witness \mathcal{W}_{Ψ_4} is very robust. The robustness of \mathcal{W}_{Ψ_4} is determined by the noise tolerance: $p_{\text{noise}} < \delta_{\text{noise}}$, is such that

$$\rho = p_{\text{noise}} \mathbf{1}/d^2 + (1 - p_{\text{noise}}) |\Psi\rangle \langle \Psi| \quad (2.97)$$

is identified as an entanglement. The witness \mathcal{W}_{Ψ_4} tolerates noise if $p_{\text{noise}} < 1/2$, independent of the number of levels.

Next, we will show that the operator \mathcal{W}_{Ψ_4} is a witness. In order to achieve this aim, we compare \mathcal{W}_{Ψ_4} with a project-based witness operator of the form:

$$\mathcal{W}_{\Psi}^p = \alpha_{\Psi}^p \mathbf{1} - |\Psi\rangle \langle \Psi|, \quad (2.98)$$

where $\alpha_{\Psi}^p = 1/d$ [70]. If measured outcomes show that $\text{Tr}(\mathcal{W}_{\Psi}^p \rho) < 0$, the state ρ is identified as an entanglement close to $|\Psi\rangle$. Then one has to show if ρ satisfies $\text{Tr}(\mathcal{W}_{\Psi_4}\rho) < 0$, it also satisfies $\text{Tr}(\mathcal{W}_{\Psi}^p \rho) < 0$, i.e., $\mathcal{W}_{\Psi_4} - \gamma_{\Psi_4} \mathcal{W}_{\Psi}^p \geq 0$ where γ_{Ψ_4} is some positive constant. Let us consider the operator $W = \mathcal{W}_{\Psi_4} - d\gamma_d/(d-1)\mathcal{W}_{\Psi}^p$. To diagonalize W , we propose a complete basis $\{|\Psi_{kv}\rangle\}$, where

$$|\Psi_{kv}\rangle = \frac{1}{\sqrt{d}} \sum_{v'=0}^{d-1} \exp(i2\pi kv'/d) |v'\rangle \otimes |v'+v\rangle, \quad (2.99)$$

for $k, v = 0, 1, \dots, d-1$, where the addition of v' and v is modulo d . Since both of \mathcal{W}_{Ψ_4} and \mathcal{W}_{Ψ}^p are diagonal in this basis, W is also diagonal. The diagonal elements of W in

this basis can be calculated analytically, and then we have

$$\langle \Psi_{kv} | W | \Psi_{kv} \rangle = \frac{d}{d-1} \gamma_d, \quad (2.100)$$

for $k \geq 1$ and $v \geq 1$, and $\langle \Psi_{kv} | W | \Psi_{kv} \rangle = 0$ otherwise. This proves our claim.

Entangled state comprised of subsystems with different dimensions

We proceed to give another witness to detect an entangled state composed of a qutrit and a ququat (quantum four-level system) of the state vector:

$$|\epsilon\rangle = \frac{1}{\sqrt{3}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle + |2\rangle \otimes |3\rangle). \quad (2.101)$$

where the kets on the left-hand side of tensor products denote single qutrits and form an orthonormal basis: $\{|0\rangle, |1\rangle, |2\rangle\}$, and the kets on the right-hand side of tensor products are ququants described by an orthonormal basis $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. When $|\epsilon\rangle$ is in the above representation, one can easily derive two sets of correlator operators to describe correlations from the knowledge of the state vector:

$$\begin{aligned} \hat{C}_0^{(1)} &= (\hat{0} - \hat{1})\hat{0}, \hat{C}_1^{(1)} = (\hat{1} - \hat{2})\hat{1}, \hat{C}_2^{(1)} = (\hat{2} - \hat{0})\hat{3}, \\ \hat{C}_0^{(2)} &= (\hat{0} - \hat{2})\hat{0}, \hat{C}_1^{(2)} = (\hat{1} - \hat{0})\hat{1}, \hat{C}_2^{(2)} = (\hat{2} - \hat{1})\hat{3}. \end{aligned} \quad (2.102)$$

Each correlator proposed above is $\langle \hat{C}_k^{(q)} \rangle = 1/3$. Similarly, by the knowledge of the state vector given by

$$|\epsilon\rangle = \frac{1}{\sqrt{3}}(|0\rangle_F \otimes |0'\rangle_F + |1\rangle_F \otimes |1'\rangle_F + |2\rangle_F \otimes |2'\rangle_F), \quad (2.103)$$

where

$$\begin{aligned}
 |0'\rangle_F &= \frac{1}{2\sqrt{3}}(3|0\rangle_F + |1\rangle_F - |2\rangle_F + |3\rangle_F), \\
 |1'\rangle_F &= \frac{1}{6}[(-3 + \sqrt{3})|1\rangle_F + 2\sqrt{3}|2\rangle_F + (3 + \sqrt{3})|3\rangle_F], \\
 |2'\rangle_F &= \frac{1}{6}[(3 + \sqrt{3})|1\rangle_F + 2\sqrt{3}|2\rangle_F + (-3 + \sqrt{3})|3\rangle_F],
 \end{aligned} \tag{2.104}$$

and $|v\rangle_F$ are defined by Eq. (2.50), we give the second type of correlator operators:

$$\begin{aligned}
 \hat{C}_{0F}^{(1)} &= (\hat{0} - \hat{1})\hat{0}', \hat{C}_{1F}^{(1)} = (\hat{1} - \hat{2})\hat{1}', \hat{C}_{2F}^{(1)} = (\hat{2} - \hat{0})\hat{2}', \\
 \hat{C}_{0F}^{(2)} &= (\hat{0} - \hat{2})\hat{0}', \hat{C}_{1F}^{(2)} = (\hat{1} - \hat{0})\hat{1}', \hat{C}_{2F}^{(2)} = (\hat{2} - \hat{1})\hat{2}'.
 \end{aligned} \tag{2.105}$$

Each correlator is $\langle \hat{C}_{kF}^{(q)} \rangle = 1/3$. Therefore, our witness consists of all of the correlator operators introduced above is

$$\mathcal{W}_\epsilon = \alpha_\epsilon \mathbf{1} - \hat{C}_\epsilon, \tag{2.106}$$

where $\alpha_\epsilon = 2$ and $\hat{C}_\epsilon = \sum_{q,k} \hat{C}_k^{(q)} + \hat{C}_{kF}^{(q)}$.

We proceed to prove the operator \mathcal{W}_ϵ is a witness. To attain this aim, we have to compare \mathcal{W}_ϵ with the following projector-based witness

$$\mathcal{W}_\epsilon^p = \alpha_\epsilon^p \mathbf{1} - |\epsilon\rangle\langle\epsilon|, \tag{2.107}$$

where $\alpha_\epsilon^p = 1/3$ [70]. With the whole knowledge of $|\epsilon\rangle$, the witness \mathcal{W}_ϵ^p can be used to identify a state ρ as the one close to $|\epsilon\rangle$ if $\text{Tr}(\mathcal{W}_\epsilon^p \rho) < 0$. We find that $\mathcal{W}_\epsilon - 3\mathcal{W}_\epsilon^p \geq 0$ and from which we deduce that if $\text{Tr}(\mathcal{W}_\epsilon \rho) < 0$ then $\text{Tr}(\mathcal{W}_\epsilon^p \rho) < 0$ also applies to ρ . Thus \mathcal{W}_ϵ is an entanglement witness operator. In addition, \mathcal{W}_ϵ is very robust against noise. When a pure state $|\epsilon\rangle$ is suffered from white noise, the mixed state is identified as entanglement if the noise fraction is less than 0.5.

Four-qubit GHZ state shared by two parties

In the previous cases of entanglement detections for qubits, each party of a system has access to perform measurements on only one qubit. It is natural to ask how to design a strategy of detections of genuine multipartite entanglement if each party has access to measure more than one qubits in a Bell-type experiment. For instance, how to construct an entanglement witness operator for detecting a four-qubit GHZ state which is shared by two parties? Since more information about nonlocal properties of the GHZ state can be acquired via measurements, it is interesting to investigate the difference between the new witness and the previous one.

We will present a witness which requires only two local measurements to attain the aim mentioned above. First, let us assume two individual pairs of qubits of a four-qubit GHZ state are shared by two parties respectively, and then each party can perform two-qubit measurements on the qubits. For the first measurement setting, we use the correlator operators introduced in the third specification for the generalized GHZ state: $\hat{C}_{0Z[\mathbf{m},\bar{\mathbf{m}}]}$ and $\hat{C}_{1Z[\mathbf{m},\bar{\mathbf{m}}]}$, i.e.,

$$\hat{C}_{0Z[\mathbf{m},\bar{\mathbf{m}}]} = (\hat{0}\hat{0} - \hat{1}\hat{1})\hat{0}\hat{0}, \hat{C}_{1Z[\mathbf{m},\bar{\mathbf{m}}]} = (\hat{1}\hat{1} - \hat{0}\hat{0})\hat{1}\hat{1}. \quad (2.108)$$

A four-qubit GHZ state of the form

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle \otimes |00\rangle + |11\rangle \otimes |11\rangle),$$

gives $\langle \hat{C}_{0Z[\mathbf{m},\bar{\mathbf{m}}]} \rangle = \langle \hat{C}_{1Z[\mathbf{m},\bar{\mathbf{m}}]} \rangle = 1/2$. For the second measurement setting, we propose the operators

$$\hat{C}_{0F[\mathbf{m},\bar{\mathbf{m}}]} = (\mathbf{0}_{\mathbf{m}F} - \mathbf{1}_{\mathbf{m}F})\mathbf{0}_{\bar{\mathbf{m}}F}, \hat{C}_{1F[\mathbf{m},\bar{\mathbf{m}}]} = (\mathbf{1}_{\mathbf{m}F} - \mathbf{0}_{\mathbf{m}F})\mathbf{1}_{\bar{\mathbf{m}}F}. \quad (2.109)$$

where

$$\begin{aligned}
 \mathbf{0}_{\mathbf{m}(\bar{\mathbf{m}})F} &= \frac{1}{2}(|00\rangle_F + |10\rangle_F)(\langle 00|_F + \langle 10|_F), \\
 \mathbf{1}_{\mathbf{m}(\bar{\mathbf{m}})F} &= \frac{1}{2}(|01\rangle_F + |11\rangle_F)(\langle 01|_F + \langle 11|_F), \\
 |vv'\rangle_F &= \frac{1}{2} \sum_{k,k'=0}^1 \exp[-i\frac{2\pi n_{vv'}}{4}(2k+k')] |kk'\rangle,
 \end{aligned} \tag{2.110}$$

$n_{00} = 0$, $n_{01} = 1$, $n_{10} = 3$, and $n_{11} = 2$. The correlators are $\langle \hat{C}_{0F[\mathbf{m},\bar{\mathbf{m}}]} \rangle = \langle \hat{C}_{1F[\mathbf{m},\bar{\mathbf{m}}]} \rangle = 1/2$.

Thus our witness is

$$\mathcal{W}_{\Phi_2} = \mathbf{1} - \sum_{k=0}^1 \hat{C}_{kZ[\mathbf{m},\bar{\mathbf{m}}]} + \hat{C}_{kF[\mathbf{m},\bar{\mathbf{m}}]}. \tag{2.111}$$

Since a comparison between \mathcal{W}_{Φ_2} and the projector-based witness \mathcal{W}_{Φ}^p satisfies $\mathcal{W}_{\Phi_2} - 2\mathcal{W}_{\Phi}^p \geq 0$, \mathcal{W}_{Φ_2} is a witness for detecting truly four-qubit entanglement for states close to $|\Phi\rangle$.

The witness \mathcal{W}_{Φ_2} is very robust against noise. The noise tolerance of \mathcal{W}_{Φ_2} is $\delta_{\Phi_2} = 1/2$, and then \mathcal{W}_{Φ_2} is more robust than the witness \mathcal{W}_{Φ} , Eq. (2.82), with $\delta_{\Phi} = 4/11 \simeq 0.3636$. In other word, \mathcal{W}_{Φ_2} based on two-qubit measurements for each party can detect more states in the proximity of $|\Phi\rangle$ and is finer than \mathcal{W}_{Φ} .

Let us consider the above example in another way. We define each pair of qubits as a single *ququat*, and then the four-qubit GHZ state can be represented by

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |3\rangle \otimes |3\rangle),$$

where $|2v+v'\rangle = |vv'\rangle$ for $v, v' = 0, 1$. Therefore constructions of correlator operators for a four-qubit GHZ state is equivalent to the ones for a two-ququat entangled sate of the above form, and then one can observe that each vector in the orthonormal basis $\{|vv'\rangle_F\}$ chosen in the second measurement setting is derived from a vector in the basis $\{|2v+v'\rangle\}$ which is transferred by a single-ququat Fourier transformation. In this situation, further

two questions arise. What are the constructions of correlator operators for a N -ququat entangled state of the form: $|\Phi\rangle = (|0\rangle^{\otimes N} + |3\rangle^{\otimes N})/\sqrt{2}$? Are the witnesses based on correlators finer than \mathcal{W}_Φ ? The investigations on these questions are the future works.

We proceed to consider another situation where one party has three qubits and another party has the rest of a four-qubit GHZ state. First, we follow the method just discussed and substitute eight-level state vector $|4v + 2v' + v''\rangle$ for three-qubit one $|vv'v''\rangle$ to express $|\Phi\rangle$ as

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |7\rangle),$$

where the kets on the left-hand side of the tensor products in the above equation denote single qubits and constitute an orthonormal basis $\{|0\rangle, |1\rangle\}$, whereas the right-hand ones are three-qubit elements of the orthonormal basis $\{|0\rangle, |1\rangle, \dots, |7\rangle\}$. Then we give the following correlator operators for states shown in this representation:

$$\hat{C}_0 = (\hat{0} - \hat{1})\hat{0}, \hat{C}_1 = (\hat{1} - \hat{0})\hat{7}, \quad (2.112)$$

and the correlators are $\langle \hat{C}_0 \rangle = \langle \hat{C}_1 \rangle = 1/2$. When $|\Phi\rangle$ is of another form:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{F_2} \otimes |0'\rangle_{F_8} + |1\rangle_{F_2} \otimes |1'\rangle_{F_8}),$$

where

$$\begin{aligned} |v\rangle_{F_2} &= \frac{1}{\sqrt{2}}[|0\rangle + (-1)^v |1\rangle], \\ |0'\rangle_{F_8} &= \sum_{k=0}^7 c_{k0} |k\rangle_{F_8}, |1'\rangle_{F_8} = \sum_{k=0}^7 c_{k1} |k\rangle_{F_8}, \\ |k\rangle_{F_8} &= \frac{1}{\sqrt{8}} \sum_{k'=0}^7 \exp(-i\frac{2\pi k}{d}k') |k'\rangle, \end{aligned} \quad (2.113)$$

c_{k0} and c_{k1} are complex numbers, and ${}_{F_8}\langle 1'|0'\rangle_{F_8} = 0$, another set of operators can be

easily derived from the knowledge of the state vector and are given by

$$\hat{C}_{0F} = (\hat{0} - \hat{1})\hat{0}', \hat{C}_{1F} = (\hat{1} - \hat{0})\hat{1}'. \quad (2.114)$$

Then our witness is

$$\mathcal{W}_{\Phi_3} = \mathbf{1} - \sum_{k=0}^1 \hat{C}_k + \hat{C}_{kF}, \quad (2.115)$$

and fulfills the condition $\mathcal{W}_{\Phi_3} - 2\mathcal{W}_{\Phi}^P \geq 0$ for detecting truly four-qubit entanglement.

The noise tolerance of \mathcal{W}_{Φ_3} is $\delta_{\Phi_3} = 1/2$ and is also superior to the one of \mathcal{W}_{Φ} .

2.5.4 Witnesses composed of the kernels of Bell inequalities for qudits

In Sec. 2.4, we have shown that the kernels of different kinds of Bell inequalities for qudits are composed of correlators which associate with necessary conditions of entangled qudits. This fact motivates us to construct entanglement witnesses comprised of the kernels to detect states close to a generalized Bell state. The constructions proposed provide a connection between entanglement witnesses and Bell inequalities.

We introduce the witness operators

$$\mathcal{W}_{\Psi_q} = \alpha_{\Psi_q} \mathbf{1} - \hat{C}_{\Psi_q}^{(d)}, \quad (2.116)$$

for $q = 1, 2, 3$, where α_{Ψ_q} are some constants and $\hat{C}_{\Psi_q}^{(d)}$ are combinations of correlators proposed in the previous section. A state is identified as an entanglement in the proximity of $|\Psi\rangle$ if the corresponding expectation value of \mathcal{W}_{Ψ_q} is negative. Although $\hat{C}_{\Psi_3}^{(d)}$ is not a kernel of Bell inequalities, we shows its utility for entanglement detection and compare it with the other ones. In addition, we also give a variant of \mathcal{W}_{Ψ_2} denoted by $\mathcal{W}_{\Psi_2:f(\alpha)=1}$. The subscript $f(\alpha) = 1$ of $\mathcal{W}_{\Psi_2:f(\alpha)=1}$ indicates that the function $f(\alpha)$ in Eq. (2.64) is

Table 2.1: Summaries of α_{Ψ_q} for \mathcal{W}_{Ψ_q} and the parameters γ_{Ψ_q} , which are utilized to prove \mathcal{W}_{Ψ_q} are witness operators.

| d | 3 | 4 | 5 | 6 |
|-------------------------------|-------|-------|-------|-------|
| α_{Ψ_1} | 1.755 | 2.047 | 2.216 | 2.328 |
| α_{Ψ_2} | 1.755 | 1.954 | 2.093 | 2.199 |
| $\alpha_{\Psi_2:f(\alpha)=1}$ | 1.755 | 2.080 | 2.095 | 2.255 |
| α_{Ψ_3} | 2.668 | 2.250 | 3.200 | 4.167 |
| γ_{Ψ_1} | 1.802 | 1.18 | 0.90 | 0.72 |
| γ_{Ψ_2} | 1.802 | 1.43 | 1.24 | 1.11 |
| $\gamma_{\Psi_2:f(\alpha)=1}$ | 1.802 | 2.18 | 1.83 | 2.11 |
| γ_{Ψ_3} | 1 | 1 | 1 | 1 |

set one, whereas \mathcal{W}_{Ψ_2} uses the one for the CGLMP inequalities. However, $\mathcal{W}_{\Psi_2:f(\alpha)=1}$ are not Bell inequalities. For proofs of \mathcal{W}_{Ψ_q} , we use the same method as the ones in the previous proofs to show the operators proposed are witnesses. The parameters for proving $\mathcal{W}_{\Psi_q} - \gamma_{\Psi_q} \mathcal{W}_{\Psi}^p > 0$ and α_{Ψ_q} are given in Table 2.1.

We compare the witnesses proposed according to their robustness against noise and summarize the corresponding noise tolerances $\delta_{\text{noise}} = \delta_{\Psi_q}$ in Table 2.2. The table also includes noise tolerance for projector-based witness \mathcal{W}_{Ψ}^p and \mathcal{W}_{Ψ_4} . For witnesses composed of Bell kernels, the witness \mathcal{W}_{Ψ_2} is more robust than \mathcal{W}_{Ψ_1} . For all witnesses considered, \mathcal{W}_{Ψ}^p is the most robust, and its noise tolerance goes one for large dimension of the generalized Bell state. When focusing on the constrain $\langle \mathcal{W}_{\Psi}^p \rangle < 0$ for a state of the form as Eq. (2.97), one can obtain $\delta_{\Psi}^p = d/(d+1)$ for maintaining entangled qudits, which proves the above statement. The superiority of \mathcal{W}_{Ψ}^p relies on the whole knowledge of $|\Psi\rangle$ used in the witness. However, in order to realize \mathcal{W}_{Ψ}^p in Bell-type experiments, \mathcal{W}_{Ψ}^p should be decomposed into sets of observable that can be measured locally. To our knowledge, a general method for decomposition of \mathcal{W}_{Ψ}^p is still lacking. For the purpose of performing detections with fewer settings, \mathcal{W}_{Ψ_4} possesses a highly tolerance to noise for detecting $|\Psi\rangle$ and is better than the other ones.

Table 2.2: Summaries of the noise tolerance δ_{Ψ_q} and δ_{Ψ}^p involved in robustness of the entanglement witness operators \mathcal{W}_{Ψ_q} and \mathcal{W}_{Ψ}^p respectively.

| d | 3 | 4 | 5 | 6 |
|-------------------------------|-------|-------|-------|-------|
| δ_{Ψ_1} | 0.389 | 0.289 | 0.231 | 0.192 |
| δ_{Ψ_2} | 0.389 | 0.326 | 0.281 | 0.247 |
| $\delta_{\Psi_2:f(\alpha)=1}$ | 0.389 | 0.290 | 0.287 | 0.236 |
| δ_{Ψ_3} | 0.333 | 0.250 | 0.200 | 0.167 |
| δ_{Ψ_4} | 0.500 | 0.500 | 0.500 | 0.500 |
| δ_{Ψ}^p | 0.750 | 0.800 | 0.833 | 0.857 |

2.6 Conclusion

In summary, we introduce criteria of quantum correlations for many-qubit and two-qudit entanglement. We show five known Bell inequalities for many qubits [13–15] and two qudits [17, 18] and the general correlation functions for qudits [109] are composed of the correlation conditions proposed. By correlators, two sets of Bell inequalities for bipartite multi-level systems which requires fewer analyses of measured outcomes are also introduced. In addition, we reveal the inequalities based on the geometry of spin vector [110] are comprised of correlators. Through the conditions, we give entanglement witness operators for detecting truly many-qubit GHZ states and the first robust witness for detecting a two-qudit Bell state. A robust witness for detecting entangled qudits composed of two particles with unequal dimensions is proposed. We also give a robust witness for detecting a four-qubit GHZ state which is shared by two parties. These witnesses require only two local measurement settings when used in experiments. The kernels of Bell inequalities are also used as witness operators for qudits, which exhibits connections between Bell inequalities and entanglement witnesses.

Our formulations reveal N -point correlation functions for qubits are the sum of sets of correlators. These correlators provide information about correlations between any two subsystems of N qubits, and the conditions involved could help to investigate the stabilizer formalism [117] in a novel way, which will be discussed elsewhere. For entangled qudits, especially, the strategy introduced provides a systematic way to analyze the correlation

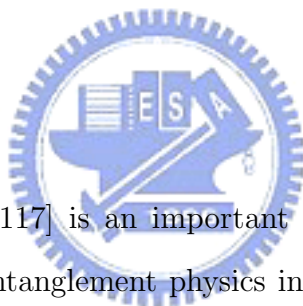
structure of measured outcomes in different physical systems [118] and then can be utilized directly for present experiments [20–23].



Chapter 3

Correlation conditions in the stabilizer formalism

3.1 Introduction



The stabilizer formalism [3, 117] is an important method for studying the operations in quantum mechanics and entanglement physics including entanglement detections [72] and Bell inequalities [119, 120]. In what follows, instead of deriving correlators from the state vector of an entangled state, we determine the correlation conditions imbedded in a set of operators which is called *stabilizer* [117]. We will show that the correlators introduced give us a new insight into stabilizers of stabilizer states, and the correlator embedded in the stabilizer can be considered as a special class of the general ones. For a given stabilizer of some stabilizer state, we can consider the stabilizer as a specification of multipartite correlations between qubits, and furthermore via the proposed conditions of correlations we can realize that the qubits are dependent on each other under different measurement settings. Most importantly, correlations shown in different directions are the manifestation of quantum entanglement. Thus one can describe the necessary characters of quantum correlations concretely by the correlators in the stabilizers for the stabilizer states.

3.2 Stabilizer formalism

When using the stabilizer formalism to specify a quantum state $|\phi\rangle$, the state is described by a set of operators that have the eigenstate $|\phi\rangle$ with the eigenvalue 1. This set of operators is called the *stabilizer* which stabilize $|\phi\rangle$. Then $|\phi\rangle$ is called the stabilizer state. For example, a N -qubit cluster state $|L_N\rangle$ [31] is stabilized by the group of stabilizer given by

$$G_{L_N} = \langle S_{1,L_N}, S_{2,L_N}, \dots, S_{N,L_N} \rangle, \quad (3.1)$$

where

$$S_{1,L_N} = X_1 Z_2, S_{N,L_N} = Z_{N-1} X_N, S_{k,L_N} = Z_{k-1} X_k Z_{k+1} \quad (3.2)$$

for $k = 2, 3, \dots, N - 1$, are the generators of the group.

Theorem 3. For some stabilizer state $|\phi\rangle$, every operator $g_\phi \in G_\phi$ with the general form, $g_\phi = \pm \bigotimes_{k=1}^m \widehat{V}_k$, where $\widehat{V}_k \in \{Z, X, Y\}$, can be specified by the correlator operators:

$$g_\phi = \widehat{C}_{0\phi} + \widehat{C}_{1\phi}, \quad (3.3)$$

with

$$\langle \widehat{C}_{0\phi} \rangle > 0 \text{ and } \langle \widehat{C}_{1\phi} \rangle > 0, \quad (3.4)$$

for $|\phi\rangle$, which implies that some subsystem of n qubits for $n < m$ is dependent on the one composed of $(m - n)$ qubits [121].

Proof. The Pauli operator \widehat{V}_k can be expressed explicitly by $\widehat{V}_k = \sum_{v_k=0}^1 (-1)^{v_k} \widehat{v}_{kk'}$ for $k' \in \{x, y, z\}$ which denote the type of Pauli operator where $\widehat{v}_{kk'} = |v_k\rangle_{k'} \langle v_k|$ and k is used to number the qubits. Then, we have $\bigotimes_{k=n'+1}^n \widehat{V}_k = \widehat{\mathbf{0}}_{(n-n')} - \widehat{\mathbf{1}}_{(n-n')}$, where

$\hat{\mathbf{0}}_{(n-n')}$ ($\hat{\mathbf{1}}_{(n-n')}$) is the sum of all $(n - n')$ -qubit operators, $\otimes_{k=n'+1}^n \hat{v}_{kk'}$, with even (odd) $\sum_{k=n'+1}^n v_k$. With the substitution given above, $g_\phi = \otimes_{k=1}^m \hat{V}_k$ can be expressed by

$$\begin{aligned} g_\phi &= \bigotimes_{k=1}^n \hat{V}_k \bigotimes_{k=n+1}^m \hat{V}_k \\ &= (\hat{\mathbf{0}}_n - \hat{\mathbf{1}}_n)(\hat{\mathbf{0}}_{(m-n)} - \hat{\mathbf{1}}_{(m-n)}) \\ &= (\hat{\mathbf{0}}_n - \hat{\mathbf{1}}_n)\hat{\mathbf{0}}_{(m-n)} + (\hat{\mathbf{1}}_n - \hat{\mathbf{0}}_n)\hat{\mathbf{1}}_{(m-n)}, \end{aligned} \quad (3.5)$$

and for $g_\phi = -\otimes_{k=1}^m \hat{V}_k$ we have

$$g_\phi = (\hat{\mathbf{0}}_n - \hat{\mathbf{1}}_n)\hat{\mathbf{1}}_{(m-n)} + (\hat{\mathbf{1}}_n - \hat{\mathbf{0}}_n)\hat{\mathbf{0}}_{(m-n)}. \quad (3.6)$$

For $g_\phi = \otimes_{k=1}^m \hat{V}_k$, since

$$\left\langle \sum_{\mathbf{v}, \mathbf{v}'=\mathbf{0}}^{\mathbf{1}} (-1)^{\mathbf{v}+\mathbf{v}'} \hat{v}_n \hat{v}'_{(m-n)} \right\rangle = \left\langle \sum_{\mathbf{v}, \mathbf{v}'=\mathbf{0}}^{\mathbf{1}} \hat{v}_n \hat{v}'_{(m-n)} \right\rangle = 1,$$

for $|\phi\rangle$, it turns out that $\langle \hat{\mathbf{1}}_n \hat{\mathbf{0}}_{(m-n)} + \hat{\mathbf{0}}_n \hat{\mathbf{1}}_{(m-n)} \rangle = 0$ and $\langle \hat{\mathbf{0}}_n \hat{\mathbf{0}}_{(m-n)} + \hat{\mathbf{1}}_n \hat{\mathbf{1}}_{(m-n)} \rangle = 1$ for all $n < m$. If $|\phi\rangle$ is not a product state, we have $\text{Tr}(|\phi\rangle \langle \phi| \hat{v}_n \hat{v}_{(m-n)}) > 0$ for $\mathbf{v} = \mathbf{0}, \mathbf{1}$ and deduce that the correlators for the operator

$$\hat{C}_{0\phi} = (\hat{\mathbf{0}}_n - \hat{\mathbf{1}}_n)\hat{\mathbf{0}}_{(m-n)}, \hat{C}_{1,\phi} = (\hat{\mathbf{1}}_n - \hat{\mathbf{0}}_n)\hat{\mathbf{1}}_{(m-n)}. \quad (3.7)$$

are all positive for $|\phi\rangle$. For $g_\phi = -\otimes_{k=1}^m V_k$, by the same approach proposed above, we have positive values of correlators corresponding to the operators

$$\hat{C}_{0\phi} = (\hat{\mathbf{0}}_n - \hat{\mathbf{1}}_n)\hat{\mathbf{1}}_{(m-n)}, \hat{C}_{1,\phi} = (\hat{\mathbf{1}}_n - \hat{\mathbf{0}}_n)\hat{\mathbf{0}}_{(m-n)}. \quad (3.8)$$

Hence, we know that the subsystem of n qubits is dependent on the one composed of $(m - n)$ qubits by the first theorem given in Sec. 2.2. \square

Given a m -qubit operator belonging to some stabilizer with the form like the one in

the third theorem, it specifies the dependence characters between any two subsystems with k qubits and $(m - k)$ ones. Each operator g_ϕ gives n_ϕ sets of correlators where

$$n_\phi = \sum_{k=1}^{\lfloor m/2 \rfloor} f(m, k) \frac{m!}{k!(m-k)!}, \quad (3.9)$$

$f(m, k) = 2^{-\delta[k, \lfloor m/2 \rfloor]}$ for even m and $f(m, k) = 1$ for odd one. The number n_ϕ has the same form as the one of Eq. (2.8) for n_c . Therefore, we can express g_ϕ as:

$$g_\phi = \frac{1}{n_\phi} \sum_{k=1}^{\lfloor m/2 \rfloor} \sum_{i=1}^{\alpha_{mk}} \hat{C}_{0\phi, ki} + \hat{C}_{1\phi, ki} \quad (3.10)$$

where $\alpha_{mk} = f(m, k)m!/k!(m-k)!$ and $(\hat{C}_{0\phi, ki}, \hat{C}_{1\phi, ki})$ denote the i th pair which belongs to the sets of correlator operators for specifying the correlation of dependence between any two subsystems with k qubits and $(m - k)$ ones respectively.

Through the third theorem, we could view the group of stabilizer as the set which contains all correlators for specifying the dependence between qubits of the N -qubit system under different measurement directions. In what follows, we will discuss the correlators derived from the stabilizer under a given measurement setting.

(a) Cluster state. First, let us consider a concrete example involved the following generators of the six-qubit cluster state: $S_{1,L_6} = X_1Z_2$, $S_{3,L_6} = Z_2X_3Z_4$, and $S_{5,L_6} = Z_4X_5Z_6$. S_{1,L_6} shows that the first qubit is dependent of the second one. S_{3,L_6} identifies the correlations: $[2|3, 4]$, $[3|2, 4]$, and $[4|2, 3]$, and S_{5,L_6} identifies the ones: $[4|5, 6]$, $[5|4, 6]$, and $[6|4, 5]$. We know that the six-qubit system possesses the multipartite correlation by these information featured in correlators. However, when measuring qubits under the setting where the odd (even)-number qubits are measured along x (z) direction, the correlation conditions given by the generators S_{1,L_6} , S_{3,L_6} , and S_{5,L_6} are incomplete. From an observation, we know that the measured directions involved in the products of the generators are the same as the ones of the generators, and we could acquire more criteria of correlations from these products of generators. For instance, $S_{1,L_6}S_{3,L_6} = X_1X_3Z_4$ let

us know the condition for $\{[1, 3, 4]\}$, $S_{1,L_6}S_{5,L_6} = X_1Z_2Z_4X_5Z_6$ for $\{[1, 2, 4, 5, 6]\}$, and $S_{3,L_6}S_{5,L_6} = Z_2X_3X_5Z_6$ for $\{[2, 3, 5, 6]\}$. Hence a complete condition of correlations can be provided from the subgroup of the stabilizer generated by S_{1,L_6} , S_{3,L_6} , and S_{5,L_6} : $G_{L_6,1} = \langle S_{1,L_6}, S_{3,L_6}, S_{5,L_6} \rangle$, if disregarding the identify operator, i.e.,

$$\tilde{G}_{L_6,1} = \{X_1X_3Z_4, X_1Z_2Z_4X_5Z_6, Z_2X_3X_5Z_6, X_1X_3X_5Z_6, X_1Z_2, Z_2X_3Z_4, Z_4X_5Z_6\}. \quad (3.11)$$

Similarly, under another measurement setting where the odd (even)-number qubits are measured along z (x) direction, the set of operators

$$\tilde{G}_{L_6,2} = \{Z_1X_2Z_3Z_5X_6, Z_3X_4X_6, Z_1X_2X_4X_6, Z_1X_2X_4Z_5, Z_5X_6, Z_1X_2Z_3, Z_3X_4Z_5\}, \quad (3.12)$$

generated by $S_{2,L_6} = Z_1X_2Z_3$, $S_{4,L_6} = Z_3X_4Z_5$, $S_{6,L_6} = Z_5X_6$, also gives an identification of multipartite correlation of $|L_6\rangle$. Furthermore, for the N -qubit cluster state, both the subgroups $G_{L_N,1} = \langle S_{k,L_N} : \text{for all odd } k \rangle$ and $G_{L_N,2} = \langle S_{k,L_N} : \text{for all even } k \rangle$ give complete descriptions of N -qubit correlation of $|\phi_d\rangle$ by $\tilde{G}_{L_N,1}$ and $\tilde{G}_{L_N,2}$, under two different measurement settings.

(b) Greenberger-Horne-Zeilinger (GHZ) state [113]. An N -qubit GHZ state is specified by the stabilizer

$$G_{\text{GHZ}_N} = \langle S_{1,\text{GHZ}_N}, S_{k,\text{GHZ}_N} : \text{for } k = 2, \dots, N \rangle, \quad (3.13)$$

where

$$S_{1,\text{GHZ}_N} = \bigotimes_{k=1}^N X_k, S_{k,\text{GHZ}_N} = Z_{k-1}Z_k, \quad (3.14)$$

for $k = 2, \dots, N$. Let us discuss S_{1,GHZ_N} first. By Theorem 3 and the related discussions, we know that there are n_{GHZ_N} sets of correlators to describe the correlations between subsystems with $\{[1, 2, \dots, N]\}$, where n_{GHZ_N} is defined by Eq. (3.10). The feature of truly

multipartite correlation is shown via these correlators under the x -direction measurements. On the other hand, the operators g_{GHZ_N} produced by generators S_{k,GHZ_N} for $k \geq 2$ specify two kinds of criterion of correlation including the dependence between *each qubit*, $[i, j]$, and the correlations between subsystems with $\{[1, 2, \dots, m]\}$ where m is even. To investigate the correlation between the k_1 th and k_2 th qubits for $k_2 > k_1$, we can utilize the product of the generators, $\prod_{k_1+1}^{k_2-1} S_{k,\text{GHZ}_N}$, to have the operator $Z_{k_1}Z_{k_2}$ and know that these qubits are dependent. For the second type of criterion, it is given by $\bigotimes_{k \in T_e} Z_k$ where T_e denotes the set which contains even number of qubits. For example, we have the same correlators as S_{1,GHZ_N} by $\prod_{k=1}^{N/2} S_{2k,\text{GHZ}_N} = \bigotimes_{k=1}^N Z_k$ where N is even. Thus, under two local measurement settings, a complete knowledge of correlation between qubits is included in $\tilde{G}_{\text{GHZ}_N,1} = \{S_{1,\text{GHZ}_N}\}$ and the set of operators $\tilde{G}_{\text{GHZ}_N,2}$ that is derived from the subgroup of stabilizer, $G_{\text{GHZ}_N,2} = \langle S_{k,\text{GHZ}_N} : \text{for } k = 2, \dots, N \rangle$, and in which the identity operator is disregarded.

(c) Graph state. A N -qubit graph state [122], $|R_N\rangle$, is specified by a graph described in terms of N vertices and some edges connecting them and is defined explicitly by the stabilizing operators:

$$S_{k,R_N} |R_N\rangle = |R_N\rangle, \quad (3.15)$$

where

$$S_{k,R_N} = X_k \bigotimes_{i \in N_k} Z_i \quad (3.16)$$

and N_k denotes the set of vertices i for which vertices k and i are adjacent. Through Theorem 3, we realize that the vertex k is dependent on the ones in the neighborhood N_k . Furthermore, we can identify the correlation between two vertices that are not adjacent via the correlators. For instance, a four-qubit box-cluster state is specified by the following

stabilizing operators:

$$S_{1,R_4} = X_1 Z_2 Z_4, S_{2,R_4} = X_2 Z_1 Z_3, S_{3,R_4} = X_3 Z_2 Z_4, S_{4,R_4} = X_4 Z_1 Z_3. \quad (3.17)$$

Although the first qubit and the third one are not adjacent, we can identify that they are dependent via $S_{1,R_4} S_{3,R_4} = X_1 X_3$. Similarly, the second qubit and the fourth one are correlated by $S_{2,R_4} S_{4,R_4} = X_2 X_4$. Therefore, the sets

$$\tilde{G}_{R_4,1} = \{X_1 Z_2 Z_4, X_3 Z_2 Z_4, X_1 X_3\}, \tilde{G}_{R_4,2} = \{X_2 Z_1 Z_3, X_4 Z_1 Z_3, X_2 X_4\}, \quad (3.18)$$

can describe the correlation inherent in the state $|R_N\rangle$ under two different measurement settings.

3.3 Entanglement witnesses for stabilizer states

When designing a witness operator to detect some multi-qubit entangled state without using the whole knowledge of which, it is crucial to feature the key characters of multi-party correlation imbedded in the entanglement. The proposed approach for correlators attains this aim. The sets of correlators can be considered as the *necessary conditions* of quantum correlations of entanglement imbedded in states to be generated. Thus, we can take a linear combination of the derived correlator operators that have been the identification of $|\phi\rangle$ to give a multi-qubit witness operator:

$$\mathcal{W}_\phi = \alpha_\phi \mathbf{1} - \hat{C}_\phi, \quad (3.19)$$

where

$$\hat{C}_\phi = \sum_k c_k (\hat{C}_{0\phi,k} + \hat{C}_{1\phi,k}), \quad (3.20)$$

Table 3.1: Kernels of entanglement witnesses. For $\phi : L_N$ and R_4 the sum of correlators $\hat{C}_{1(2)k}$ denotes the k^{th} stabilizing operators belonging to $\tilde{G}_{\phi,1(2)}$ with $(\gamma_{1(2)} - 1)$ elements, and $\gamma_{1(2)}$ is given by $\gamma_{1(2)} = 2^{n_{q1(2)}}$ where $n_{q1(2)}$ is the number of generators which create $\tilde{G}_{\phi,1(2)}$.

| W_ϕ | \hat{C}_ϕ | α_ϕ |
|--------------------|---|---|
| W_{L_N} | $\gamma_2 \sum_{k=1}^{\gamma_1-1} \hat{C}_{1k} + \gamma_1 \sum_{k=1}^{\gamma_2-1} \hat{C}_{2k}$ | $3\gamma_1\gamma_2/2 - \gamma_1 - \gamma_2$ |
| W_{GHZ_N} | $\gamma_2 \sum_{k=1}^{\gamma_1-1} \hat{C}_{1k} + \gamma_1 \sum_{k=1}^{\gamma_2-1} \hat{C}_{2k}$ | $3\gamma_1\gamma_2/2 - \gamma_1 - \gamma_2$ |
| W_{R_4} | $\gamma_2 \sum_{k=1}^{\gamma_1-1} \hat{C}_{1k} + \gamma_1 \sum_{k=1}^{\gamma_2-1} \hat{C}_{2k}$ | $3\gamma_1\gamma_2/2 - \gamma_1 - \gamma_2$ |

α_ϕ , and c_k 's are constants. If $\text{Tr}(\mathcal{W}_\phi \rho) < 0$, the state ρ is identified as a genuine multipartite entanglement. Therefore, making a utilization of the correlators for the multipartite entangled states proposed above, we construct the corresponding entanglement witnesses and detail the kernels in Table 3.1. Note that the witnesses for N -qubit GHZ states are of the same form as the one of the witnesses given in Sec. 2.5.1. The proofs of the entanglement witnesses are shown in Appendix B.

We remind that each stabilizing operator is composed of correlator operators with the structure as Eq. (3.7) or Eq. (3.8) and hence the witnesses for stabilizer states fit the general definition shown in Eq. (3.19). When comparing \mathcal{W}_{L_N} and $\mathcal{W}_{\text{GHZ}_N}$ with the ones of Ref. [72], they possess the same structures, which means that one can cast new light on the stabilizer entanglement witnesses [72] via the concrete and analytical conditions of correlations based on correlators.

3.4 Correlator-based Bell inequalities for many-qubit graph states

Combinations of partial or all operators in the stabilizer are central to entanglement detections. Very recently, Gühne *et al.* [119] derived a family of Bell inequalities for graph states. Since their method is general for different interesting graphs, the kernels of the proposed Bell inequalities are composed of $2^N - 1$ operators of the stabilizer (excluding the identity operator), and they show that each graph state there is an inequality maximally

CHAPTER 3. CORRELATION CONDITIONS IN THE STABILIZER FORMALISM

violated only by that state. Their results imply that combinations of all of the correlator operators could help to tell the nonlocal properties of the graph states from the classical correlations. In addition, since all operators that involves conditions for dependence in the stabilizer have been used, each particle requires three measurement settings. It is possible to utilize partial necessary conditions of correlation imbedded in graph states to construct Bell inequalities. For example, the subgroup of stabilizer of start and cycle subgraphs involved two local measurement settings for each particle can be utilized for Bell inequalities [120].



Chapter 4

Entanglement detection via the condition of quantum correlation

4.1 Method



In addition to detections of stabilizer states, the correlations proposed can also be utilized to detect states with non-local stabilizers. We use the correlator operators involved in the necessary condition of quantum correlation to construct entanglement witnesses for detecting genuine multi-partite entanglement about the generalized GHZ state with two local measurement settings, and three-qubit W states and four-qubit singlet states [123] with only three settings. More recently, it has been shown that four qubit singlet state is very useful for quantum secret sharing [45]. Through our method, 15 local measurement settings required for the entanglement witnesses by Ref. [70] can be reduced greatly. In what follows, we give a theorem based on the same concept as the one of Theorems 1 and 2 to detect the states mentioned above.

For a N -qubit system, the kernel of our strategy for identifying correlation between a specific subsystem, say A , and another one, say B , under some local measurement setting,

M_l , relies on the sets of correlators with the following forms:

$$\langle \widehat{C}_0^{(l)} \rangle = P(v_{A0}, v_{B0}) - P(v_{A1}, v_{B0}), \langle \widehat{C}_1^{(l)} \rangle = P(v_{A1}, v_{B1}) - P(v_{A0}, v_{B1}), \quad (4.1)$$

where $P(v_{Ai}, v_{Bj})$ is the joint probability for obtaining the measured outcomes v_{Ai} for the A subsystem and v_{Bj} for the B one. By the values of the correlators for an experimental output state, we could identify correlations between outcomes of measurements for the subsystems.

Theorem 4. If the results of measurements reveal that $\langle \widehat{C}_0^{(l)} \rangle$ and $\langle \widehat{C}_1^{(l)} \rangle$ are *all positive* or *all negative*, i.e., $\langle \widehat{C}_0^{(l)} \rangle \langle \widehat{C}_1^{(l)} \rangle > 0$, then the outcomes of measurements performed on the A subsystem are correlated with the ones performed on the B subsystem [73].

Proof. If the A subsystem is independent of the B one, we recast $P(v_{Ai}, v_{Bj})$ as $P(v_{Ai})P(v_{Bj})$, where $P(v_{Ai})$ and $P(v_{Bj})$ denote the marginal probabilities for obtaining results v_{Ai} and v_{Bj} respectively. Then, we have

$$C_{0,n}^{(l)} = [P(v_{A0}) - P(v_{A1})]P(v_{B0}), C_{1,n}^{(l)} = [P(v_{A1}) - P(v_{A0})]P(v_{A1}). \quad (4.2)$$

Since $P(v_{A1}), P(v_{B0}) \geq 0$, we conclude that $C_0^{(l)}C_1^{(l)} \leq 0$. Therefore, $C_0^{(l)}C_1^{(l)} > 0$ implies that the measured outcomes performed on the A subsystem are dependent with the one performed on the B subsystem. \square

4.2 Generalized GHZ states

We start showing the strategy with the help of Theorem 4 to derive correlation conditions for the generalized four-qubit GHZ state:

$$|\Phi(\theta, \phi)\rangle = \cos(\theta) |0000\rangle_z + e^{i\phi} \sin(\theta) |1111\rangle_z, \quad (4.3)$$

for $0 < \theta < \pi/4$ and $0 \leq \phi < \pi/2$, where $|v_1v_2v_3v_4\rangle_z = \otimes_{k=1}^4 |v\rangle_{kz}$ for $v \in \{0, 1\}$ and $|v\rangle_{kz}$ corresponds to an eigenstate of σ_z with eigenvalue $(-1)^v$ for the party k . Firstly, to

describe the correlation between *a specific party* and *others* of the four-qubit system, we give four sets of correlator operators:

$$\hat{C}_{0,nz}^{(z)} = (\hat{0}_{nz} - \hat{1}_{nz}) \otimes \hat{0}_{mz} \otimes \hat{0}_{pz} \otimes \hat{0}_{qz}, \hat{C}_{1,nz}^{(z)} = (\hat{1}_{nz} - \hat{0}_{nz}) \otimes \hat{1}_{mz} \otimes \hat{1}_{pz} \otimes \hat{1}_{qz}, \quad (4.4)$$

for $n = 1, \dots, 4$, where $\hat{v}_{nz} = |v\rangle_{nznz} \langle v|$ and n, m, p , and q denote four different parties under the local measurement setting, $M_{4z} = (Z, Z, Z, Z)$. In order to have compact forms, in what follows, symbols of tensor product will be omitted from correlator operators. Then, for some experimental output state, the expectation values of the Hermitian operators $\hat{C}_{0,n}^{(z)}$ and $\hat{C}_{1,n}^{(z)}$ are expressed in the following correlators in terms of joint probabilities:

$$\begin{aligned} \langle \hat{C}_{0,n}^{(z)} \rangle &= P(v_n = 0, \mathbf{v} = 0) - P(v_n = 1, \mathbf{v} = 0), \\ \langle \hat{C}_{1,n}^{(z)} \rangle &= P(v_n = 1, \mathbf{v} = 3) - P(v_n = 0, \mathbf{v} = 3), \end{aligned} \quad (4.5)$$

where $\mathbf{v} = \sum_{i=1, i \neq n}^4 v_i$. By Theorem 4, we know that if results of measurements reveal that $\langle \hat{C}_{0,n}^{(z)} \rangle \langle \hat{C}_{1,n}^{(z)} \rangle > 0$, the outcomes of measurements performed on the n th party are correlated with the ones performed on the rest. If the n th party is independent of the rest, we have

$$\begin{aligned} \langle \hat{C}_{0,n}^{(z)} \rangle &= [P(v_n = 0) - P(v_n = 1)]P(\mathbf{v} = 0), \\ \langle \hat{C}_{1,n}^{(z)} \rangle &= [P(v_n = 1) - P(v_n = 0)]P(\mathbf{v} = 3), \end{aligned}$$

and realize that $\langle \hat{C}_{0,n}^{(z)} \rangle \langle \hat{C}_{1,n}^{(z)} \rangle \leq 0$.

For a pure generalized four-qubit GHZ state, $|\Phi(\theta, \phi)\rangle$, we have

$$C_{0,n,\Phi(\theta,\phi)}^{(z)} = \cos^2(\theta), \quad C_{1,n,\Phi(\theta,\phi)}^{(z)} = \sin^2(\theta), \quad (4.6)$$

and hence $C_{0,n,\Phi(\theta,\phi)}^{(z)} C_{1,n,\Phi(\theta,\phi)}^{(z)} > 0$, which describes the outcomes of measurements are correlated. Then the condition, $C_{0,n}^{(z)} C_{1,n}^{(z)} > 0$, is a *necessary condition* of the pure generalized four-qubit GHZ state.

Further, we construct the following correlator operators to identify correlations between *a specific group*, which is composed of the n th and m th parties, and *another*:

$$\hat{C}_{0,nm}^{(z)} = (\hat{0}_{nz}\hat{0}_{mz} - \hat{1}_{nz}\hat{1}_{mz})\hat{0}_{pz}\hat{0}_{qz}, \hat{C}_{1,nm}^{(z)} = (\hat{1}_{nz}\hat{1}_{mz} - \hat{0}_{nz}\hat{0}_{mz})\hat{1}_{pz}\hat{1}_{qz}, \quad (4.7)$$

for $n, m = 1, \dots, 4$ and $n \neq m$. Moreover, we can express the expectation values of the Hermitian operators $\hat{C}_{0,nm}^{(z)}$ and $\hat{C}_{1,nm}^{(z)}$ in terms of joint probabilities for some output state:

$$\begin{aligned} \langle \hat{C}_{0,nm}^{(z)} \rangle &= P(v_{nm} = 0, \mathbf{v}' = 0) - P(v_{nm} = 2, \mathbf{v}' = 0), \\ \langle \hat{C}_{1,nm}^{(z)} \rangle &= P(v_{nm} = 2, \mathbf{v}' = 2) - P(v_{nm} = 0, \mathbf{v}' = 2), \end{aligned} \quad (4.8)$$

where $v_{nm} = v_n + v_m$ and $\mathbf{v}' = \sum_{i=1, i \neq n \neq m}^4 v_i$. Theorem 4 shows that if the subsystem composed of the n th and the m th parties is uncorrelated with another one, the measured outcomes must satisfy $\langle \hat{C}_{0,nm}^{(z)} \rangle \langle \hat{C}_{1,nm}^{(z)} \rangle \leq 0$. On the other hand, $\langle \hat{C}_{0,nm}^{(z)} \rangle \langle \hat{C}_{1,nm}^{(z)} \rangle > 0$ indicates that they are dependent.

It is clear that, for a pure generalized four-qubit GHZ state, we have

$$\langle \hat{C}_{0,nm}^{(z)} \rangle = \cos^2(\theta), \quad \langle \hat{C}_{1,nm}^{(z)} \rangle = \sin^2(\theta), \quad (4.9)$$

and hence $\langle \hat{C}_{0,nm}^{(z)} \rangle \langle \hat{C}_{1,nm}^{(z)} \rangle > 0$. Thus we know that the subsystem composed of the n th and the m th parties are correlated with another. Therefore, the condition, $\langle \hat{C}_{0,nm}^{(z)} \rangle \langle \hat{C}_{1,nm}^{(z)} \rangle > 0$, is also a necessary condition of the state $|\Phi(\theta, \phi)\rangle$.

After introducing two correlation conditions for the pure generalized GHZ state under M_{4z} , let us progress towards the third one for correlation. Under the local measurement setting, $M_{4x} = (X, X, X, X)$, we formulate four sets of correlators which correspond to the following operators for identifying correlations between the n th party and others:

$$\hat{C}_{0,n}^{(x)} = (\hat{0}_{nx} - \hat{1}_{nx}) \otimes \hat{\mathbf{E}}, \hat{C}_{1,n}^{(x)} = (\hat{1}_{nx} - \hat{0}_{nx}) \otimes \hat{\mathbf{O}}, \quad (4.10)$$

where

$$\hat{\mathbf{E}} = (\hat{0}_{mx}\hat{0}_{px}\hat{0}_{qx} + \hat{0}_{mx}\hat{1}_{px}\hat{1}_{qx} + \hat{1}_{mx}\hat{0}_{px}\hat{1}_{qx} + \hat{1}_{mx}\hat{1}_{px}\hat{0}_{qx}), \quad (4.11)$$

$$\hat{\mathbf{O}} = (\hat{1}_{mx}\hat{1}_{px}\hat{1}_{qx} + \hat{1}_{mx}\hat{0}_{px}\hat{0}_{qx} + \hat{0}_{mx}\hat{1}_{px}\hat{0}_{qx} + \hat{0}_{mx}\hat{0}_{px}\hat{1}_{qx}). \quad (4.12)$$

From the expectation values of $\hat{C}_{0,n}^{(x)}$ and $\hat{C}_{1,n}^{(x)}$ for some state and Theorem 4, we could know the correlation behavior of the system, i.e., for a system in which the n th party is uncorrelated with the rest under M_{4x} , the outcomes of measurements must satisfy the condition: $C_{0,n}^{(x)}C_{1,n}^{(x)} \leq 0$.

For the pure state, $|\Phi(\theta, \phi)\rangle$, the expectation values of $\hat{C}_{k,n}^{(x)}$ is given by

$$\langle \hat{C}_{0,n}^{(x)} \rangle = \langle \hat{C}_{1,n}^{(x)} \rangle = \sin(2\theta) \cos(\phi)/2, \quad (4.13)$$

and ensure that there are correlations between measured outcomes under the local measurement setting, M_{4x} . Thus the condition, $C_{0,n}^{(x)}C_{1,n}^{(x)} > 0$, is necessary for the pure generalized four-qubit GHZ state.

Entanglement imbedded in the pure generalized four-qubit GHZ state manifests itself via necessary conditions of correlations presented above under two local measurement settings. Therefore we combine all of the correlator operators involved in the necessary conditions:

$$\hat{C}_{\Phi} = \hat{C}^{(z)} + \hat{C}^{(x)},$$

where

$$\begin{aligned} \hat{C}^{(z)} &= \sum_{j=0}^1 \left(\sum_{n=1}^4 \hat{C}_{j,n}^{(z)} + \sum_{m=2}^4 \hat{C}_{j,1m}^{(z)} \right) \\ &= 8(\hat{0}_{1z}\hat{0}_{2z}\hat{0}_{3z}\hat{0}_{4z} + \hat{1}_{1z}\hat{1}_{2z}\hat{1}_{3z}\hat{1}_{4z}) - \mathbf{1}, \end{aligned} \quad (4.14)$$

$$\begin{aligned} \hat{C}^{(x)} &= \sum_{n=1}^4 \sum_{k=0}^1 \hat{C}_{k,n}^{(x)} \\ &= 4X_1X_2X_3X_4, \end{aligned} \quad (4.15)$$

Table 4.1: Summaries of numerical results of $\alpha_{\Phi}(\theta, \phi)$ for $\mathcal{W}_{\Phi}(\theta, \phi)$, the parameters, γ_{Φ} , which are utilized to prove $\mathcal{W}_{\Phi}(\theta, \phi)$ and $\delta_{\text{noise}, \Phi}$ involved in robustness of the proposed witness operator for detecting truly multipartite entanglement. Three different cases for the state $|\Phi(\theta, \phi)\rangle$ corresponding to $\mathcal{W}_{\Phi}(\theta, \phi)$ have been demonstrated.

| (θ, ϕ) | $(\frac{\pi}{4}, \frac{\pi}{6})$ | $(\frac{\pi}{4.9}, 0)$ | $(\frac{\pi}{3.7}, \frac{\pi}{9})$ |
|------------------|----------------------------------|------------------------|------------------------------------|
| α_{Φ} | 9.01 | 9.21 | 8.92 |
| γ_{Φ} | 6.54 | 6.44 | 6.86 |
| δ_{Φ} | 0.139 | 0.150 | 0.169 |

and then utilize the operator \hat{C}_{Φ} to construct witness operator for detections of truly multipartite entanglement. Three example are shown as follows. The witness operator:

$$\mathcal{W}_{\Phi}(\theta, \phi) = \alpha_{\Phi}(\theta, \phi)\mathbf{1} - \hat{C}_{\Phi}, \quad (4.16)$$

where $\alpha_{\Phi}(\theta, \phi)$ is some constant, detects genuine multipartite entanglement for the cases, (θ, ϕ) : $(\pi/4, \pi/6)$, $(\pi/4.9, 0)$, and $(\pi/3.7, \pi/9)$. Table 4.1 gives a summary of $\alpha_{\Phi}(\theta, \phi)$ for these cases.

In order to prove that $\mathcal{W}_{\Phi}(\theta, \phi)$ is a entanglement witness for detecting genuine multipartite entanglement, we have to show the following comparison between

$$\mathcal{W}_{\Phi}^p(\theta, \phi) = \alpha_{\Phi}^p \mathbf{1} - |\Phi(\theta, \phi)\rangle \langle \Phi(\theta, \phi)|, \quad (4.17)$$

and $\mathcal{W}_{\Phi}(\theta, \phi)$ [72]: if a state ρ satisfies $\text{Tr}(\mathcal{W}_{\Phi}(\theta, \phi)\rho) < 0$, it also satisfies $\text{Tr}(\mathcal{W}_{\Phi}^p(\theta, \phi)\rho) < 0$, i.e., $\mathcal{W}_{\Phi}(\theta, \phi) - \gamma_{\Phi}\mathcal{W}_{\Phi}^p(\theta, \phi) \geq 0$, where $\gamma_{\Phi}(\theta, \phi)$ is some positive constant. Through the method given by Bourennane *et al.* [70], we derive the operator $\mathcal{W}_{\Phi}^p(\theta, \phi)$ and have $\alpha_{\Phi}^p = \cos^2(\theta)$ for $0 < \theta \leq \pi/4$ and $\alpha_{\Phi}^p = \sin^2(\theta)$ for $\pi/4 \leq \theta < \pi/2$. Table 4.1 summarizes the parameters γ_{Φ} utilized to prove that the proposed operators are indeed entanglement witnesses for detecting truly multipartite entanglement.

In addition, we are concerned with the robustness to noise for the witness $\mathcal{W}_{\Phi}(\theta, \phi)$. The robustness of $\mathcal{W}_{\Phi}(\theta, \phi)$ depends on the noise tolerance: $p_{\text{noise}} < \delta_{\text{noise}}$, is such that

Table 4.2: Expectation values of three proposed entanglement witnesses including $\mathcal{W}_\Phi(\frac{\pi}{4}, \frac{\pi}{6})$, $\mathcal{W}_\Phi(\frac{\pi}{4.9}, 0)$, and $\mathcal{W}_\Phi(\frac{\pi}{3.7}, \frac{\pi}{9})$ for the pure states $|\Phi\rangle$: $|\Phi(\frac{\pi}{4}, \frac{\pi}{6})\rangle$, $|\Phi(\frac{\pi}{4.9}, 0)\rangle$, and $|\Phi(\frac{\pi}{3.7}, \frac{\pi}{9})\rangle$.

| $ \Phi\rangle$ | $ \Phi(\frac{\pi}{4}, \frac{\pi}{6})\rangle$ | $ \Phi(\frac{\pi}{4.9}, 0)\rangle$ | $ \Phi(\frac{\pi}{3.7}, \frac{\pi}{9})\rangle$ |
|---|--|------------------------------------|--|
| $\text{Tr}(\mathcal{W}_\Phi(\frac{\pi}{4}, \frac{\pi}{6}) \Phi\rangle\langle\Phi)$ | -1.45 | -1.83 | -1.72 |
| $\text{Tr}(\mathcal{W}_\Phi(\frac{\pi}{4.9}, 0) \Phi\rangle\langle\Phi)$ | -1.25 | -1.63 | -1.52 |
| $\text{Tr}(\mathcal{W}_\Phi(\frac{\pi}{3.7}, \frac{\pi}{9}) \Phi\rangle\langle\Phi)$ | -1.55 | -1.92 | -1.81 |

$\rho = p_{\text{noise}}/21 + (1 - p_{\text{noise}})|\Phi(\theta, \phi)\rangle\langle\Phi(\theta, \phi)|$, is identified as a genuine multipartite entanglement. Three cases for the robustness to noise for the witness $\mathcal{W}_\Phi(\theta, \phi)$ have been summarized in Table 4.1.

Further, we show the expectation values of the proposed entanglement witnesses for different pure states by Table 4.2. From comparison with the results we know that a aim state, say $|\Phi(\theta', \phi')\rangle$, does not always give the smallest expectation value of the corresponding witness operator, $\mathcal{W}_\Phi(\theta', \phi')$. One can identify with the operator $\mathcal{W}_\Phi(\theta', \phi')$ that an experimental output ρ is truly multipartite entanglement if $\text{Tr}(\mathcal{W}_\Phi(\theta', \phi')\rho) < 0$. Further, if $\text{Tr}(\mathcal{W}_\Phi(\theta', \phi')\rho) < \text{Tr}(\mathcal{W}_\Phi(\theta', \phi')|\Phi(\theta', \phi')\rangle\langle\Phi(\theta', \phi')|)$, the state ρ is not in the state $|\Phi(\theta', \phi')\rangle$ class.

The novel approach to derive \hat{C}_Φ shown above can be applied to the cases for arbitrary number of qubits straightforwardly. One can formulate sets of correlator operators to identify correlations between two subsystems under two local measurement settings and then construct the witness operators further.

4.3 Four-qubit singlet state

Very recently, four-party quantum secret sharing has been demonstrated via the resource of four photon entanglement [45], which is called the four-qubit singlet state [123]. Through the same method for the witness of a generalized four-qubit GHZ state, we give a novel entanglement witness to detect the four-qubit singlet state.

The four-qubit singlet state is expressed as the following form:

$$|\Psi_4\rangle = \frac{1}{\sqrt{3}} \left[|0011\rangle_z + |1100\rangle_z - \frac{1}{2}(|0110\rangle_z + |1001\rangle_z + |0101\rangle_z + |1010\rangle_z) \right]. \quad (4.18)$$

Under the local measurement setting, M_{4z} , we formulate eight sets of criteria for identifying quantum correlation between a specific party and others: the first type of identifications include the following four sets of correlators:

$$\begin{aligned} \hat{C}_{0,m}^{(z)} &= \hat{0}_{1z}\hat{0}_{2z}\hat{1}_{3z}\hat{1}_{4z} - X_m(\hat{0}_{1z}\hat{0}_{2z}\hat{1}_{3z}\hat{1}_{4z})X_m, \\ \hat{C}_{1,m}^{(z)} &= \hat{1}_{1z}\hat{1}_{2z}\hat{0}_{3z}\hat{0}_{4z} - X_m(\hat{1}_{1z}\hat{1}_{2z}\hat{0}_{3z}\hat{0}_{4z})X_m, \end{aligned} \quad (4.19)$$

where $X_m = \sigma_x$ is performed on the m th party for $m = 1, \dots, 4$. Then, the second type criteria are formulated as:

$$\begin{aligned} \hat{C}_{0n,k}^{(z)} &= [\hat{0}_{(2n+1)z}\hat{1}_{(2n+2)z} - X_k(\hat{0}_{(2n+1)z}\hat{1}_{(2n+2)z})X_k] [\hat{0}_{(2n\oplus 3)z}\hat{1}_{(2n\oplus 4)z} + \hat{1}_{(2n\oplus 3)z}\hat{0}_{(2n\oplus 4)z}], \\ \hat{C}_{1n,k}^{(z)} &= [\hat{1}_{(2n+1)z}\hat{0}_{(2n+2)z} - X_k(\hat{1}_{(2n+1)z}\hat{0}_{(2n+2)z})X_k] [\hat{0}_{(2n\oplus 3)z}\hat{1}_{(2n\oplus 4)z} + \hat{1}_{(2n\oplus 3)z}\hat{0}_{(2n\oplus 4)z}], \end{aligned} \quad (4.20)$$

where $k = (2n + 1), (2n + 2)$ for $n = 0, 1$; and the symbol \oplus behaves as the addition modulo 4 for $n = 1$ and as an ordinary addition for $n = 0$. The expectation values of the operators $\hat{C}_{l,m}^{(z)}$ and $\hat{C}_{ln,k}^{(z)}$ for the pure four-qubit singlet state can be evaluated directly and are given by $C_{l,m,\Psi_4}^{(z)} = 1/3$ and $C_{ln,k,\Psi_4}^{(z)} = 1/6$ for $l = 0, 1$.

Through Theorem 4, it is easy to see that the conditions involved in the expectation values of $\hat{C}_{l,m}^{(z)}$ and $\hat{C}_{ln,k}^{(z)}$:

$$\langle \hat{C}_{0,m}^{(z)} \rangle \langle \hat{C}_{1,m}^{(z)} \rangle > 0, \quad \langle \hat{C}_{0n,k}^{(z)} \rangle \langle \hat{C}_{1n,k}^{(z)} \rangle > 0, \quad (4.21)$$

are necessary for the pure four-qubit singlet state.

For invariance of the wave function presented in the eigenbasis of σ_x (σ_y), in analogy,

we can construct 8 sets of Hermitian operators,

$$(\hat{C}_{0,m}^{(x(y))}, \hat{C}_{1,m}^{(x(y))}) \text{ and } (\hat{C}_{0n,k}^{(x(y))}, \hat{C}_{1n,k}^{(x(y))}), \quad (4.22)$$

via the replacement of the index z in above hermitian operators by the index x (y) and constructing the operators in the eigenbasis of $\sigma_{x(y)}$. The expectation values of the above operators are all positive for the state $|\Psi_4\rangle$, and so we have the following necessary conditions of the state $|\Psi_4\rangle$:

$$\langle \hat{C}_{0,m}^{(x(y))} \rangle \langle \hat{C}_{1,m}^{(x(y))} \rangle > 0 \text{ and } \langle \hat{C}_{0n,k}^{(x(y))} \rangle \langle \hat{C}_{1n,k}^{(x(y))} \rangle > 0, \quad (4.23)$$

Then, we combine all of the correlator operators proposed above:

$$\hat{C}_{\Psi_4} = \hat{C}_{\Psi_4}^{(x)} + \hat{C}_{\Psi_4}^{(y)} + \hat{C}_{\Psi_4}^{(z)}, \quad (4.24)$$

where

$$\hat{C}_{\Psi_4}^{(i)} = \sum_{l=0}^1 \left[5 \sum_{m=1}^4 \hat{C}_{l,m}^{(i)} + \sum_{n=0}^1 \sum_{k=2n+1}^{2n+2} \hat{C}_{ln,k}^{(i)} \right], \quad (4.25)$$

for $i = x, y, z$, and present a entanglement witness to detect the four-qubit singlet state. The following witness operator detects truly multipartite entanglement for states close to the state $|\Psi_4\rangle$:

$$\mathcal{W}_{\Psi_4} = \alpha_{\Psi_4} \mathbf{1} - \hat{C}_{\Psi_4}, \quad (4.26)$$

where $\alpha_{\Psi_4} = 36.5$.

We use the method utilized for $\mathcal{W}_{\Phi}(\theta, \phi)$ to prove \mathcal{W}_{Ψ_4} is a entanglement witness. First, we seek the witness operator $\mathcal{W}_{\Psi_4}^p$. Through Ref. [70], the operator is given by:

$$\mathcal{W}_{\Psi_4}^p = \frac{3}{4} \mathbf{1} - |\Psi_4\rangle \langle \Psi_4|. \quad (4.27)$$

Then, we have to show that if a state ρ satisfies $\text{Tr}(\mathcal{W}_{\Psi_4}\rho) < 0$, it also satisfies $\text{Tr}(\mathcal{W}_{\Psi_4}^p\rho) < 0$. We find that $\gamma_{\Psi_4} = 30$ is such that $\mathcal{W}_{\Psi_4} - \gamma_{\Psi_4}\mathcal{W}_{\Psi_4}^p \geq 0$.

The sets of correlator operators $\hat{C}_{\Psi_4}^{(x)}$, $\hat{C}_{\Psi_4}^{(y)}$, and $\hat{C}_{\Psi_4}^{(z)}$ note that only three local measurement settings are used in the witness operator \mathcal{W}_{Ψ_4} . The number of local measurement settings is smaller than the required one, 15 local measurement settings, in Ref. [70]. Moreover, the robustness of the witness \mathcal{W}_{Ψ_4} is specified by $\delta_{\Psi_4} = 15/88 \simeq 0.1705$. This result satisfies the experimental requirement of robustness in Ref. [70].

4.4 Three-qubit W state

Let us proceed to study the correlations imbedded in the three-qubit W state:

$$|W_3\rangle = \frac{1}{\sqrt{3}}(|001\rangle_z + |010\rangle_z + |100\rangle_z), \quad (4.28)$$

When $|W_3\rangle$ is shown in this representation, the following correlator operators are utilized to show that the n th qubit is dependent on the other ones:

$$\begin{aligned} \hat{C}_{0n}^{(z)} &= (\hat{0}_{nz} - \hat{1}_{nz}) \otimes (\hat{0}_{mz} \otimes \hat{1}_{qz} + \hat{1}_{mz} \otimes \hat{0}_{qz}), \\ \hat{C}_{1n}^{(z)} &= (\hat{1}_{nz} - \hat{0}_{nz}) \otimes (\hat{0}_{mz} \otimes \hat{0}_{qz}), \end{aligned} \quad (4.29)$$

for $n = 1, 2, 3$. For the pure state $|W_3\rangle$, it is clear that $\langle \hat{C}_{0n}^{(z)} \rangle = 2/3$ and $\langle \hat{C}_{1n}^{(z)} \rangle = 1/3$, and, through Theorem 4, we are convinced that the n th qubit is dependent on the subsystem composed of the m th and q th ones, i.e., all three qubits of the system are dependent on each other. Furthermore, $|W_3\rangle$ can also be expressed by

$$|W_3\rangle = \frac{1}{2}\sqrt{\frac{3}{2}}(|000\rangle_x + |111\rangle_x) + \frac{1}{2\sqrt{6}}(|001\rangle_x + |010\rangle_x - |011\rangle_x + |100\rangle_x - |101\rangle_x - |110\rangle_x), \quad (4.30)$$

where $|v\rangle_{nx} = (|0\rangle_{nz} + (-1)^v |1\rangle_{nz})/\sqrt{2}$ for $v \in \{0, 1\}$. Thus, we give the following correlator operators to show all qubits of the system are dependent on each other:

$$\hat{C}_{0n}^{(x)} = (\hat{0}_{nx} - \hat{1}_{nx})\hat{0}_{mx}\hat{0}_{px}, \hat{C}_{1n}^{(x)} = (\hat{1}_{nx} - \hat{0}_{nx})\hat{1}_{mx}\hat{1}_{px}, \quad (4.31)$$

with $C_{0xn} = C_{1xn} = 1/3$. Similarly, the operators given by

$$\hat{C}_{0n}^{(y)} = (\hat{0}_{ny} - \hat{1}_{ny})\hat{0}_{my}\hat{0}_{py}, \hat{C}_{1n}^{(y)} = (\hat{1}_{ny} - \hat{0}_{ny})\hat{1}_{my}\hat{1}_{py}, \quad (4.32)$$

where $|v\rangle_{ny} = (|0\rangle_{nz} + (-1)^v |1\rangle_{nz})/\sqrt{2}$, also provide $\langle \hat{C}_{0n}^{(y)} \rangle = \langle \hat{C}_{1n}^{(y)} \rangle = 1/3$, and by which we can feature the correlation character of $|W_3\rangle$ in the correlator operators $\hat{C}_{0n}^{(y)}$ and $\hat{C}_{1n}^{(y)}$. In conclusion, the sets of correlators $(\langle \hat{C}_{0n}^{(z)} \rangle, \langle \hat{C}_{1n}^{(z)} \rangle)$, $(\langle \hat{C}_{0n}^{(x)} \rangle, \langle \hat{C}_{1n}^{(x)} \rangle)$, and $(\langle \hat{C}_{0n}^{(y)} \rangle, \langle \hat{C}_{1n}^{(y)} \rangle)$ can be the essential properties of the state $|W_3\rangle$. When using the operator

$$\hat{C}_{W_3} = \hat{C}_{W_3}^{(x)} + \hat{C}_{W_3}^{(y)} + \hat{C}_{W_3}^{(z)}, \quad (4.33)$$

where

$$\hat{C}_{W_3}^{(i)} = \sum_{l=0}^1 \sum_{m=1}^3 \hat{C}_{lm}^{(i)}, \quad (4.34)$$

for $i = x, y, z$, to construct a witness for detecting states close to $|W_3\rangle$, we have the operator

$$\mathcal{W}_{W_3} = \alpha_{W_3} \mathbf{1} - \hat{C}_{W_3}, \quad (4.35)$$

where $\alpha_{W_3} = 5.6$, which can be shown to be a witness by the fact $\mathcal{W}_{W_3} - 6\mathcal{W}_{W_3}^p \geq 0$, where [70]

$$\mathcal{W}_{W_3}^p = \frac{2}{3}\mathbf{1} - |W_3\rangle\langle W_3|. \quad (4.36)$$

\mathcal{W}_{W_3} is robust against noise and has a noise tolerance $\delta_{\Psi_4} = 0.2631$.

4.5 Conclusion

We illustrate the utility of the conditions of correlations proposed by detections of three different types of entangled states that cannot be described by local stabilizers. With the help of Theorem 4, we give the corresponding entanglement witnesses that require fewer local measurement settings when used in experiments. This chapter and the previous two chapters show that the criteria of quantum correlation proposed do not only help to reveal correlation structures of many-qubit and two-qudit entanglement but also can be utilized to construct entanglement witnesses with highly noise tolerance. In the next chapter, we progress to introduce a general condition of correlation for many-qudit entanglement.

Chapter 5

Phase-dependent criterion for many-qudit entanglement

5.1 Motivation



While the entanglement of bipartite qudits is still under intensive study [17], the many-qudit entanglement has attracted increasing attention for its distinct features [18, 19]. The GHZ argument [19] and the generic Bell inequalities [18] for many qudits provide a refutation of locality and realism. Measurements of some specific observables involved higher-order correlation functions play important roles to reveal the quantum nonlocality [17–19]. In this situation, it is natural to ask whether product of observables in a specific direction of measurement can provide information about dependence of entangled qudits. Can one obtain necessary conditions of correlation of entangled qudits from the general correlation function? Furthermore, the question of whether one can detect truly multipartite quantum correlations with fewer measurements is crucial to both entanglement physics and the quantum information processing.

In this chapter, we introduce a novel phase-dependent condition of correlations for many-qudit entanglement. We reveal that the correlation functions utilized in the GHZ argument [19] and the generic Bell inequalities [18] are comprised of phase-dependen

criterion of correlations. We construct entanglement witness operators with highly robustness for detecting truly many-qudit entanglement. All of the witnesses presented can be realized with fewer experimental efforts and can be applied to present experiments for entangled qudits [20–23] directly. Especially, the criteria introduced in the previous three chapters are special cases of the phase-dependent condition of correlations.

5.2 Basic idea

In each run of Bell-type experiments for revealing correlations inherent in a multi-level multipartite system, a set of local measurement setting, denoted by $M_l = (V_1, V_2, \dots, V_N)$ is chosen and single-qudit measurements of observable V_i for $i = 1, \dots, N$ are taken on the N particles in parallel. After measurements, one can acquire a set of results $v_{[\mathbf{N}]} = (v_1, v_2, \dots, v_N)$ where v_i is an element of the set $\{0, 1, \dots, d-1\}$. If sufficient runs of such measurements have been made under a chosen local measurement setting, the correlation between experimental outcomes can be revealed through the analytical analysis of experimental records.

To investigate the correlations between two sets of results $\{v_{[\mathbf{m}]}\}$ and $\{v_{[\mathbf{n}]}\}$ for the subsystem of m particles and the one of n particles, in what follows, we will present a novel method to attain this aim. The formulation of our strategy to investigate correlations between any two subsystems consists of two parts. Firstly, we introduce the following condition that holds for any physical systems:

$$\sum_{k=1}^{\lambda} A_k = 0, \quad (5.1)$$

where

$$A_k = \sum_i \gamma_{ik} P(v_{[\mathbf{m}]ik}), \quad (5.2)$$

γ_{ik} is a complex number with a unit norm, and $P(v_{[\mathbf{m}]ik})$ denotes the joint probability to

get the result $v_{[\mathbf{m}]ik}$ for the subsystem composed of m particles. The number of sets λ relies on $\{A_k\}$ designed. It is worth noting the above condition implies that all the A_k 's are not in the same phase. Then, we give correlation polynomials of the form

$$C_k = \sum_i \gamma_{ik} P(v_{[\mathbf{m}]ik}, v_{[\mathbf{n}]k}), \quad (5.3)$$

and the dependency of one subsystem on another one can be described by the following theorem:

Theorem 5. If the arguments of all C_k 's are the selfsame, then the outcomes of measurement for the two subsystems are dependent [124].

Proof. If the two subsystems are independent, the joint probability $P(v_{[\mathbf{m}]ik}, v_{[\mathbf{n}]k})$ must be a product of two individual ones: $P(v_{[\mathbf{m}]ik})P(v_{[\mathbf{n}]k})$, and then C_k is recast as

$$C_k = P(v_{[\mathbf{n}]k})A_k. \quad (5.4)$$

Since the phases of A_k 's are not all identical, the arguments of C_k 's must be different, whereas a contradiction reveals the dependency of one subsystem on another one. \square

We call C_k 's correlators for their utility. Since entanglement is the physical property that manifests itself via different local measurement settings, according to the knowledge of the entangled qudits to be created we can construct more sets of correlators under the condition of dependence and different local measurement settings. Then we utilize them to analyze the experimental outputs. Determination of the value of $|\sum_k C_k|$ could be one possible means for identifying correlations embedded in entangled qudits. It is clear that $|\sum_k A_k P(v_{[\mathbf{n}]k})| \leq 1$ for independent subsystems, whereas we could feature the correlation of entangled qudits to be created in the criterion $|\sum_k C_k| = 1$ under several local measurement settings. From which, we will see that truly many-qudit entanglement can be detected in a systematic way. In what follows, we will present two types of $\{C_k\}$ associated with different designation of $\{A_k\}$.

5.3 Many-qudit Bell inequalities

Let us give a concrete example to illustrate the first kind of correlators. For a three-qudit GHZ state with the state vector:

$$|\Psi_{3 \times d}\rangle = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} |v\rangle^{\otimes 3}, \quad (5.5)$$

where $\{|v\rangle\}$ is a complete set of orthonormal basis, we can use the correlators corresponding to the following operators to specify the correlation between the i th qudit and the subsystem composed of the j th and the q th ones of the state $|\Psi_{3 \times d}\rangle$:

$$\hat{C}_k^{(n)} = \sum_{v_i=0}^{d-1} \omega^{n(v_i+k)} \hat{v}_{if} \otimes \hat{v}_{[jq]f}, \quad (5.6)$$

for $k = 0, 1, \dots, d-1$, where n is some positive integer, $\omega = \exp(i2\pi/d)$, $\hat{v}_{if} = |v_i\rangle_{ff} \langle v_i|$, $\hat{v}_{[jq]f} = \sum_{v_j, v_q} \hat{v}_{jf} \otimes \hat{v}_{qf}$, $|v_i\rangle_f = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} \omega^{-v_i v} |v\rangle$, $v_j + v_q \doteq k$, and \doteq denotes equality modulo d . Since $C_{kQ}^{(n)} = \langle \Psi_{3 \times d} | \hat{C}_k^{(n)} | \Psi_{3 \times d} \rangle = 1/d$ for all k 's and partitions of the systems: $[1|23]$, $[2|13]$, and $[3|12]$. Then a linear combination of $\hat{C}_k^{(n)}$'s can be consider as a means of identification of the state $|\Psi_{3 \times d}\rangle$ and we have

$$\sum_{k=0}^{d-1} \hat{C}_k^{(n)} = \hat{V}_{1f}^n \otimes \hat{V}_{2f}^n \otimes \hat{V}_{3f}^n \quad (5.7)$$

where

$$\hat{V}_{if} = \sum_{v_i=0}^{d-1} \omega^{v_i} \hat{v}_{if}. \quad (5.8)$$

Furthermore, more operators of correlators under different local measurement settings can be introduced to specify the dependence of qudits, and the sum of these operators

can be the following ones:

$$\hat{V}_{if}^n \otimes \hat{V}_{jf}^n \otimes \hat{V}_{qF}^n, \hat{V}_{if}^n \otimes \hat{V}_{jF}^n \otimes \hat{V}_{qF}^n, \hat{V}_{iF}^n \otimes \hat{V}_{jF}^n \otimes \hat{V}_{qF}^n, \quad (5.9)$$

where

$$\hat{V}_{iF}^n = \sum_{v_i=0}^{d-1} \omega^{v_i} \hat{v}_{iF} \quad (5.10)$$

and the eigenstates of the observable are of the form $|v_i\rangle_F = \frac{1}{\sqrt{d}} \sum_{v_i=0}^{d-1} w^{-v(v_i+1/2)} |v_i\rangle$. In addition to the operators involved correlators discussed above, their Hermitian conjugates also work in the same way for correlation.

The generalized GHZ state can be featured in correlators under different local measurement settings. Each set of correlators is one necessary condition of a GHZ state. Then, one can combine all of the operators of correlators as a single identification to distinguish the quantum correlations imbedded in the generalized GHZ state and the ones predicted by local realistic theories. It is remarkable that the kernel of the generic Bell inequalities for three qudits [18] represented by the observable

$$\hat{B}_3 = \frac{1}{2^3} \sum_{n=1}^{d-1} \bigotimes_{i=1}^3 (\hat{V}_{if} + \omega^{n/2} \hat{V}_{iF}) + \text{H.c.}, \quad (5.11)$$

is composed of operators of correlators associated with necessary conditions of the GHZ state. For N -qudit Bell inequalities, through a direct calculation, we rephrase the expected value of the N -qudit Bell kernel \hat{B}_N [18] for the N -qudit GHZ state by the following

polynomial of correlators:

$$B_{NQ} = \frac{1}{2^{N-1}} \sum_{l=1}^{2^{N-1}} \sum_{n=1}^{d-1} \sum_{k=0}^{d-1} C_{lkQ}^{(n)}, \quad (5.12)$$

where l 's denote local measurement settings and $C_{lkQ}^{(n)}$'s fulfill the specifications of correlators. In particular, since $C_{lkQ}^{(n)} = 1/d$ for all the parameters involved and for any partitions of the N qudits considered, the correlation properties of the generalized N -qudit GHZ state have been shown concretely. For example, the operator $\hat{V}_0 = \bigotimes_{i=1}^N \hat{V}_{if}^n$ is one of the elements of \hat{B}_N and can be represented by $\sum_{k=0}^{d-1} \hat{C}_k^{(n)}$, where $\hat{C}_k^{(n)} = \omega^{nk} \hat{v}_{[m]f} \bigotimes_{i=m+1}^N \hat{V}_{if}^n$, $\hat{v}_{[m]f} = \sum_{v_1, \dots, v_m} \bigotimes_{i=1}^m \hat{v}_{if}$, and $\sum_{i=1}^m v_i \doteq k$. Since $C_{lkQ}^{(n)} = 1/d$ for all k 's, we realize that the subsystem comprised of the first m qudits is dependent on the one composed of the rest. This result holds for any partitions of the system, which provide the information about correlations between any two subsystems with m qudits and $(N - m)$ ones respectively by n_c sets of correlators, where $n_c = \sum_{m=1}^{\lfloor N/2 \rfloor} f(N, m) \frac{m!}{m!(N-m)!}$, $f(N, m) = 2^{-\delta[m, \lfloor N/2 \rfloor]}$ for N even, and $f(N, m) = 1$ for N odd, i.e., the definition (2.8).

The following operator will be shown useful studying the generalized GHZ state:

$$\begin{aligned} \hat{V}_{iy} &= \sum_{v_i=0}^{d-1} \omega^{v_i+p/2} |(v_i - 1) \bmod v_i\rangle \langle v_i| \\ &= \sum_{v_i=0}^{d-1} \omega^{v_i+p} \hat{v}_{iy}, \end{aligned} \quad (5.13)$$

where $\hat{v}_{iy} = |v_i\rangle_{ff} \langle v_i|$, $\{|v_i\rangle_y\}$ is the set of orthonormal eigenbasis of \hat{V}_{iy} , $p = 0$ for d odd, and $p = 1$ for d even. Tensor products of \hat{V}_{if} and \hat{V}_{ky} can be used to reveal the correlations embedded in a N -qudit entanglement. The operators

$$\hat{V}_i = \bigotimes_{k=1; k \neq i}^N \hat{V}_{kf} \otimes \hat{V}_{if}^{d-1}, \quad (5.14)$$

for $i = 1, \dots, N$ can be decomposed into operators of correlators like \hat{V}_0 , and each correlator is $-1/d$. The operators \hat{V}_i 's are the central part of the GHZ contradictions for many qudits [19]. Through the conditions of correlations, one can realize that the utility of each operator is to specify the quantum correlations between qudits and to show the properties of dependence of the generalized N -qudit GHZ state under $N + 1$ local measurement settings.

5.4 Entanglement witnesses for many-qudit entangled states

We proceed to introduce the second type of correlators and give several entanglement witness operators which need only two local measurement settings. The correlators proposed in the second and the third chapters are classified to this type. The witness operators proposed are of the form: $\mathcal{W}_\phi = \alpha_\phi \mathbf{1} - \hat{C}_\phi$, where α_ϕ is some constant and \hat{C}_ϕ is a linear combination of operators of correlators associated with the necessary conditions of the many-qudit state $|\phi\rangle$. If measured outcomes show that $\text{Tr}(\mathcal{W}_\phi \rho) < 0$, an experimental output state ρ is identified as a truly multipartite entanglement which is close to the aim state $|\phi\rangle$. Moreover, we also show that the proposed witnesses are robust to noise. The robustness of \mathcal{W}_ϕ is determined by the noise tolerance: $p_{\text{noise}} < \delta_{\text{noise}}$, is such that $\rho = p_{\text{noise}} \mathbf{1}/d^n + (1 - p_{\text{noise}}) |\phi\rangle \langle \phi|$ is identified as a genuine many-qudit entanglement. The proof for showing that the proposed operators are entanglement witnesses and the robustness of the witness operators are shown in Appendix C.

(a) Two-qudit singlet state. Firstly, we will show how to detect states close a two-qudit singlet state of the state vector:

$$|s\rangle = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} (-1)^v |v\rangle \otimes |d - v - 1\rangle. \quad (5.15)$$

For the first local measurement setting, the correlators are given via the operators,

$$\hat{C}_k^{(u)} = [\hat{k} - U(\hat{k})] \otimes \hat{v}_2, \quad (5.16)$$

for $k = 0, \dots, d-1$ and $u = 1, \dots, \beta_d$, where $v_2 = d-1-k$, U is a injective map s.t. $U(\hat{k}) \mapsto \hat{k}'$ and $k' \neq k$, and each $\{U(\hat{k})\}$ is numbered by u . Then there are β_d sets of $\{\hat{C}_k^{(u)}\}$. Let us take $d = 3$ for example. We have two sets of correlator operators, i.e., $\beta_3 = 2$, given by

$$\begin{aligned} \{\hat{C}_0^{(1)} = (\hat{0} - \hat{1}) \otimes \hat{2}, \hat{C}_1^{(1)} = (\hat{1} - \hat{2}) \otimes \hat{1}, \hat{C}_2^{(1)} = (\hat{2} - \hat{0}) \otimes \hat{0}\}, \\ \{\hat{C}_0^{(2)} = (\hat{0} - \hat{2}) \otimes \hat{1}, \hat{C}_1^{(2)} = (\hat{1} - \hat{0}) \otimes \hat{2}, \hat{C}_2^{(2)} = (\hat{2} - \hat{1}) \otimes \hat{0}\}. \end{aligned}$$

For general d , β_d can be determined analytically by the definition (2.10) of γ_d . Since $C_{kQ}^{(u)} = 1/d$ for all k 's and u 's, the properties of dependence have be shown. For the second local measurement setting, operators of correlators are defined by $\hat{C}_{rk}^{(u)} = [\hat{k}_r - U(\hat{k}_r)] \otimes \hat{v}_{2k}$, where $v_2 + k \doteq 0$, the projector \hat{k}_r 's correspond to elements of a complete set of orthonormal basis vectors $\{|k\rangle_r\}$ and

$$|k\rangle_r = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} (-1)^{k+v} w^v |v\rangle. \quad (5.17)$$

Through a simple calculation, we have the correlators $C_{rkQ}^{(u)} = 1/d$ for all the parameters considered.

The kernel of our entanglement witness for detecting states close to a generalized singlet state consists of $\hat{C}_k^{(u)}$'s and $\hat{C}_{rk}^{(u)}$'s and is defined explicitly by

$$\hat{C}_s = \sum_{u,k} \hat{C}_k^{(u)} + \hat{C}_{rk}^{(u)}. \quad (5.18)$$

The witness operator \mathcal{W}_s composed of \hat{C}_s can be utilized to detect arbitrarily high-dimensional singlet state with only two local measurement settings, and in particular

it is highly robust against to noise, independent of the number of dimensions of quantum system.

(b) Four-ququat supersingelt state. Let us progress towards another entanglement witness operator for detecting a four-ququat supersingelt state [69] with the state vector

$$|S\rangle = \frac{1}{\sqrt{24}} \sum_{(v_1 v_2 v_3 v_4) \in \mathbf{G}} (-1)^t |v_1 v_2 v_3 v_4\rangle, \quad (5.19)$$

where \mathbf{G} is the set which includes all permutations of the series (0123) and t is the number required to transpose pairs s.t. the series $(v_1 v_2 v_3 v_4)$ is arranged to (0123). The characters of the state $|S\rangle$ can be described by correlations between two subsystems of two ququats, and then we introduce the following operators to feature these properties:

$$\hat{C}_{k[ij|pq]}^{(u)} = [\hat{k}_{[ij]} - U(\hat{k}_{[ij]})] \otimes \hat{k}'_{[pq]}, \quad (5.20)$$

for $k = 0, \dots, 5$ and $u = 1, \dots, \beta_6$, where $\hat{0}_{[ij]} = \hat{0}\hat{1} + \hat{1}\hat{0}$, $\hat{1}_{[ij]} = \hat{0}\hat{2} + \hat{2}\hat{0}$, $\hat{2}_{[ij]} = \hat{0}\hat{3} + \hat{3}\hat{0}$, $\hat{3}_{[ij]} = \hat{1}\hat{2} + \hat{2}\hat{1}$, $\hat{4}_{[ij]} = \hat{1}\hat{3} + \hat{3}\hat{1}$, $\hat{5}_{[ij]} = \hat{2}\hat{3} + \hat{3}\hat{2}$, and $k+k' = 5$. For the four-lateral rotationally invariance of the supersinglet state [69], we have the following operators which are similar to $\hat{C}_{k[ij|pq]}^{(u)}$'s:

$$\hat{C}_{fk[ij|pq]}^{(u)} = [\hat{k}_{[ij]f} - U(\hat{k}_{[ij]f})] \otimes \hat{k}'_{[pq]f}, \quad (5.21)$$

where $\hat{k}_{[ij]f} = \sum_{v_i v_j} \hat{v}_{if} \otimes \hat{v}_{jf}$ has the same definition as $\hat{k}_{[ij]}$. It is clear that $C_{k[ij|pq]}^{(u)} = C_{fk[ij|pq]}^{(u)} = 1/6$. Then we have the central part of the witness

$$\hat{C}_S = \sum_{u,k} \sum_{\{[ij|pq]\}} \hat{C}_{k[ij|pq]}^{(u)} + \hat{C}_{fk[ij|pq]}^{(u)}, \quad (5.22)$$

where $\{[\cdot]\}$ denotes the set include different kinds of partitions of the four ququats and the number of elements of which is defined by n_c (2.8).

(c) Four-level four-qubit GHZ state. The next illustration of the criterion proposed is

given by an entanglement witness for a four-level four-partical GHZ state

$$|\Psi_{4 \times 4}\rangle = \frac{1}{2} \sum_{v=0}^3 |v\rangle^{\otimes 4}. \quad (5.23)$$

The witness consists of the operators of correlator as the following:

$$\hat{C}_{k[i|j|pq]}^{(u)} = [\hat{k} - U(\hat{k})] \otimes \hat{k}_{[j|pq]}, \hat{C}_{k[ij|pq]}^{(u)} = [\hat{k}_{[ij]} - U(\hat{k}_{[ij]})] \otimes \hat{k}_{[pq]}, \quad (5.24)$$

$$\hat{C}_{fk[i|j|pq]}^{(u)} = [\hat{k}_f - U(\hat{k}_f)] \otimes \hat{k}'_{[j|pq]f}, \hat{C}_{fk[ij|pq]}^{(u)} = [\hat{k}_{[ij]f} - U(\hat{k}_{[ij]f})] \otimes \hat{k}'_{[pq]f}, \quad (5.25)$$

for $k = 0, 1, 2, 3$ and $u = 1, \dots, \beta_4$, where $\hat{k}_{[j|pq]} = \hat{k} \otimes \hat{k} \otimes \hat{k}$, $\hat{k}_{[pq]} = \hat{k} \otimes \hat{k}$, $\hat{k}'_{[j|pq]f} = \sum_{j|pq} \hat{v}_{jf} \otimes \hat{v}_{pf} \otimes \hat{v}_{qf}$ with $v_j + v_p + v_q = k'$, $\hat{k}_{[ij]f} = \sum_{ij} \hat{v}_{if} \otimes \hat{v}_{jf}$ with $v_i + v_j = k$, $\hat{k}'_{[pq]f} = \sum_{pq} \hat{v}_{pf} \otimes \hat{v}_{qf}$ with $v_p + v_q = k'$, and $k + k' \doteq 0$. Then we have the kernel

$$\hat{C}_\Psi = \sum_{u,k} \sum_{\{[i|j|pq]\}} 3\hat{C}_{k[i|j|pq]}^{(u)} + 2\hat{C}_{fk[i|j|pq]}^{(u)} + \sum_{u,k} \sum_{\{[ij|pq]\}} 3\hat{C}_{k[ij|pq]}^{(u)} + 2\hat{C}_{fk[ij|pq]}^{(u)}. \quad (5.26)$$

(d) Many-qttrit GHZ states. The previous two examples show that via correlators the genuine four-party correlation of quantum states can be tested by two local measurement settings. This approach can be applied to cases involved more correlated qudits. For instance, to detect many-qttrit ($d = 3$) GHZ states of the representation:

$$|\Psi_{N \times 3}\rangle = \frac{1}{\sqrt{3}} \sum_{v=0}^2 |v\rangle^{\otimes N} \quad (5.27)$$

for $N = 3, 4, \dots, 7$, \mathcal{W}_{Φ_N} 's are comprised of operators that describe correlations between any two subsystems and given by

$$\hat{C}_{\Psi_{N \times 3}} = \sum_{u,k} \sum_{\{\mathbf{m}|\bar{\mathbf{m}}\}} 3\hat{C}_{k[\mathbf{m}|\bar{\mathbf{m}}]}^{(u)} + 2\hat{C}_{fk[\mathbf{m}|\bar{\mathbf{m}}]}^{(u)}, \quad (5.28)$$

where \mathbf{m} and $\bar{\mathbf{m}}$ signify subsystems with m qttrits and $N - m$ ones respectively, and $\hat{C}_{k[\mathbf{m}|\bar{\mathbf{m}}]}^{(u)}$ and $\hat{C}_{fk[\mathbf{m}|\bar{\mathbf{m}}]}^{(u)}$ are in terms of the eigenbasis $\{|v\rangle\}$ and $\{|v\rangle_f\}$ respectively and denote correlator operators for specifying correlations between the subsystem \mathbf{m} and $\bar{\mathbf{m}}$.

It is remarkable that these witnesses are very robust against to noise, independent of the number of qutrits.

5.5 Conclusion and outlook

We develop a phase-dependent condition of many-particle correlation for qudits. From which, we proposed novel entanglement witness operators with highly robustness for many qudits. These witnesses detect genuine entanglement close to two-qudit singlet, many-qudit GHZ, and supersinglet states [69]. They need only two local measurement settings when utilized in the present experiments. In particular, we reveal the essential elements of the GHZ paradoxes [19] and the generic Bell inequalities [18] for many qudits are comprised of the phase-dependent condition of correlations.

The framework of this work also helps to investigate the correlations of random variables, e.g., to define a new *coefficient of correlation* between random variables in the probability theory [125]. For two-bit cases, the new correlation coefficient is defined as

$$C(V_1, V_2) = \sum_{v_1, v_2=0}^1 (-1)^{M_2(v_1+v_2)} H(v_1, v_2), \quad (5.29)$$

where $H(v_1, v_2) = -\log_4 p(v_1, v_2)$, with $-1 \leq C(V_1, V_2) \leq 1$. If it is equal to zero, then V_1 and V_2 are said to be *uncorrelated*. Unlike the conventional one [125], there is no need to consider marginal probabilities. Further applications in statistics will be discussed in detail elsewhere.

Chapter 6

Entanglement purification

6.1 Background and motivation

The IBM [74, 75] and the Oxford [74–76] protocols are essential to entanglement purification for entangled-qubit pairs (see the introduction in Sec. 1.3). By using the IBM protocol, Alice and Bob can asymptotically regain the desired pure state, but they have to consume operation time in twirling the state in between each purification LOCC operation into a Werner state [126] whose fidelity relative to the desired pure state is always greater than $1/2$. Compared with the IBM protocol, the Oxford protocol can provide higher output yield, defined as the purified pairs per impure input pair, especially when the initial fidelity with respect to the desired pure state of the input state is close to $1/2$. In particular, the Oxford protocol is capable of purifying any state whose average fidelity with respect to at least one maximally entangled pure state is greater than $1/2$ and can be directly applied to purify states which are not necessarily of the Werner form. However, since the Oxford protocol occasionally may purify a pure state other than the desired one, i.e., it could yield two possible pure states, depending on the initial mixed state, Alice and Bob then are suggested to take efforts additional to the purification LOCC operations to transform the pure state with greatest component ($> 1/2$) in the input mixed state into the desired state; such action also costs operation time in the additional local unitary op-

erations and classical communications to identify the mixed state and thus consumes some pairs before the standard purification LOCC operations. The output yields induced by the IBM and Oxford protocols are rather poor, but can be increased somewhat provided both protocols are combined with hashing protocols, as described in Refs. [74, 75]. So far, there have been modified protocols dedicated to increasing the yield of an entanglement purification procedure, e.g., see Refs. [127–129].

Surveying on these modified methods, one finds that while inducing greater yields, they at the same time require more local unitary operations and classical communications in the reordering schemes and hashing protocols [74, 75] that are combined in the standard purification protocols. So, when comparing the performances of two protocols, say A and B, we can say protocol A performs better than B either when the yield of protocol A is greater than that of protocol B if both protocols cost equal operation times, or when protocol A requires less operation time than protocol B provided they induced equal yields. Instead of focusing on increasing the yield, in this chapter we are intended to propose an idea of establishing entanglement purification protocols in which the required operations are the fewest, when compared with the standard IBM and Oxford protocols. These protocols can purify a desired pure state by using the standard LOCC operations alone. When using these protocols, the mixed state to be purified needs not be transformed into the Werner state nor be reordered so that its fidelity with respect to the desired pure state is the largest. Furthermore, the protocols presented in this chapter in fact can provide better yields than that induced by the Oxford protocol [130].

6.2 Basic idea of entanglement purification

The standard purification LOCC operation considered in this chapter, as shown in Fig. 6.1, should be mentioned first. In each purification LOCC operation, Alice and Bob first perform local operations by operators U and U^* , which will be defined latter, respectively. Then Alice and Bob each performs a quantum control-not operation. They then measure

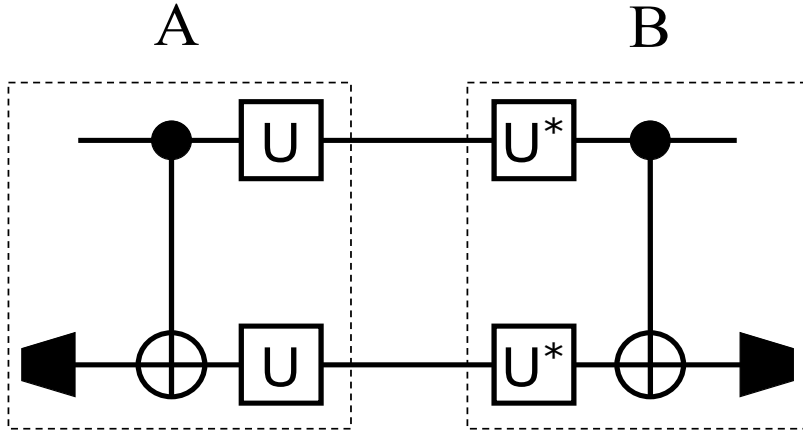


Figure 6.1: The standard purification LOCC operations including the local controlled-NOT operation, single qubit measurement, and local unitary operation in each party. Note that the classical communication is not shown in this figure.

the target qubits in the computational basis, and if the outcomes, communicated via classical channel, coincide they keep the control pair for the next step and discard the target pair. If the outcomes do not coincide, both pairs are discarded. In the purification LOCC operation, the state to be purified needs not be of a Werner form. We express the mixed state in the Bell basis $\{|\Phi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle\}$:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad (6.1)$$

where $|0\rangle$ and $|1\rangle$ form the computational basis of the two-dimensional space belonging to the EPR pairs. Let $\{a_0, b_0, c_0, d_0\}$ be the average initial diagonal elements of the density operator representing the mixed state before the protocol is begun with, and $\{a_r, b_r, c_r, d_r\}$ be the average diagonal elements of the surviving state after the r -th step. It can be shown that a purification LOCC operation in fact is relative to a nonlinear map, where the diagonal entries of the surviving state after the LOCC operation are nonlinear functions of those before the operation. Therefore the purification protocol considered in this work is composed of consecutive nonlinear maps of the Bell-diagonal elements used to transform an initial state asymptotically to a desired pure state. Suppose the state $|\Phi^+\rangle \langle \Phi^+|$ is the desired one to be purified through the purification, we then are willing

to map step by step the initial state $\{a_0, b_0, c_0, d_0\}$, where one of the elements should be greater than $1/2$, to converge to the desired attractor $\{1, 0, 0, 0\}$ as the step number r is sufficiently large. But the intrinsic property of the nonlinear map reveals that the desired attractor is not the only one, as can be seen in the article of Macchiavello [131], who has given the analytical convergence in the recurrence scheme of the QPA protocol.

The interesting nonlinear behavior of the recurrence scheme in a distillation protocol is dominantly influenced by the local unitary operations operators U and U^* applied by Alice and Bob in the purification LOCC operation. Generalized expression for U , controlled by two phases θ and ϕ , is given by

$$U(\theta, \phi) = \begin{bmatrix} \cos(\frac{\theta}{2}) & -e^{-i\phi} \sin(\frac{\theta}{2}) \\ e^{i\phi} \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix}. \quad (6.2)$$

It is clear that distinct choices of θ and ϕ will lead to different destinations of the protocol. For example, in using the original QPA protocol, Alice and Bob choose $\theta = \phi = \pi/2$, i.e., they apply the operator

$$U(\frac{\pi}{2}, \frac{\pi}{2}) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}. \quad (6.3)$$

In this case, one will have a map $\{a_{r-1}, b_{r-1}, c_{r-1}, d_{r-1}\} \rightarrow \{a_r, b_r, c_r, d_r\}$ according to the following relations:

$$\begin{aligned} a_r &= \frac{a_{r-1}^2 + b_{r-1}^2}{p_{r-1}}, b_r = \frac{2c_{r-1}d_{r-1}}{p_{r-1}}, \\ c_r &= \frac{c_{r-1}^2 + d_{r-1}^2}{p_{r-1}}, d_r = \frac{2a_{r-1}b_{r-1}}{p_{r-1}}, \text{ for } \theta = \phi = \pi/2, \end{aligned} \quad (6.4)$$

where $p_{r-1} = (a_{r-1} + b_{r-1})^2 + (c_{r-1} + d_{r-1})^2$ is the probability in the r th step that Alice and

Bob obtain coinciding outcomes in the measurements on the target pairs (so only $p_{r-1}/2$ of the pairs before the r th step is surviving after the step). Let us define the domains

$$\begin{aligned}
 \mathcal{D}_a &= \{a \in (0.5, 1]; a + b + c + d = 1\}, \\
 \mathcal{D}_b &= \{b \in (0.5, 1]; a + b + c + d = 1\}, \\
 \mathcal{D}_c &= \{c \in (0.5, 1]; a + b + c + d = 1\}, \\
 \mathcal{D}_d &= \{d \in (0.5, 1]; a + b + c + d = 1\}, \\
 \mathcal{D}_{ab} &= \mathcal{D}_a \cup \mathcal{D}_b, \\
 \mathcal{D}_{cd} &= \mathcal{D}_c \cup \mathcal{D}_d, \\
 \mathcal{D}_{abcd} &= \mathcal{D}_a \cup \mathcal{D}_b \cup \mathcal{D}_c \cup \mathcal{D}_d.
 \end{aligned} \tag{6.5}$$

In what follows we will consider the case that an initial mixed state to be purified is in the applicable \mathcal{D}_{abcd} because any state $\rho \in \mathcal{D}_{abcd}$ is distillable. It has been proved [131] that, for the Oxford protocol, an initial state in the domain \mathcal{D}_{ab} will eventually be mapped to converge to the attractor $\{1, 0, 0, 0\}$ representing the desired pure state $|\Phi^+\rangle\langle\Phi^+|$. While if the initial state is in the domain \mathcal{D}_{cd} , then it will be mapped to approach another attractor $\{0, 0, 1, 0\}$, or the pure state $|\Psi^+\rangle\langle\Psi^+|$. In the end, according to Ref. [76], using the QPA protocol, Alice and Bob will regain the desired pure state from any state $\rho \in \mathcal{D}_{abcd}$ provided they first take efforts additional to the standard purification LOCC operations to transform the pure state $|\Psi^+\rangle\langle\Psi^+|$, or $|\Phi^-\rangle\langle\Phi^-|$, into the desired state $|\Phi^+\rangle\langle\Phi^+|$ if the input state is in the domain \mathcal{D}_{cd} . Meanwhile, such efforts also have meaningful implication as if the QPA is considered to be combined with the hashing protocol [74, 75] to improve its output yield. These tedious transformations cannot be avoided even when the input state is already in the domain \mathcal{D}_{ab} , because Alice and Bob initially do not have an idea about whether the input state is exactly in the domain \mathcal{D}_{ab} or \mathcal{D}_{cd} . For example, if the input state has the element $c_0 = 0.7$, then Alice and Bob should transform the state $|\Psi^+\rangle\langle\Psi^+|$ into $|\Phi^+\rangle\langle\Phi^+|$ before the purification procedure so that the mixed state in turn will have the element $a_0 = 0.7$.

As another example, if Alice and Bob choose $\theta = \pi/2$ and $\phi = 0$, then they have the operator

$$U(\pi/2, 0) = \mathbf{XH} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad (6.6)$$

where \mathbf{X} is quantum NOT gate and \mathbf{H} is the Hadamard transformation. Accordingly, in this case, the recurrence scheme is described by

$$\begin{aligned} a_r &= \frac{a_{r-1}^2 + c_{r-1}^2}{p_{r-1}}, b_r = \frac{2b_{r-1}d_{r-1}}{p_{r-1}}, \\ c_r &= \frac{b_{r-1}^2 + d_{r-1}^2}{p_{r-1}}, d_r = \frac{2a_{r-1}c_{r-1}}{p_{r-1}}, \text{ for } \theta = \pi/2, \phi = 0, \end{aligned} \quad (6.7)$$

where $p_{r-1} = (a_{r-1} + c_{r-1})^2 + (b_{r-1} + d_{r-1})^2$. It should be mentioned here that the relations (6.7) can also be resulted from the utility of Hadamard transformation only, i.e., $U = \mathbf{H}$, but this transformation does not belong to the $SU(2)$ operator defined in (6.2). Although the analytical convergency in the recurrence scheme (6.7) has not yet been proved, we find that an initial state in some domain $\mathcal{D}_u \subset \mathcal{D}_{abcd}$, which is not yet defined, will be mapped to approach the periodic attractor representing a state interchanging step by step between $\{0.5, 0, 0, 0.5\}$ and $\{0.5, 0, 0.5, 0\}$, while a state in the domain \mathcal{D}_u^c , where $\mathcal{D}_u^c \cup \mathcal{D}_u = \mathcal{D}_{abcd}$, will be mapped to converge to the fixed attractor $\{1, 0, 0, 0\}$, as wanted. For example, one can easily check to see that the initial state $\{0.1, 0.2, 0.6, 0.1\}$ will be mapped to converge to the fixed attractor but the initial state $\{0.2, 0.1, 0.6, 0.1\}$, on the other hand, will be mapped to approach the mentioned periodic attractor. So a protocol in which the operator \mathbf{XH} is used, unlike the QPA protocol, will not guarantee to purify pure maximally entangled pairs.

6.3 Entanglement purification with a two-map protocol

In this work, we call a protocol a one-map protocol if Alice and Bob each uses only one single local operator in all the purification LOCC operations, such as the IBM and Oxford protocols. From the above examples we realize that if only the standard purification LOCC operations are implemented, all one-map protocols will encounter the same situation that there is always another attractor in addition to the desired one, $\{1, 0, 0, 0\}$, for a state $\rho \in \mathcal{D}_{abcd}$ to be mapped to converge to. This situation thus becomes the ultimate limitation for the one-map algorithm. Therefore, in this work, we will present a viewpoint of hybrid maps for a purification protocol and show the fixed state $\{1, 0, 0, 0\}$ can be the only attractor for an initial state $\rho \in \mathcal{D}_{abcd}$ to be mapped to approach. The simple idea can be interpreted briefly. If we have known a one-map protocol, say, controlled by θ_1 and ϕ_1 , in which a state ρ belonging to some defined domain $\mathcal{D}_1 (\subset \mathcal{D}_{abcd})$ can be mapped to approach the fixed attractor $\{1, 0, 0, 0\}$, then all we have to do is to find another map, controlled by θ_0 and ϕ_0 , in which a state $\rho \in \mathcal{D}_{abcd}$ will be mapped on to a subdomain of the defined \mathcal{D}_1 . This kind of protocol is what we call a two-map protocol, which can ensure Alice and Bob to regain the desired pure state $|\Phi^+\rangle \langle \Phi^+|$ all by using the standard purification LOCC operations.

For the idea we have just presented, the most difficult task is the definition of the domain \mathcal{D}_1 . Fortunately, Macchiavello [131] has defined the domain \mathcal{D}_1 for the QPA protocol, in which $\mathcal{D}_1 = \mathcal{D}_{ab}$, as defined in (6.5). Therefore the QPA protocol is so far the most convenient one-map protocol to be improved by our idea. As to the one-map protocol described in (6.7), on the contrast, no definition of the corresponding \mathcal{D}_1 have been proved. A concrete example of our idea, however, will utilize these two one-map protocols. That is, in this example the option $\theta_1 = \pi/2$ and $\phi_1 = \pi/2$ will be chosen and accordingly the choice $\theta_0 = \pi/2$ and $\phi_0 = 0$ follows. We begin with the derivation of $(1 - 2a_r)$ and $(1 - 2c_r)$ for $\theta_0 = \pi/2$ and $\phi_0 = 0$. According to (6.7), we have

$$1 - 2a_r = \frac{(1 - 2a_{r-1})(1 - 2c_{r-1})}{p_{r-1}}, \quad 1 - 2c_r = \frac{(1 - 2b_{r-1})(1 - 2d_{r-1})}{p_{r-1}}, \quad (6.8)$$

for arbitrary positive integer r . It is now clear to find that, since $p_{r-1} > 0$, when $a_0 > 1/2$ or $c_0 > 1/2$, then after the first purification LOCC operation we have $a_1 > 1/2$, while as $b_0 > 1/2$ or $d_0 > 1/2$, then we in turn have $c_1 > 1/2$, which consequently implies $a_2 > 1/2$ after the second purification LOCC operation. As a result, we know by now that using the one-map protocol (6.7), we can always in two steps map an initial state $\rho \in \mathcal{D}_{abcd}$ on to the domain \mathcal{D}_a , which is exactly a subdomain of $\mathcal{D}_1 (= \mathcal{D}_{ab})$ for the standard QPA protocol. Now, we have come to the two-map protocols we wish to present in this work. Using this two-map protocol (symbolized by TM1), Alice and Bob have an agreement that in the first two steps of the purification procedure, they will apply the operators $U(\pi/2, 0)$ and $U^*(\pi/2, 0)$, respectively, to map a state $\rho \in \mathcal{D}_{abcd}$ on to the domain $\mathcal{D}_a = \{a \in (0.5, 1], a + b + c + d = 1\}$, and then they will apply the standard QPA operators $U(\pi/2, \pi/2)$ and $U^*(\pi/2, \pi/2)$ to purify the surviving state to the desired state $|\Phi^+\rangle \langle \Phi^+|$ in the rest purification LOCC operations. Interestingly, an alternative two-map protocol (symbolized by TM2) can be used as well, in which the operators $U(\pi/2, 0)$ and $U^*(\pi/2, 0)$ are applied only at the second purification LOCC operation, since after the first LOCC operation, in which the QPA operators $U(\pi/2, \pi/2)$ and $U^*(\pi/2, \pi/2)$ are used, the state has been mapped on to the domain \mathcal{D}_{ac} [131].

Apparently, our protocols TM1 and TM2 are composed of only the standard purification LOCC operations, without using any additional local operations and classical communications in transforming the mixed state into a Werner state, as needed in the IBM protocol, or transforming one of the Bell states whose fidelity is the largest into the desired pure state $|\Phi^+\rangle$ in advance of the Oxford operations. Therefore the fewest operations are required in our purification algorithms, as compared with the IBM and Oxford protocols. Furthermore, when comparing the output yields and the fidelities (or purities)

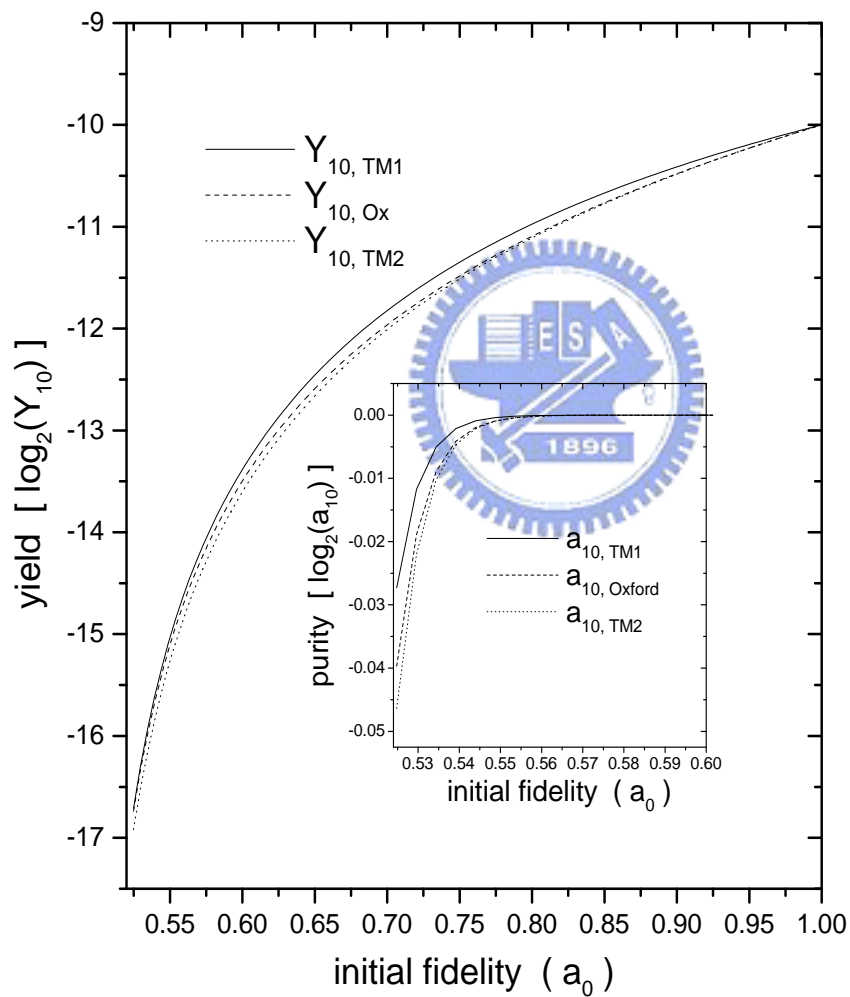


Figure 6.2: The variations of the yield and the comparing purity (in the inserted diagram) at ten times of the recurrence method.

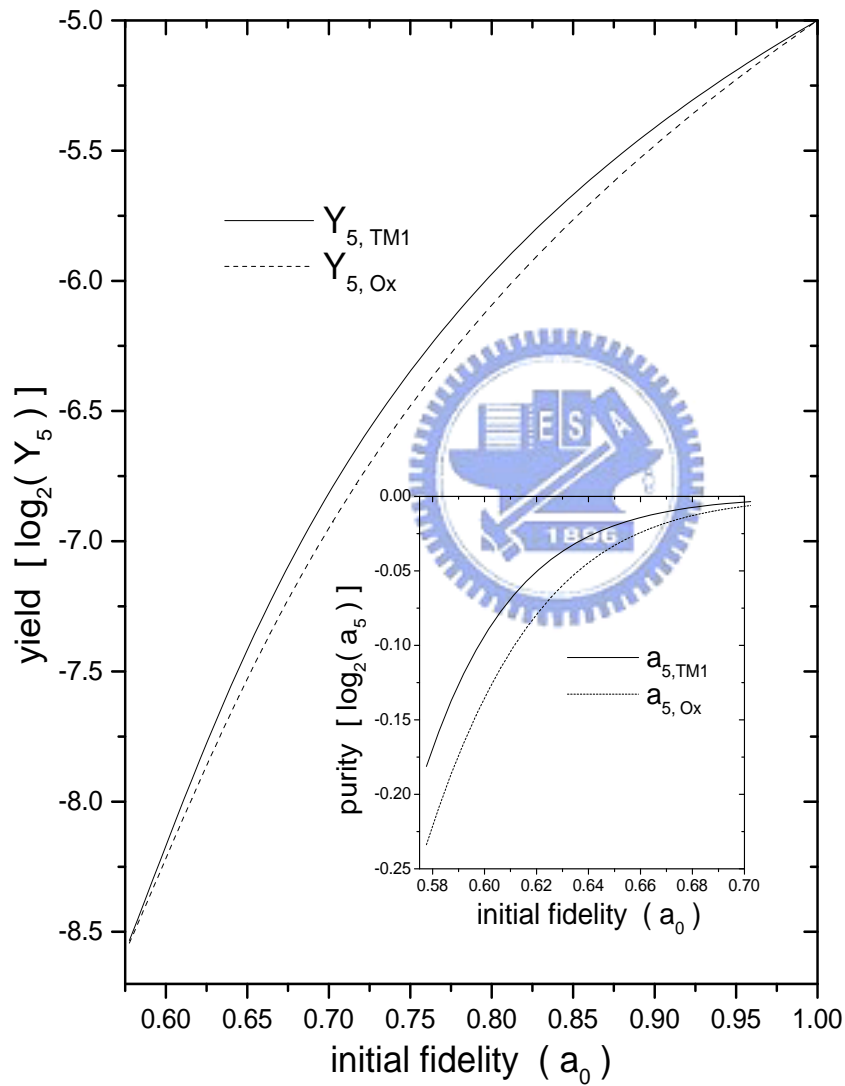


Figure 6.3: The variations of the yield and the comparing purity (in the inserted diagram) at five times of the recurrence method.

produced by the IBM, the Oxford, and our two-map protocols, we find the protocol TM1 can provide better yields and fidelities than the Oxford protocol (which performs better than the IBM protocol), while the protocol TM2 can perform almost equally to the Oxford protocol, although this is not the primary purpose of this work. In our numerical simulations, the yield, or the fraction of the surviving pairs, defined by $Y_r = p_0 p_1 \dots p_{r-1} (2^{-r})$, where r denotes the iteration number, was first computed up to $r = 10$ for each input state to be purified. The variations of the yield as functions of the initial fidelity a_0 are shown in Fig. 6.2, in which (and also in the following figures) each yield (and each purity) was the average value computed over ten thousand random states possessing the same initial fidelity. The corresponding purities after the ten iterations are also shown in Fig. 6.2. It is shown that although, after the ten iterations, the resulted purities produced by using the Oxford, TM1, and TM2 are high, the yields of them are rather poor, especially when the initial fidelity is close to $1/2$.

The yield, however, can be further improved by combining the recurrence method with the hashing protocol [74, 75] as long as the purity is high enough (e.g. higher than 0.8107 for a Werner state) when the recurrence scheme is performed in only a few iterations. In Fig. 6.3 we show the yields Y_5 and the correspond purities a_5 produced by the Oxford and the TM1 protocols after five iterations, respectively. This figure shows that when the initial fidelities are greater than some specific values near $1/2$ for both cases (of course the specific fidelities can be lowered if the iteration is increased), the hashing protocols then are applicable after the five iterations in running the recurrence schemes. Fig. 6.3 shows that after the five iterations, the surviving fraction $Y_{5, TM1}$ and the corresponding purity $a_{5, TM1}$, produced by the the TM1 protocol are slightly higher than the surviving fraction $Y_{5, Ox}$ and the purity $a_{5, Ox}$, which are resulted from using the Oxford protocol. The slight differences in Y_5 and a_5 , however, can induce significant difference between the improved yields when the hashing protocol is switched on after the five iterations. The evidence can be seen in Fig. 6.4, in which both the improved yields $Y'_{5, TM1}$ and $Y'_{5, Ox}$ and the ratio of the improved yields ($Y'_{5, TM1}/Y'_{5, Ox}$) as functions of the initial fidelity are shown; the

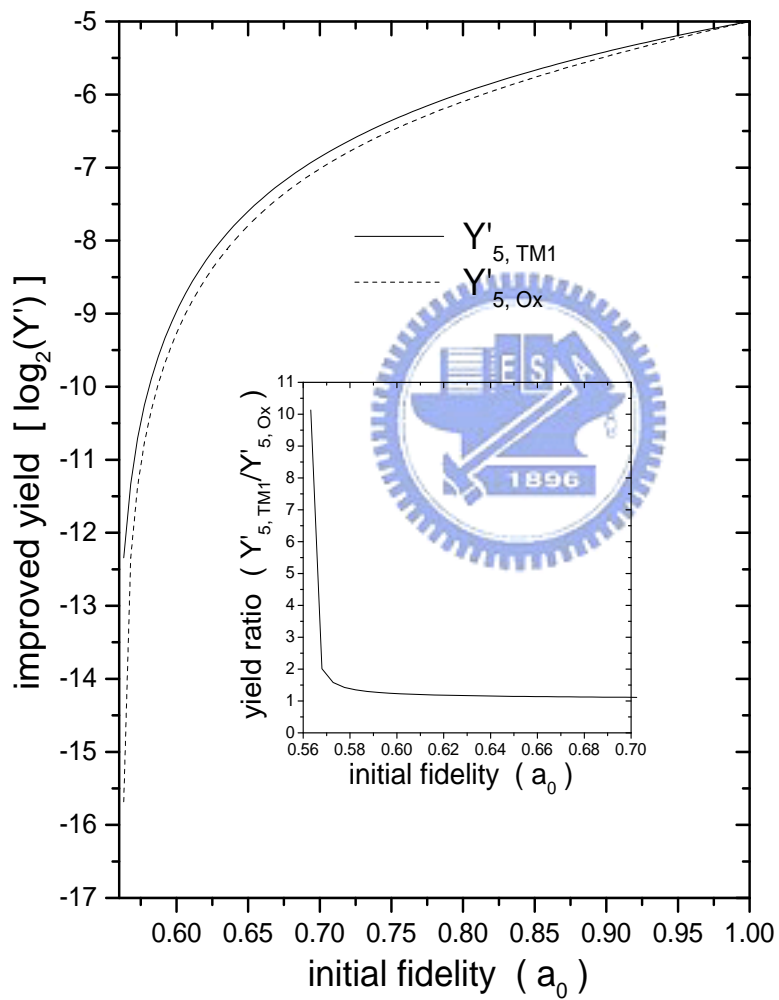


Figure 6.4: The variations of the improved yields $Y'_{5, TM1}$ and $Y'_{5, Ox}$ and the comparing ratio ($Y'_{5, TM1}/Y'_{5, Ox}$) (in the inserted diagram).

improved yield is defined by $Y'_r = Y_r(1 - S(\rho_r))$, where $S(\rho_r)$ is the von Neumann entropy of the surviving mixed state ρ_r . It is clearly shown in Fig. 6.4 that the ratio $Y'_{5, TM1}/Y'_{5, Ox}$ becomes greater as the initial fidelity is closer to $1/2$.

6.4 Conclusion

In the recurrence scheme of a one-map entanglement purification protocol, the nonlinear behavior of the four Bell-diagonal elements of the density matrix representing the mixed state to be purified reveals that there is always another attractor other than the desired fixed attractor. This indicates that not all the distillable input state can be purified to the desired maximally entangled pure state all by the standard purification LOCC operations in a one-map protocol. Therefore some tedious efforts additional to the purification LOCC operations are needed in using the typical IBM and Oxford protocols to purify a desired pure state from any distillable state. The proposed two-map purification protocols TM1 and TM2, on the contrast, can guarantee that all the distillable input states can be purified to the desired pure state all by the standard purification LOCC operations. That an entanglement purification can be accomplished all by the standard purification LOCC operations is crucially important to a significant improvement for the purification process. By such improvement, we then do not have to identify the mixed state and consequently do not consume any pairs before the purification LOCC operations. The proposed two-map protocols perform better than the one-map IBM and Oxford protocols in the sense that they require the least operation times in yielding a same amount of useful EPR pairs. Surprisingly, the protocol TM1 is found able to induce higher yields and purities than the Oxford protocol. This is crucially important as the hashing protocol is combined with the recurrence algorithm to improve the output yield. The proposed two-map protocols, however, like the standard IBM and Oxford protocols, should be implemented if the initial state possesses a fidelity very close to $1/2$ only after enhancing the state's fidelity. For example, it has been shown [132] that only inseparable two-qubit state with "free"

entanglement, however small, can be distillable to a pure form by using local filtering [133, 134] to enhance the state's fidelity first. An interaction with the environment [135] can even be allowed to enhance the fidelity of a quantum teleportation. The fidelity enhancement, however, is not an issue to be concerned with in this work.



Chapter 7

Quantum error-correcting codes and entanglement purification

7.1 Introduction

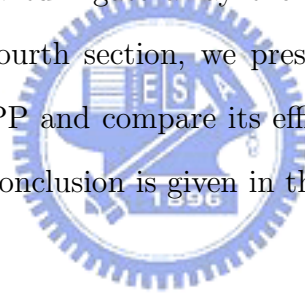


The five-qubit quantum error-correcting code (QECC) that protects a qubit of information against general one-qubit errors is one of special interests for quantum computations. It has been proven to be the best and smallest block code [78]. It is also a perfect non-degenerate code because it saturates the quantum Hamming bound [136] and thus is capable of correcting all one-qubit errors with minimum number of extra qubits. Laflamme *et al.* [77] and Bennett *et al.* [74] independently showed the first five-qubit QECCs. Recent developments of most QECCs are attributed to the stabilizer formalism [117, 137, 138]. In the work of Laflamme *et al.* [77], the five-qubit error correction is described to perform in a rather simple procedure. The initial one-qubit information, as accompanied with four extra qubits in the state $|0\rangle$, is encoded by a circuit representing a sequence of single-qubit Pauli operations and two-qubit controlled Pauli operations. Then, after the interaction of environment that causes generic one-qubit errors, the polluted five-qubit state is decoded by running the same encoder circuit in a reverse order. Eventually, the tensor product state of the four extra qubits is measured in the computational basis

($|0\rangle$ and $|1\rangle$) to decide the corresponding final Pauli operation for recovering the original state of the information carried qubit. By computer search, Braunstein and Smolin [139] found a simplified encoder circuit which can encode the one-qubit information in 24 laser pulses. For the stabilizer code, however, the initial one-qubit information is encoded by the actions of all the operators belonging to the group generated by the stabilizers. The encoded five-qubit state is then allowed to be affected by generic one-qubit errors followed by measurements of the stabilizer observables to detect and correct the qubit on which the error has occurred. The five-qubit stabilizer code has been experimentally implemented using nuclear magnetic resonance by Knill *et al.* [140].

The five-qubit QECC introduced by Bennett *et al.* [74] was derived from a restricted one-way entanglement purification protocol (1-EPP) which purifies one good Bell state from a noisy block of five Bell states. The entanglement purification protocol (EPP) allows Alice and Bob to perform local unitary transformations and measurements and even allows them to coordinate their actions through one-way or two-way classical communication. It, however, does not allow Alice and Bob to perform non-local actions nor to transmit fresh quantum states from one to the other. An EPP involving two-way communication is called a two-way EPP (2-EPP), in which both Alice and Bob need to know the results of measurement from each other. Typical 2-EPPs include the IBM protocol [75] and the Oxford protocol [76], which also belong to the recurrence method. On the other hand, a one-way EPP (1-EPP) requires only Alice to send her measurement result through classical channel to Bob, who when combining it with his own result can decide a following action to perform. Thus, the 1-EPP can produce pure maximally entangled pairs which are separated both in space and in time. The hashing protocol [74] and the breeding protocol [75] are examples of the 1-EPP. In fact, it can be shown that the Bennett *et al.* protocol is equivalent to the error correction of Laflamme *et al.* However, the QECC of Bennett *et al.* can be well derived so that it requires a simpler circuit for both encoding and decoding than the original one reported by Laflamme *et al.*. Bennett *et al.* suggested to use a Monte Carlo search program for deriving the QECC.

In realistic situations, to reduce the number of two-qubit gates necessary in the encoder-decoder circuit is significantly important for reliable five-qubit QECCs because two-qubit operations could be the more difficult ones to be implemented in a physical apparatus [51]. This work thus is motivated to derive five-qubit, single-error corrections which can be performed by using the least number of two-qubit operations in their encoder-decoder networks [141]. The QECC presented as an example herein is derived analytically from the restricted 1-EPP proposed by Bennett *et al.* [74] and its encoder-decoder circuit contains only six controlled-NOT (CNOT) gates and three single-qubit operations. The restricted 1-EPP therefore is depicted first in the next section. In the third section, we describe the systematic method for deriving 1-EPP in detail. A concrete example for the simplest quantum gate array then will be given to show the capacity of the present method. In fourth section, we present the coding circuit which is converted directly from the 1-EPP and compare its efficiency with those of several existent encoder-decoder circuits. A conclusion is given in the final section.



7.2 The 5-EPR-pair single-error-correcting code

Suppose there exists a finite block-size 1-EPP which distills one good pair of spins in a specific Bell state from a block of five pairs, and no more than one of the five pairs is subjected to noise. When this 1-EPP is combined with a teleportation protocol, two parties, Alice and Bob, can transmit quantum states reliably from one to the other. The combination of the 1-EPP and teleportation protocol therefore is equivalent to a QECC. The 1-EPP considered herein is schematically depicted in Fig. 7.1. Suppose Alice is the encoder, Bob the decoder, and the Bell state $\Phi^+ = (|00\rangle + |11\rangle)/\sqrt{2}$ is the good state to be purified. Alice and Bob are supposed to be provided with five pairs of spins in the state Φ^+ by a quantum source (QS). However, they actually share five Bell states in which generic errors have or have not occurred on at most one Bell state due to the presence of noise N_B in the quantum channel via which the pairs are transmitted. The noise models

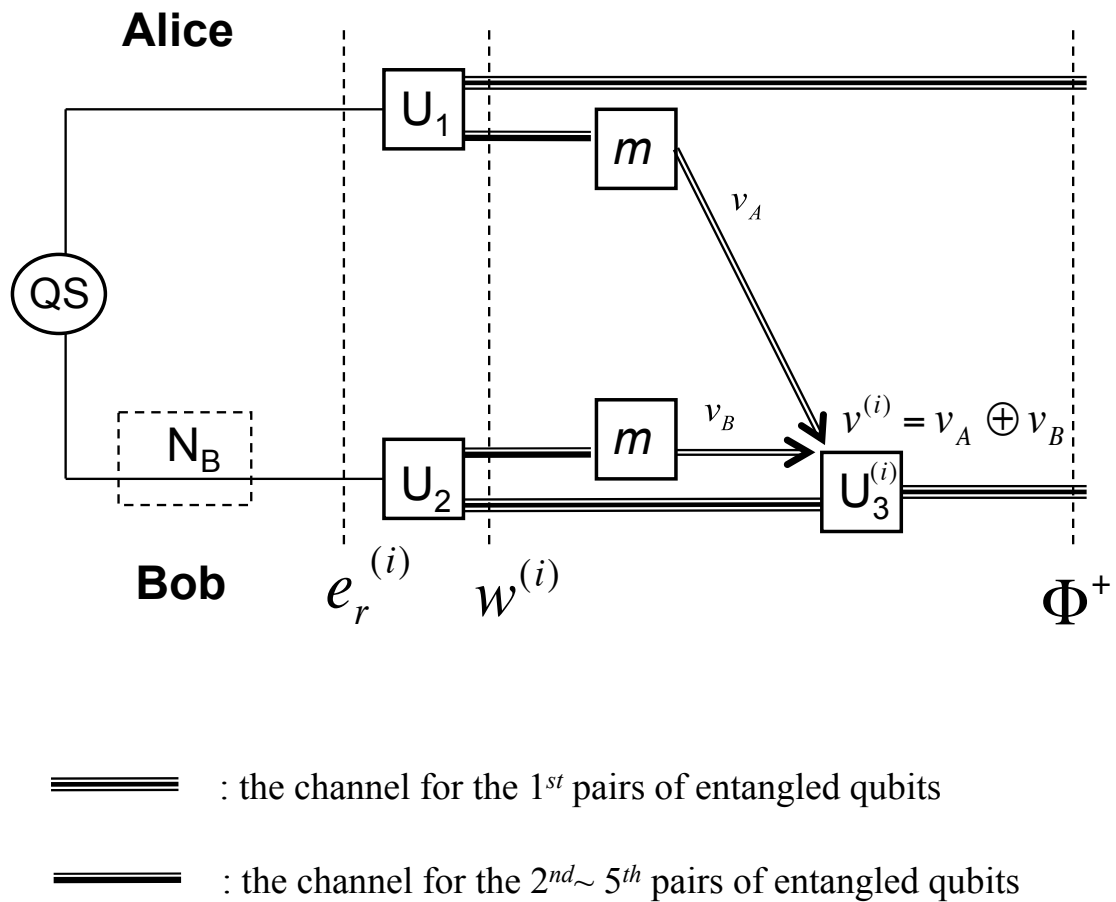


Figure 7.1: The 1-EPP with notations used in the context. Alice performs U_1 and m and then sends her classical result (v_A) to Bob. Bob performs U_2 and m , and then combines his own result (v_B) and Alice's to control a final operation $U_3^{(i)}$.

are assumed to be one-sided [74] and can cause the good Bell state Φ^+ to become one of the incorrect Bell states

$$\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \Psi^\pm = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (7.1)$$

The good Bell state Φ^+ can become one of the erroneous Bell states expressed in (1) if it is subjected to either a phase error ($\Phi^+ \rightarrow \Phi^-$), an amplitude error ($\Phi^+ \rightarrow \Psi^+$), or both ($\Phi^+ \rightarrow \Psi^-$) [78, 142]. When performing the 1-EPP, Alice and Bob have a total of 16 error syndromes to deal with. The collection of error syndromes includes the case that none of the five pairs has been subjected to errors and the 15 cases in which one of the five pairs has been subjected to one of the three types of error. The strategy of Alice and Bob is to perform a sequence of unilateral and bilateral unitary operations (as shown in Fig. 7.1, U_1 and U_2 performed by Alice and Bob, respectively) to transform the collection of the 16 error syndromes to another collection that can provide information about the errors subjected by their particles. Suppose the state of the first pair in the block is to be recovered. After performing the sequence of their operations (U_1 and U_2 respectively), Alice and Bob, should then perform local measurements on their respective halves of the second to fifth pairs. Alice sends her result via classical channels to Bob who then performs the Pauli operation U_3 to recover the original state of the first pair conditionally on both Alice's and his results. The ultimate requirement of these results of final measurement is that each and every of them should be distinguishable from the others. In other words, there should be 16 distinct measurements obtained from the aforementioned transformation of the error syndrome. The main issue now is that the sequence of unilateral and bilateral unitary operations performed by the two parties to transform the error syndrome should be well designed so the requirement just mentioned can be fulfilled.

To arrange the sequence of operations, basic concepts of linear algebra are used. The

CHAPTER 7. QUANTUM ERROR-CORRECTING CODES AND ENTANGLEMENT PURIFICATION

Table 7.1: The correspondence among the error syndrome $e_r^{(i)}$ ($E_r^{(i)}$), the codeword $w^{(i)}$ ($W^{(i)}$), the measurement result $v^{(i)}$, and the Pauli operation $U_3^{(i)}$ controlled by the measurement result in the restricted 1-EPP (five-qubit QECC) applying the encoder-decoder circuit shown in Fig. 7.3.2 (Fig. 7.4)

| i | $e_r^{(i)}, E_r^{(i)}$ | $w^{(i)}, W^{(i)}$ | $v^{(i)}$ | $U_3^{(i)}$ |
|-----|------------------------|--------------------|-----------|-------------|
| 0 | 00 00 00 00 00 | 00 00 00 00 00 | 0000 | I |
| 1 | 10 00 00 00 00 | 11 00 00 01 01 | 0011 | σ_y |
| 2 | 01 00 00 00 00 | 01 00 01 01 00 | 0110 | σ_x |
| 3 | 11 00 00 00 00 | 10 00 01 00 01 | 0101 | σ_z |
| 4 | 00 10 00 00 00 | 00 01 00 00 01 | 1001 | I |
| 5 | 00 01 00 00 00 | 00 11 01 01 00 | 1110 | I |
| 6 | 00 11 00 00 00 | 00 10 01 01 01 | 0111 | I |
| 7 | 00 00 10 00 00 | 11 01 10 01 01 | 1011 | σ_y |
| 8 | 00 00 01 00 00 | 00 00 01 00 00 | 0100 | I |
| 9 | 00 00 11 00 00 | 11 01 11 01 01 | 1111 | σ_y |
| 10 | 00 00 00 10 00 | 10 01 00 10 00 | 1000 | σ_z |
| 11 | 00 00 00 01 00 | 00 00 00 01 00 | 0010 | I |
| 12 | 00 00 00 11 00 | 10 01 00 11 00 | 1010 | σ_z |
| 13 | 00 00 00 00 10 | 00 00 00 00 01 | 0001 | I |
| 14 | 00 00 00 00 01 | 01 11 01 00 10 | 1100 | σ_x |
| 15 | 00 00 00 00 11 | 01 11 01 00 11 | 1101 | σ_x |

four Bell states Φ^\pm and Ψ^\pm are first labeled by two classical bits, namely,

$$\Phi^+ = 00, \Phi^- = 10, \Psi^+ = 01, \Psi^- = 11. \quad (7.2)$$

The right, low-order or amplitude bit identifies the Φ/Ψ property of the Bell state, while the left, high-order or phase bit identifies the $+/-$ property. Note that the combined result of the local measurements obtained by Alice and Bob on a Bell state is revealed by the Bell state's low or amplitude bit. In the representation of the high-low bits, each error syndrome thus is expressed as a ten-bit codeword, e.g., the error syndrome $\Phi^+\Psi^-\Phi^+\Phi^+\Phi^+$ is written as 00 11 00 00 00. Codewords of the error syndrome, denoted by $e_r^{(i)}$, $i = 0, 1, \dots, 15$, are listed in Table 7.1. The effect of the sequence of unilateral and bilateral unitary operations performed by Alice and Bob is to map the codewords $e_r^{(i)}$ onto another collection of ten-bit codewords $w^{(i)}$. If both the codewords $e_r^{(i)}$ and $w^{(i)}$ are

written as column vectors in the ten-dimensional Boolean-valued ($\in \{0, 1\}$) space, then the mapping $e_r^{(i)} \rightarrow w^{(i)}$ can be simply expressed by a matrix equation

$$w^{(i)} = \mathbf{M}e_r^{(i)}, \quad (7.3)$$

provided that the mapping is confined to $w^{(0)} = e_r^{(0)} (= 00\ 00\ 00\ 00\ 00)$. The four error syndromes, $e_r^{(3k)}$, $e_r^{(3k-1)}$, $e_r^{(3k-2)}$, and $e_r^{(0)}$, corresponding to a common erroneous pair, form a group and are characterized by

$$e_r^{(3k-2)} \oplus e_r^{(3k-1)} = e_r^{(3k)}, k = 1, 2, \dots, 5, \quad (7.4)$$

where k enumerates the erroneous pair and \oplus is the addition modulo 2. Accordingly, the 16 codewords $w^{(i)}$ should be subdivided into five corresponding groups, each of which has $w^{(3k)}$, $w^{(3k-1)}$, $w^{(3k-2)}$, and $w^{(0)}$, and holds the relation

$$w^{(3k-2)} \oplus w^{(3k-1)} = w^{(3k)}, k = 1, 2, \dots, 5. \quad (7.5)$$

Therefore the matrix \mathbf{M} can be simply expressed by a 10×10 matrix, such as

$$\mathbf{M} = [w^{(1)}w^{(2)}w^{(4)}w^{(5)}w^{(7)}w^{(8)}w^{(10)}w^{(11)}w^{(13)}w^{(14)}], \quad (7.6)$$

in accordance with the arrangement of error syndromes listed in Table 7.1. The first two rows of \mathbf{M} represent the states of the pair to be recovered, and the 4th, 6th, 8th, and 10th rows represent the low bits of the second to fifth Bell states and thus construct the four-bit codewords for the measurement results $v^{(i)}$. The measurement result $v^{(i)}$ of course is also characterized by

$$v^{(3k-2)} \oplus v^{(3k-1)} = v^{(3k)}, k = 1, 2, \dots, 5, \quad (7.7)$$

in accordance with relations (7.4) and (7.5). In the language of linear algebra, the action of

the sequence of unilateral and bilateral unitary operations that accounts for the mapping $e_r^{(i)} \rightarrow w^{(i)}$ is to perform a sequence of elementary row operations on the 10×10 identity matrix $\mathbf{1}$ to reduce it to the matrix \mathbf{M} . In this spirit, Bennett *et al.* [74] have undertaken a Monte Carlo numerical search program to find out suitable solutions for matrix \mathbf{M} and their corresponding encoder-decoder networks. Basically, the approach implemented by Bennett *et al.* is a tedious numerical method of trial and error performing the transformation $\mathbf{1} \rightarrow \mathbf{M}$ subjected to a *forward* sequence of local operations. In this work, we will present an analytical method for creating \mathbf{M} implemented in the present QECC. The present method will be described in detail in the next section.

7.3 Analytical technique for simplification of the encoder-decoder circuit for a perfect five-qubit error correction



7.3.1 Theory

The unilateral and bilateral unitary operations performed in the 1-EPP in fact are their own inverse transformations, so if the sequence of operations is run in the reverse order, then the inverse transformations $\mathbf{M} \rightarrow \mathbf{1}$ is accomplished. In the spirit of inverse transformation, it thus allows us to derive all appropriate versions of \mathbf{M} and the corresponding encoder-decoder networks by following an analytical way. More importantly, for a derived \mathbf{M} , rearranging the sequence of row operations on the same inverse transformation $\mathbf{M} \rightarrow \mathbf{1}$ will help in constructing its simplest encoder-decoder circuit.

An elementary row operation corresponds to a basic unilateral or bilateral unitary operation. In the present protocol, Alice and Bob are confined to perform only three basic unitary operations because these operations are necessary and sufficient for the elementary row operations needed to achieve the mapping $\mathbf{M} \rightarrow \mathbf{1}$, and vice versa. These

basic operations are: (1) a bilateral CNOT (BXOR), which performs the bit change $(x_S, y_S)(x_T, y_T) \rightarrow (x_S \oplus x_T, y_S)(x_T, y_S \oplus y_T)$, where the subscripts S and T denote the source and target pairs, respectively; (2) a bilateral $\pi/2$ -rotation B_y , which performs $(x, y) \rightarrow (y, x)$; and (3) a composite operation $\sigma_x B_x$, which performs $(x, y) \rightarrow (x, x \oplus y)$. The unitary Pauli operation σ_x performs a π -rotation of Alice or Bob's spin about the x -axis, while the bilateral operation B_x (B_y) performs a $\pi/2$ -rotation of both Alice and Bob's spins about the x (y)-axis. The unilateral operations are defined as those operators performed by Alice or Bob but not both. The bilateral operations are represented by a tensor product of one part of Bob and the same part of Alice. Note that the bilateral CNOT is performed such that the source qubits of Alice and Bob belong to a common pair, and the target qubits belong to another common pair.

The information obtained through local measurements and one-way communications can only deduce the low bit of a Bell pair, and the original state of the first Bell pair can only be recovered by the low-bit information. Then, for a successful 1-EPP, or its equivalent QECC, each and every measurement result $v^{(i)}$ is required to be distinguishable from the others, so the collection of $v^{(i)}$ in fact should contain all elements in the 4-dimensional Boolean-valued space. To perform the aforementioned inverse transformation $\mathbf{M} \rightarrow \mathbf{1}$, the codewords of measurement result are first arranged according to relations

(7.7) and the matrix \mathbf{M} can be assumed as

$$\mathbf{M} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 & c_{10} \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_9 & f_{10} \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (7.8)$$

It should be noted that the arrangement of the results of measurements shown in the above matrix is only one of the possible choices. By performing a sequence of row operations corresponding to the basic unitary operations, the assumed matrix \mathbf{M} (7.8) actually is allowed to be reduced to one of all the alternatives akin to the identity matrix $\mathbf{1}$, and a suitable encoder-decoder circuit is constructed accordingly. The alternatives akin to the identity $\mathbf{1}$ are those obtained by 1– permuting column vectors within one of the five sets of two column vectors ($x^{(3k-2)}$ and $x^{(3k-1)}$, $k = 1, 2, \dots, 5$), or 2– adding one column to the other within each of the groups, or 3– performing both actions. For example, an

alternative could be

$$\mathbf{1}_{akin} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (7.9)$$

When the derivation of \mathbf{M} is done, the alternative akin to $\mathbf{1}$ is then converted back to the identity $\mathbf{1}$ by well rearranging its columns and the derived \mathbf{M} is adjusted via the same column changes, in order to conform equation (7.3). The procedure of reducing the matrix \mathbf{M} to the alternative akin to the identity $\mathbf{1}$ is similar to the Gauss-Jordan elimination method for solving systems of linear equations. During the procedure of row operations, all the unknowns appearing in the assumed matrix \mathbf{M} (7.8) are given or solved according to the structure of the alternative akin to $\mathbf{1}$. Details of the derivation can be found in Ref. [143].

7.3.2 A systematic scenario example

There are so many solutions for the assumed \mathbf{M} which are all suitable for the 1-EPP, however, only one of them has been adjusted and presented as:

$$\mathbf{M}_1 = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 & c_{10} \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_9 & f_{10} \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (7.10)$$

Let us show the systematic scenario for accomplishing the transformation $\mathbf{M}_1 \rightarrow \mathbf{1}$ by one of the simplest networks. The matrix \mathbf{M}_1 can be rephrased as

$$\mathbf{M}_1 = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{15} \\ m_{21} & m_{22} & \cdots & m_{25} \\ \vdots & \vdots & & \vdots \\ m_{51} & m_{52} & \cdots & m_{55} \end{bmatrix},$$

where the matrix elements $m_{\alpha\beta}$ denote the 2×2 matrices:

$$m_{11} = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}, m_{21} = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}, \dots, \quad (7.11)$$

and so forth. The next step of our method is a procedure of elementary row operations on the matrix \mathbf{M}_1 (7.10) subjected to a suitable sequence of the basic operations. When

the assumed matrix \mathbf{M}_1 is transformed into the identity matrix $\mathbf{1}$ under the series of row operations, the unknowns a_r, b_r, \dots, f_r will be solved stepwise in accordance with the structure of $\mathbf{1}$. It is easy to show that a sequence of row operations can do the transformation on two Bell states α and β in a group enumerated by γ , namely,

$$\begin{bmatrix} m_{\alpha\gamma} \\ m_{\beta\gamma} \end{bmatrix} \rightarrow \begin{bmatrix} \mathbf{I} \\ 0 \end{bmatrix}, \quad (7.12)$$

provided that $\det(m_{\alpha\gamma}) = 1$ and $\det(m_{\beta\gamma}) = 0$. Here \mathbf{I} denotes the 2×2 identity matrix.

For example, the consecutive transformation

$$\begin{bmatrix} m_{\alpha\gamma} \\ m_{\beta\gamma} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

can be accomplished if the operation B_y is first performed on Bell state β , then a $\sigma_x B_x$ is performed on Bell state α followed by a BXOR performed on both states, as Bell state α being the source and Bell state β being the target. It can be found in what follows that the unknowns assumed in the matrix \mathbf{M}_1 either will be given based on the requirement for the transformation described in (7.13), or will be determined according to the unique structure of the identity matrix $\mathbf{1}$.

In the first stage of row operations, we are confined to performing a transformation of the matrix \mathbf{M}_1 (7.11) such that $m_{44} \rightarrow \mathbf{I}$ and $m_{4k}, m_{k4} \rightarrow 0$, for $k = 1, 2, 3$, and 5 , according to the structure of $\mathbf{1}$. Let $\det(m_{44}) = 1$ and $\det(m_{14}) = \dots = \det(m_{54}) = 0$, which imply

$$a_7 b_8 \oplus a_8 b_7 = 0, c_8 = 0, e_7 = 1; c_7, d_7, d_8, e_8, f_7, f_8 \in \{0, 1\}. \quad (7.13)$$

Clearly, there are totally 640 solutions for the unknowns appearing in (7.10) to be con-

sidered in this stage. (10 for the condition $a_7b_8 \oplus a_8b_7 = 0$, 2 for each of the 6 arbitrary Boolean valued unknowns, and thus totally $10 \times 2^6 = 640$ solutions) To illustrate the simplest way of creating Boolean functions, however, only one among these 640 cases is considered. Let us consider the case in which

$$a_7 = 1, b_7 = a_8 = b_8 = c_7 = d_7 = d_8 = e_8 = f_7 = f_8 = 0. \quad (7.14)$$

Then, by performing the operations shown in Fig. 7.2(a), we have the transformation $\mathbf{M}_1 \rightarrow \mathbf{M}'_1$,

$$\mathbf{M}'_1 = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 & 0 & a_9 & a_{10} \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & 0 & 0 & d_9 & d_{10} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & 0 & 0 & f_9 & f_{10} \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} m'_{11} & m'_{12} & m'_{13} & 0 & m'_{14} \\ m'_{21} & m'_{22} & m'_{23} & 0 & m'_{25} \\ m'_{31} & m'_{32} & m'_{33} & 0 & m'_{35} \\ 0 & 0 & 0 & \mathbf{I} & 0 \\ m'_{51} & m'_{52} & m'_{53} & 0 & m'_{55} \end{bmatrix}, \quad (7.15)$$

in which we have chosen the following setting for the unknowns:

$$\begin{aligned}
 b_1 = 1, b_2 = 1, b_3 = 0, b_4 = 0, b_5 = 1, b_6 = b_9 = 0, b_{10} = 1, \\
 c_1 = 0, c_2 = c_3 = 0, c_4 = 1, c_5 = c_6 = c_9 = 0, c_{10} = 1, \\
 e_1 = e_2 = e_3 = e_4 = e_5 = e_6 = e_9 = e_{10} = 0.
 \end{aligned} \tag{7.16}$$

Let us proceed to apply the second series of operations, as depicted in the Fig. 7.2(b), to perform the transformations $m'_{22} \rightarrow \mathbf{I}$ and $m'_{2k}, m'_{k2} \rightarrow 0$, for $k = 1, 3$, and 5 . As a result, we have

$$\begin{aligned}
 d_1 = f_1 = d_2 = f_2 = 0, d_3 = d_4 = f_3 = f_4 = 0, d_5 = 1, d_6 = 0 = f_5 = f_6 = 0, \\
 d_9 = f_9 = d_{10} = 0, f_{10} = 1, a_3 = a_4 = 0.
 \end{aligned} \tag{7.17}$$

Note that according to the requirements $\det(m'_{2k})=0$ and $\det(m'_{k2})=0$, $a_3 = a_4 = 0$ is only one of the suitable choices and $d_3 = d_4 = 0$ is the only choice. Therefore, the \mathbf{M}'_1 is

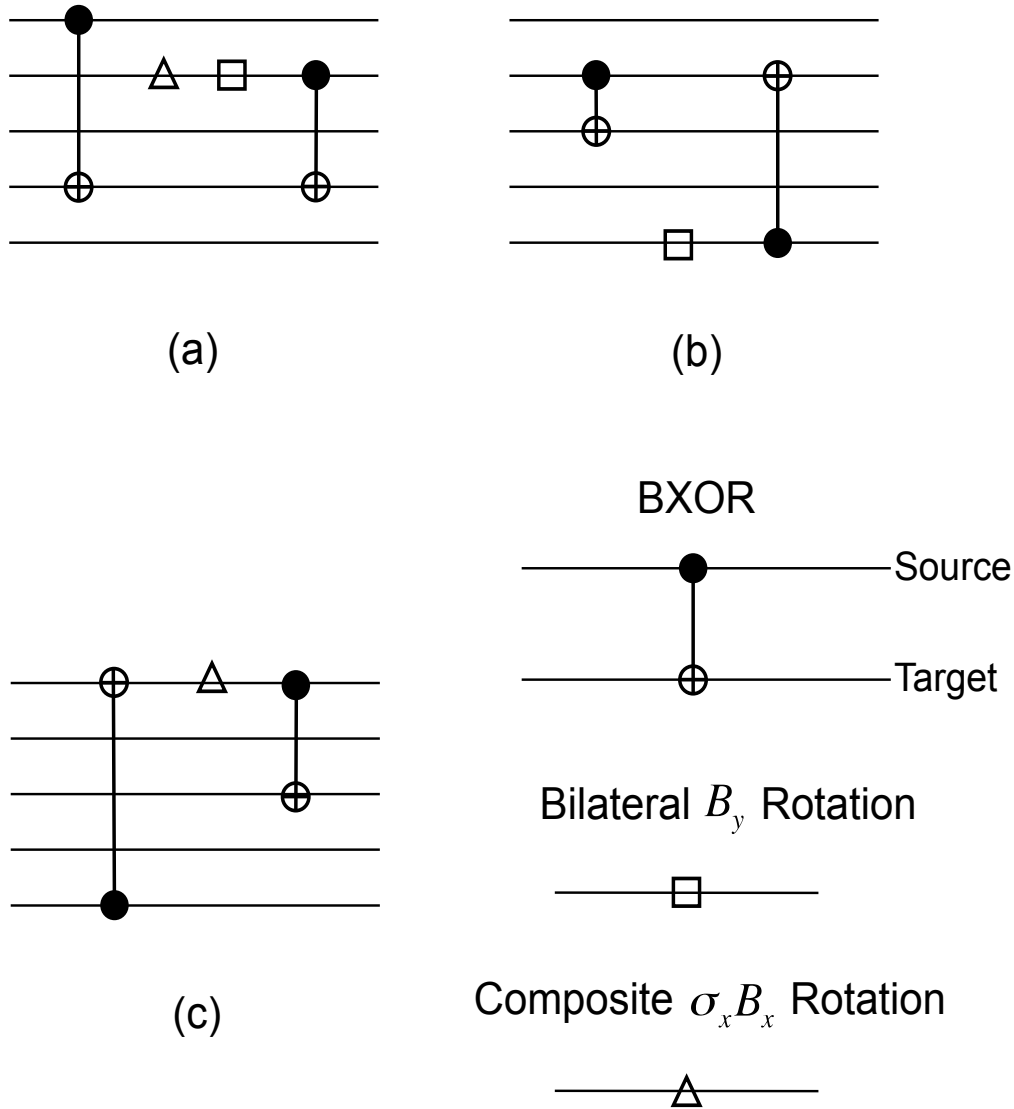


Figure 7.2: The three quantum gate arrays performed in the stage of row operations: (a) for $\mathbf{M}_1 \rightarrow \mathbf{M}'_1$; (b) for $\mathbf{M}'_1 \rightarrow \mathbf{M}''_1$; and (c) for $\mathbf{M}''_1 \rightarrow \mathbf{1}$.

transformed into \mathbf{M}_1'' :

$$\begin{aligned}
 \mathbf{M}_1'' &= \begin{bmatrix} a_1 & a_2 & 0 & 0 & a_5 & a_6 & 0 & 0 & a_9 & a_{10} \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\
 &= \begin{bmatrix} m''_{11} & 0 & m''_{13} & 0 & m''_{14} \\ 0 & \mathbf{I} & 0 & 0 & 0 \\ m''_{31} & 0 & m''_{33} & 0 & m''_{35} \\ 0 & 0 & 0 & \mathbf{I} & 0 \\ m''_{51} & 0 & m''_{53} & 0 & m''_{55} \end{bmatrix} \quad (7.18)
 \end{aligned}$$

Finally, if the matrix \mathbf{M}_1'' is transformed through additional two BXOR and one $\sigma_x B_x$ operations, as shown in Fig. 7.2(c), it results to the identity matrix $\mathbf{1}$. In this stage, we have set the rest of the unknowns to be one of the alternatives: $a_1 = 1, a_2 = 0, a_5 = 1, a_6 = 0, a_9 = 0$, and $a_{10} = 0$. The whole sequence of basic operations, as shown in Fig. 7.3, is obtained by combining the three sub-sequences as shown in Figs. 7.2(a)-(c). It will transform the matrix \mathbf{M}_1 into the identity matrix $\mathbf{1}$. This circuit is the simplest one

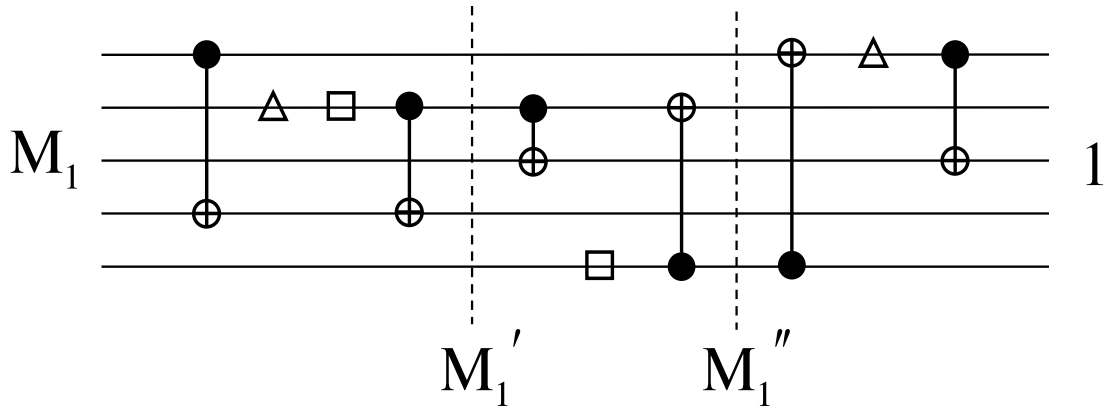


Figure 7.3: The gate array for the transformation $\mathbf{M}_1 \rightarrow \mathbf{1}$. The basic unitary operations are performed in the order from left to right, while if they are performed from right to left, then the inverse transformation $\mathbf{M}_1 \rightarrow \mathbf{1}$ is accomplished.

since it involves only six BXORs, and the corresponding matrix reads

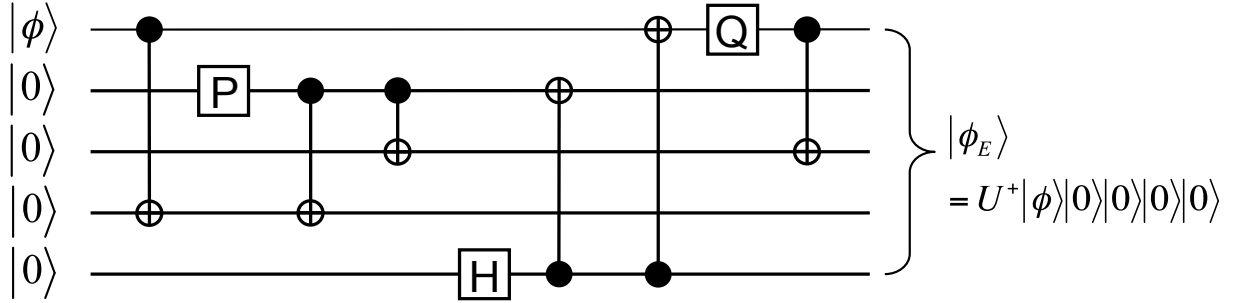
$$\mathbf{M}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{7.19}$$

Performed by this circuit, the correspondence between the error syndromes $e_r^{(i)}$ and the combined measurement results $v_r^{(i)}$ is also listed in Table 7.1. Referring to Table 7.1, or the matrix \mathbf{M}_1 , when Bob obtains the measurement result $v^{(2)} (= 0110)$, for example, he knows the pair to be purified is in the state $\Psi^+ (= 01)$ and thus simply performs the Pauli operation $U_3^{(2)} = \sigma_x$ to recover it to the good state Φ^+ .

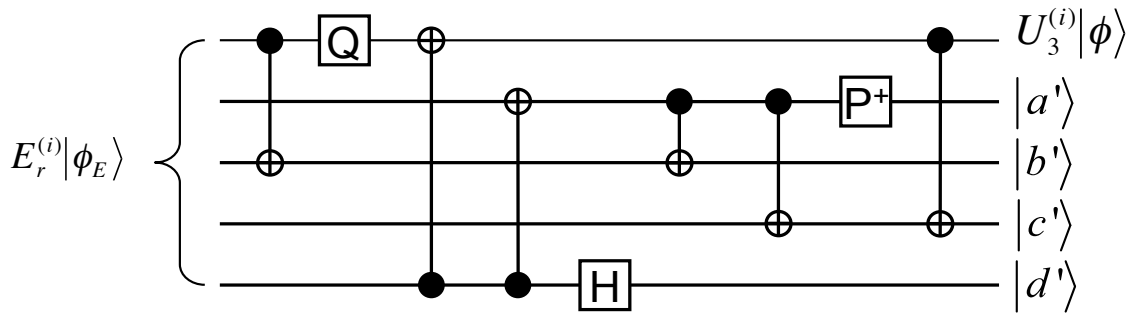
7.4 The encoder-decoder circuit for a perfect five-qubit error correction

The 1-EPP depicted above can be directly converted to a five-qubit QECC whose encoder-decoder circuit has the same configuration as the one shown in Fig. 7.4 [141]. However, in the language of QECC, the classical high-low or phase-amplitude bits used to code the Bell state in the 1-EPP are now used to code operators belonging to the Pauli group, namely, $\mathbf{I} = 00, \sigma_x = 01, \sigma_z = 10, \sigma_y = 11$. When acting on a single qubit, the Pauli operator produces either no error (by \mathbf{I}), a bit flip error (by σ_x), a phase flip error (by σ_z), or a bit-phase flip error (by σ_y). Therefore, such a code is convenient because the codewords $e_r^{(i)}$ are now replaced by $E_r^{(i)}$, which represent the 16 error syndromes described by five-Pauli-operator tensor products. Furthermore, the transformation described by the matrix equation (7.3) is now replaced by the similarity transformation of operators described as: $W^{(i)} = UE_r^{(i)}U^+$, where U (U^+) represents the sequence of the basic operations performed in the decoder (encoder) circuit. Clearly, both the encoder and decoder circuits have exactly the same quantum gate arrangement but they should be run in opposite orders. In order to perform the transformation mentioned above, this time the single-qubit Hadamard transformation: $H = H^+ = (\sigma_x + \sigma_z)/\sqrt{2}$, is used to perform the bit change $H(x, y)H^+ \rightarrow (y, x)$, the single-qubit transformation: $Q = Q^+ = (\sigma_y + \sigma_z)/\sqrt{2}$, is used to perform $Q(x, y)Q^+ \rightarrow (x, x \oplus y)$, and the two-qubit CNOT gate is used to perform $(\text{CNOT})(x_S, y_S)(x_T, y_T)(\text{CNOT})^+ \rightarrow (x_S \oplus x_T, y_S)(x_T, y_S \oplus y_T)$, respectively. That is, in the five-qubit QECC to be presented the basic single- and two-qubit operations needed to be implemented are H , Q , and CNOT.

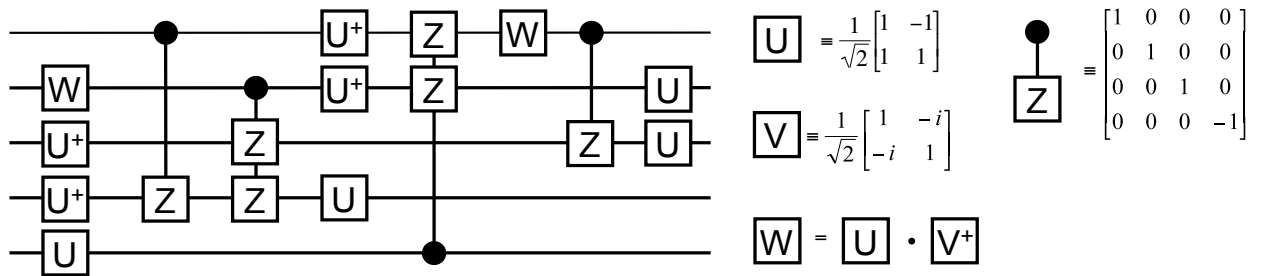
For the present five-qubit QECC, the correspondence between the codewords $W^{(i)}$ and $E_r^{(i)}$ is exactly the same as that between the derived matrix \mathbf{M}_1 given in (7.9) and the identity $\mathbf{1}$. The QECC is performed as follows. If a state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ is to be protected in a quantum computation, it is first accompanied with four extra qubits in the state $|0\rangle$. Then the five-qubit state $|\phi\rangle|0\rangle|0\rangle|0\rangle|0\rangle$ is encoded by the performance of U^+ .



(a) The operation of encoder circuit



(b) The operation of decoder circuit



(c) The operation of encoder circuit for ion-trap quantum computers

Figure 7.4: The perfect five-qubit error correction. (a) The initial tensor product state is encoded to an entangled state $|\phi_E\rangle$. (b) After suffering from the single-qubit error, the state $E_r^{(i)}|\phi_E\rangle$ is then decoded, resulting in the final tensor product state $(U_3^{(i)}|\phi\rangle)|a'b'c'd'\rangle$. Here, $\mathbf{P} = HQ$, $\mathbf{P}^+ = QH$. (c) The encoder circuit from (a) is rewritten in terms of the gate primitives of an ion-trap quantum computer.

After the encoded state is subjected to $E_r^{(i)}$, the erroneous state then is decoded by the implementation of U . The resulting state turns out to be

$$\begin{aligned}
 |\phi_r^{(i)}\rangle &= UE_r^{(i)}U^+(|\phi\rangle|0\rangle|0\rangle|0\rangle|0\rangle) \\
 &= W^{(i)}(|\phi\rangle|0\rangle|0\rangle|0\rangle|0\rangle) \\
 &= (U_3^{(i)}|\phi\rangle)|a'\rangle|b'\rangle|c'\rangle|d'\rangle,
 \end{aligned} \tag{7.20}$$

where $U_3^{(i)}$ is the single-qubit Pauli operation acting on the first qubit and is dependent on the measurement result on the four extra qubits. When the extra qubits are measured in the computational basis, the measurement result $v^{(i)} = a'b'c'd'$ is obtained. Eventually, the corresponding Pauli operation $U_3^{(i)}$ is performed on the remaining qubit, which is in the state $U_3^{(i)}|\phi\rangle$, to recover the initial state $|\phi\rangle$. The procedure of performing the five-qubit QECC is quite simple, same as the one reported by Laflamme *et al.* [77], and is displayed schematically in Fig. 7.4. The present QECC is equivalent to the aforementioned 1-EPP, which adopts the circuit shown in Fig. 7.4, so Table 7.1 is also useful to it. As a result, when referring to Table 7.1 again, if the measurement result $v^{(2)} = 0110$ is read, then $U_3^{(2)} = \sigma_x$ is performed to recover the initial state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. The encoder-decoder circuit required to perform the present QECC, as shown in Figs. 7.4(a) and (b), is rather simple; it contains nine operations, in which only six CNOTs are required. As a matter of fact, this circuit is one of the simplest ones derived so far. The other best known circuit is the one presented by Braunstein and Smolin [139] and its corresponding

matrix is

$$\mathbf{M}_{BS} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \quad (7.21)$$

The efficiency of a coding scheme can be characterized by the shortness of the encoder-decoder circuit. The shortness criterion is based on the fewest total operations or the fewest CNOT operations [74]. The total operations include one-qubit rotations and CNOTs. It is equivalent to determine the minimum experimental efforts for implementing the shortest coding circuit on a quantum computer. The number of laser pulses required to perform a encoder-decoder circuit is a reasonable measure of the efficiency for ion-trap computers [139, 144]. To count the number of laser pulses, the encoder circuit from Fig. 7.4(a) is rewritten in terms of the gate primitives of an ion-trap quantum computer and shown in Fig. 7.4(c). It is interesting to observe that two pairs of CNOTs (the 2nd and 3rd and the 4th and 5th ones) in the present circuit can be combined as two three qubit gates and can be implemented as single element. Besides, the functions of operators U and V implemented on an ion-trap quantum computer are equivalent to the ones of operators H and Q respectively. Since each single-qubit operation requires one laser pulse, the two-qubit gate needs three pulses, and the three-qubit gate requires four laser pulses, the present circuit also requires only 24 laser pulses if it is implemented on an ion-trap quantum computer, same as the Braunstein and Smolin circuit. The numbers of total

Table 7.2: Three efficiency criteria and the corresponding costs for four circuits have been presented. Circuit 1 is given by Bennett *et al.* (Fig. 18 in Ref. [74]) and is unoptimized. The optimized circuit of Bennett *et al.*, denoted by Circuit 2, mentioned in Ref. [74] consists of six two-qubit controlled-NOT gates only. Since the number of laser pulses depends on the detailed structure of the circuit, it is not shown here for lacking the detailed information. Circuit 3 is the simplification of the coding circuit of Laflamme *et al.* proposed by Braunstein and Smolin (Fig. 1 in Ref. [139]). One can find that the original circuit of Laflamme *et al.* (Fig. 1 in Ref. [77]) is more complicated and requires 41 laser pulses. Circuit 4 denotes the simplest circuit has been found by computer search (Fig. 3 in Ref. [139]) and by the systematic method presented in this work.

| Criteria | Circuit 1 | Circuit 2 | Circuit 3 | Circuit 4 |
|----------------------------|-----------|-----------|-----------|-----------|
| Total number of operations | 12 | 11 | 10 | 9 |
| Number of CNOT | 7 | 6 | 7 | 6 |
| Number of laser pulse | 35 | * | 26 | 24 |

operations, CNOTs, and laser pulses for the circuits presented by Bennett *et al.* [74] and Braunstein and Smolin [139] have also been summarized in Table 7.2.

7.5 Conclusion



This chapter has presented a rather simple encoder-decoder circuit to perform the five-qubit, single-error correction protocol. The QECC derived herein is converted directly from the restricted 1-EPP depicted above, so a major part of this work is dedicated to the depiction of the 1-EPP. The present encoder-decoder circuit is the simplest one corresponding to the derived matrix \mathbf{M}_1 given in (7.20), which is derived via an analytical approach [143]. This analytical approach, as shown, can help in deriving not only the suitable matrix \mathbf{M} for the five-qubit QECC but also the simplest version of encoder-decoder circuit corresponding to the derived matrix. However, many possible matrices \mathbf{M} suitable for the QECC remained to be discovered analytically and thus, so many candidates of encoder-decoder circuit that require only six CNOTs. The simplest circuit that is even simpler than the present one and the Braunstein and Smolin circuit [139] might not be found from these candidates. However, a more convinced proof which could be a numerical approach based on the analytical approach introduced in Ref. [143] is

CHAPTER 7. QUANTUM ERROR-CORRECTING CODES AND ENTANGLEMENT PURIFICATION

required in the future work.



Chapter 8

Generation of many-qubit entanglement via conditional measurements on cavity photons



8.1 Introduction

The regulation methods of quantum information processing [29, 30, 37] rely on sharing maximally entangled pairs between distant parties. As it is well known, the entangled pairs may become undesired mixed states due to inevitable interactions with environments [145]. For this reason, great attentions have been focused on the agreement of entanglement purification [74–76], experimental schemes of entanglement distillation [146], and the decoherence mechanisms of qubits in a reservoir [147].

The environment may play an active role on the formation of the nonlocal effect under well considerations. Many investigations [148] have been devoted to the considerations of the reservoir-induced entanglement between two remote qubits. Many schemes have been proposed to enhance the entanglement fidelity by manipulating a third system which interacts with two remote qubits [149–152]. We propose a scheme to generate (or purify) multi-particle entanglement between dot-like single quantum well (QW) excitons inside

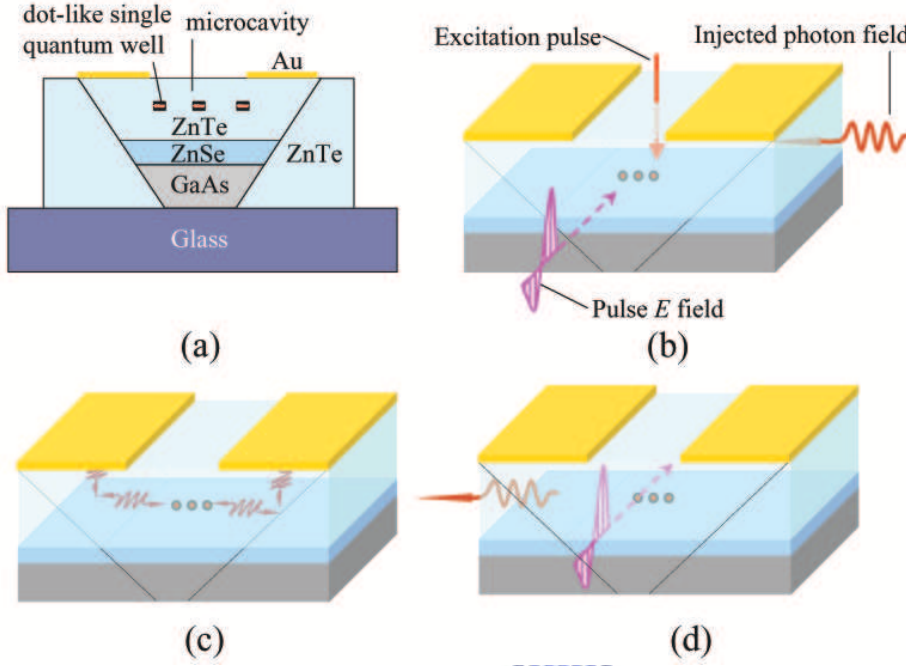


Figure 8.1: (a) The quantum devices with three dot-like quantum wells embedded in a microcavity which is constructed by a ZnTe medium and two Au mirrors. This device can be prepared by the MBE, the e-beam lithography, and the conventional semiconductor processing. (b) Initial state preparation for W state generation. (c) Evolution of the QWs and cavity field for a specific time period. (d) Detection of cavity field for determining the number of the cavity photon. Procedures (b)-(d) are repeated until finishing the entanglement generation.

a single-mode microcavity as depicted in Fig. 8.1(a) [153, 154]. The whole procedure, as shown in Fig. 8.1(b)-(d), can be performed by optical initialization, manipulation, and read-out of exciton state. In the present scheme, the logical state $|1\rangle_i$ in the i th QW is coded by the presence of an exciton, while the logical state $|0\rangle_i$ represents the crystal ground state with no electron and hole. To analyze the dynamics of the many-exciton entanglement, a series of conditional measurements are taken on the cavity field state by means of the electro-optic effect. First of all, we demonstrate how double-exciton Bell state can be generated via conditional measurements. Then, we discuss the cause of multi-exciton W state, and propose a general formulation of entanglement generation. Finally, application to quantum teleportation is pointed out, and may be achieved with current technologies.

In the QW-cavity system, we assume that the lateral size of the QWs are sufficiently

larger than the Bohr radius of excitons but smaller than the wavelength of the photon field. The dipole-dipole interactions and other nonlinear interactions therefore can be neglected. Under the rotating wave approximation, the n QWs and the cavity field are described by the Hamiltonian

$$H_n = \sum_{i=1}^n \hbar \gamma_i (b \sigma_i^+ + b^\dagger \sigma_i^-) + \sum_{i=1}^n \frac{\omega_i}{2} \sigma_i^z + \omega_b b^\dagger b, \quad (8.1)$$

where γ_i denotes the coupling between the i th QW with an excitation energy ω_i and the photon with an energy ω_b , b^\dagger (b) is the creation (annihilation) operator of the cavity field, and σ_i^+ (σ_i^-) represents the creation (annihilation) operator of the excitons in the i th QW. If the cavity mode is assumed further to be resonant with the excitons and equally interact with each QW, i.e. $\omega_i = \omega_b = \omega$ and $\gamma_i = \gamma$, Eq. (8.1) can be reduced to a simple form in the interaction picture:

$$H_{n(I)} = \sum_{i=1}^n \gamma (b \sigma_i^+ + b^\dagger \sigma_i^-), \quad (8.2)$$

where $\hbar = 1$ has been set and $\sigma^\pm = \sum_{i=1}^{i=n} \sigma_i^\pm$.

8.2 Bell states generation

Plenio *et al.* [149] have shown that a maximally entangled state, or called Bell state, for two atoms can be created through a leaky cavity via continuously measurements of the vacuum cavity field state $|0\rangle_c$. Here we investigate further how the measured photons affect the Bell state generation especially when the photon number is greater than zero. Suppose we start with the initial state $|\psi_0\rangle |0\rangle_c = |1\rangle_2 |0\rangle_1 |0\rangle_c = |10\rangle |0\rangle_c$, and then a pulse with $(Q - 1)$ photons is injected into the microcavity. The total number of quantum count of the system is Q . As the $(Q - 1)$ photons have been injected into the cavity, the total system will evolve with time, and if the system evolves without interruption, it will go into a QW1-QW2-cavity field entangled state. If a measurement on the cavity

field state is taken at some instant, the detector would count $(Q - 1)$, $(Q - 2)$, or Q photons. Since the Bell state involves a single excitation, if the cavity mode stays in state $|Q - 1\rangle_c$ we can infer that the double-QW will evolve into a maximal entangled state via the quantum jump approach [155]. After measuring the cavity field state, injecting the subsequent $(Q - 1)$ photons into the cavity is necessary for the sake of keeping the photon in its state. We then let the whole system evolve for another period of time τ . Again, we proceed to measure the cavity photon to make sure whether it is $(Q - 1)$ or not. If the cavity photon remains in the $(Q - 1)$ -photon state, the repetition continues; if not, the whole procedure should be started over.

The time evolution of the n QWs subsystems under N times of successful repetitions is described by the operator:

$$U(\tau)^N = [{}_c\langle Q - 1 | e^{-iH_n(t)\tau} | Q - 1 \rangle_c]^N, \quad (8.3)$$

The conditional operator $U(\tau)$ can be explicitly evaluated

$$U(\tau) = \cos\left(\sqrt{(2Q - 1)\sigma^+\sigma^- - (Q - 1)\sigma^z}\gamma\tau\right), \quad (8.4)$$

where $\sigma^z = \sum_{i=1}^{i=n} \sigma_i^z$. In deriving the above result we have utilized the expansion for the time evolution operator $e^{-iH_n(t)}$ and the algebra $[\sigma^+, \sigma^-] = \sigma^z$. One also notes that both $\sigma^+\sigma^-$ and σ^z commute with the translational operator, which transfers $|\phi_1\rangle = |01\rangle$ to the state $|\phi_2\rangle = |10\rangle$ as $n = 2$ has been set, so for two-qubit case the operator $U(\tau)$ can be decomposed by the eigenstates of the translation operator

$$|L_l\rangle = \frac{1}{\sqrt{2}} \sum_{h=1}^2 e^{i\frac{2\pi l}{n}(h-1)} |\phi_h\rangle, \quad (8.5)$$

with $l = 0, 1$. Thus we get the conditional operator in the diagonal form:

$$U(\tau) = \cos(\sqrt{4Q - 2}\gamma\tau) |L_0\rangle\langle L_0| + |L_1\rangle\langle L_1|. \quad (8.6)$$

Furthermore, the probability of success for measuring $(Q - 1)$ photons after N times of repetitions, $P(N, n = 2)$, and the fidelities $F_{L_0}(N, 2)$ and $F_{L_1}(N, 2)$ with respect to $|L_0\rangle$ and $|L_1\rangle$ can be worked analytically

For a general case of $\gamma\tau$ and Q , $P(N, 2)$ approaches to the value of $1/2$ in the limit of large N ; meanwhile the subsystem goes in to the QW1-QW2 maximally entangled state: $|L_1\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. On the other hand, one can also find a suitable condition such that the probability goes to unity. In this case, the system will not evolve with time, which is similar to the Zeno paradox with *finite* duration between two measurements.

8.3 Multi-qubit W state

We may directly follow the scheme based on continuous measurements to achieve the multi-particle entanglement generation. In what follows we will show that the multi-particle entangled state indeed can be produced via conditional and constant measurements. Moreover, the W-type maximally entanglement can be generated in the multi-QWs system.

Suppose the whole system is initially prepared in the state $|\psi_0\rangle |1\rangle_c = |1\rangle_n |0\rangle_{n-1} \dots |0\rangle_1 |1\rangle_c = |10\dots 0\rangle |1\rangle_c$. We follow the same formalism for two-particle entanglement, but $Q = 2$ is set in this case. The conditional propagator $U(\tau) = {}_c \langle 1 | e^{-iH_n(\tau)} | 1 \rangle_c$ that governs the progress of the n dot-like single QWs is given by

$$U(\tau) = \cos \left(\sqrt{3\sigma^+\sigma^- - \sigma^z\gamma\tau} \right), \quad (8.7)$$

which is derived from Eq. (8.4) for $Q = 2$. The set of the eigenbasis for the translational operator is expressed as

$$|L_l\rangle = \frac{1}{\sqrt{2}} \sum_{h=1}^n e^{i\frac{2\pi l}{n}(h-1)} |\phi_h\rangle, \quad (8.8)$$

where $|\phi_h\rangle = |1\rangle_h \otimes_{i=1, i \neq h}^n |0\rangle_i$ and $l = 0, 1, 2, \dots, n - 1$, is exerted to represent $U(\tau)$ in the

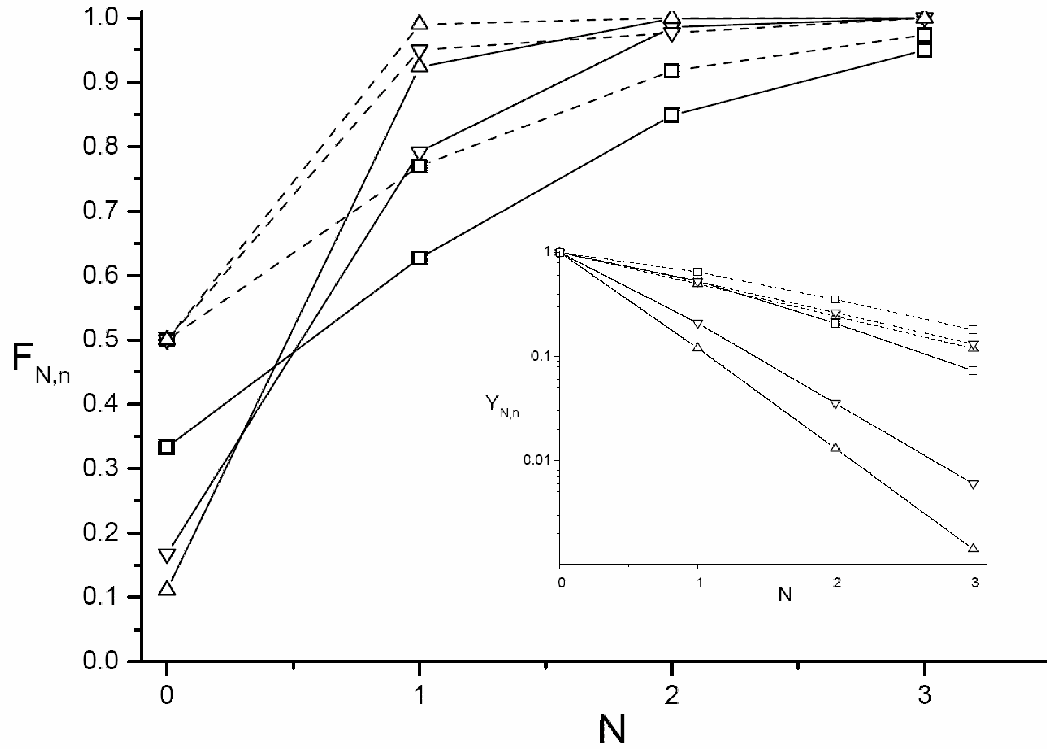


Figure 8.2: The variations of fidelity $F_{N,n}$ and the purification yield $Y_{N,n}$ (in the inserted diagram) for cases $n = 3(\square)$, $6(\nabla)$, and $9(\triangle)$, and for two different kinds of initial states: $\rho = p\mathbf{1} + (1 - np)|L_0\rangle\langle L_0|$ (dash) and $|\psi_0\rangle$ (solid), in which the evolution time of each case, $\tau_3 = \pi/(\sqrt{10}\gamma)$, $\tau_6 = \pi/(\sqrt{22}\gamma)$, and $\tau_9 = \pi/(4\sqrt{2}\gamma)$ has been set.

diagonal form:

$$U(\tau) = \cos(\sqrt{4n-2}\gamma\tau) |L_0\rangle \langle L_0| + \cos(\sqrt{n-2}\gamma\tau) \sum_{l=1}^{n-1} |L_l\rangle \langle L_l|. \quad (8.9)$$

Here, $|L_0\rangle$ is just the W-type entangled state:

$$|L_0\rangle = |W\rangle = \frac{1}{\sqrt{n}}(|0\dots 01\rangle + |0\dots 10\rangle + \dots + |10\dots 0\rangle). \quad (8.10)$$

The probability of success for N conditional measurements and the fidelity of the QWs with respect to the W state at the N -th stage can also be obtained

Fig. 8.2 shows the variations of the probability $P(N, n)$ and the purification yield $Y(N, n)$, defined by $Y(N, n) = \prod_{i=0}^N P(i, n)$, for the cases of $n = 3, 6$, and 9 with two different kinds of initial states. The fidelity increases with the number of the measurements, the probability, however, decreases more rapidly. Although, the yield $Y(N, n)$ actually decreases with the increasing of N , even at one step the whole particles can be entangled in the W-type state. In addition to the entanglement generation, present scheme can also be applied to entanglement purification. If the initial state is a mixed one with a single excitation and is expressed as the form: $\rho = p\mathbf{1} + (1 - np) |L_0\rangle \langle L_0|$, where p is the noise intensity, it can be purified into a pure state. The purification yield and the fidelity are shown in Fig. 8.2 for the case $p = 0.5$.

To discuss our formulation further, let us consider the $Q = 1$ case. If we take conditional and constant measurements on the photon state $|0\rangle_c$ and let the initial state of the whole system situate in $|\psi_0\rangle |0\rangle_c = |10\dots 0\rangle |0\rangle_c$, the operator $U(\tau)^N = \cos^N(\sqrt{\sigma^+\sigma^-}\gamma\tau)$ can be diagonalized into the following form

$$U(\tau)^N = [\cos^N(\sqrt{n}\gamma\tau) - 1] |W\rangle \langle W| + \mathbf{1}, \quad (8.11)$$

where $\mathbf{1}$ is the identity operator. The probability of success under the process can then

be written as

$$P(N, n) = \frac{1}{n} [(n - 1) + \cos^{2N}(\sqrt{n}\gamma\tau)], \quad (8.12)$$

and the fidelity for obtaining the W state is

$$F_W(N, n) = \frac{\cos^{2N}(\sqrt{n}\gamma\tau)}{(n - 1) + \cos^{2N}(\sqrt{n}\gamma\tau)}. \quad (8.13)$$

For a generic setting of $\gamma\tau$ and large N , the QWs is indeed in the final state:

$$|L\rangle = \frac{1}{\sqrt{n(n-1)}} [(n-1)|10\dots0\rangle - |010\dots0\rangle \dots - |0\dots01\rangle]. \quad (8.14)$$

When $n = 2$ and $Q = 1$, the above formulation reduced to the Bell state [149]. However, for $n \geq 3$ the multi-QWs W state cannot be generated in this system if we continuously monitor the cavity vacuum.

Fig. 8.1(b)-(d) depict the implementation procedure of the three-qubit W state generation for demonstrating our proposed scheme discussed above. Firstly, three dot-like single quantum wells are in ground states, and then one is excited by an excitation pulse. A resonant photon with vertical linear polarization generated via a quartz plate is injected into the cavity which is constructed by ZnTe with both Au films. Meanwhile, through the pulse E field [156], the linear polarization of injected photon is rotated from vertical to horizontal via the Electro-optic effect in ZnTe [157] (Fig. 8.1(b)). After a sufficient evolution time with dot-like single quantum wells, as shown in Fig. 8.1(c), the photon in cavity could be leaked out the cavity by a pulse E field with suitable timing and detected by a single photon avalanche diode for checking whether the number of the cavity photon is desired, as shown in Fig. 8.1(d). This procedure would be repeated until finishing the purification.

8.4 Quantum teleportation

Experiments of teleportation have already been realized in several different physical systems. See the introduction in the first chapter. In solid state systems, however, experimental demonstration of teleportation in charge qubits is still lacking, and only few theoretical schemes are proposed [158]. Here, we demonstrate that present device can also be applied to quantum teleportation via superradiance [159].

Consider now two QWs embedded inside the cavity. First of all, controlling the orientation or the band gap of the excitons in QWs via the external field such that only QW-1 can interact with the cavity photon. After injecting one photon into the cavity, singlet entangled state can be created between QW-1 and the photon with appropriate evolution time τ . One then switches off the cavity effect such that the photon may leak out of the cavity. Meanwhile, a pulse laser is applied to QW-2 to create an unknown state $\alpha |1\rangle_2 + \beta |0\rangle_2$, which is to be teleported. In this case, the total wave function of the system can be written as

$$\begin{aligned}
 |\Psi\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_c |1\rangle_1 - |1\rangle_c |0\rangle_1) \otimes (\alpha |1\rangle_2 + \beta |0\rangle_2) \\
 &= |0\rangle_c \otimes \left(\frac{\alpha}{\sqrt{2}} |T_1\rangle_{12}\right) + |1\rangle_c \otimes \left(\frac{-\beta}{\sqrt{2}} |T_{-1}\rangle_{12}\right) \\
 &\quad + (\alpha |1\rangle_c + \beta |0\rangle_c) \otimes \frac{|S_0\rangle_{12}}{2} + (-\alpha |1\rangle_c + \beta |0\rangle_c) \otimes \frac{|T_0\rangle_{12}}{2}. \tag{8.15}
 \end{aligned}$$

where $|T_1\rangle = |1\rangle_1 |1\rangle_2$, $|T_{-1}\rangle = |0\rangle_1 |0\rangle_2$, $|S_0\rangle_{12} = (|1\rangle_1 |0\rangle_2 - |1\rangle_2 |0\rangle_1)/\sqrt{2}$, and $|T_0\rangle_{12} = (|1\rangle_1 |0\rangle_2 + |1\rangle_2 |0\rangle_1)/\sqrt{2}$.

If both the QWs are now tuned to be resonant with each other, common photon reservoir will drive the system to decay collectively with four possibilities for the detector's results: zero photon, two photons, one photon via the superradiant channel, or one photon via the subradiant channel [160]. If the measurement outcome is a single photon with a suppressed decay rate, the teleportation is achieved automatically. As for the result of one photon with enhanced decay rate, all we have to do is to perform a phase-gate operation

on the cavity photon state to complete the teleportation.

Since decay time is a statistical average, one might ask how to distinguish between sub- and superradiant photons via the decay time in one single shot? We would like to point out that because of the collective decay, the momentum of the emitted photon \vec{k} depends on the separation of the two QWs \vec{r} , i.e. $\vec{k} \cdot \vec{r} = 0$ or π corresponds to the emission of super- or sub-radiant photon, respectively [160]. Therefore, sub- and super-radiance can be distinguished by placing detectors at appropriate angles. The teleportation can then be tested by repeating this scheme over many cycles and probing the state of the cavity (one or no photon) after each cycle.

In usual teleportation scheme, one has to perform Hadamard and CNOT transformations on one of the entangled particles and the teleported quantum state. After that, the information from the joint measurements of the two particles has to be sent to the other entangled particle in order to allow proper unitary operations. In our proposal, however, the Hadamard and CNOT transformations are omitted and the joint measurements are performed naturally by collective decay. This kind of “one-pass” teleportation is similar to S. Bose’s proposal [161], where the teleportation between two trapped atoms in two independent cavities is achieved by the leaked cavity photons impinging on a 50-50 beam splitter. Just like S. Bose’s protocol, our probabilistic proposal can be modified to teleportation with insurance, so that in the cases when the protocol is unsuccessful the original teleported state is not destroyed, but mapped onto another reserve QW [162].

Chapter 9

Quantum search algorithm

9.1 Quantum search problem

To solve a search problem associated a unsorted database, the remarkable Grover's quantum algorithm [57, 58] provides a quadratic speedup over its classical counterpart. The search problem can be described as follows: for a given function f , there is one unknown element in the set $\{0, 1, \dots, N - 1\}$ that satisfies $f(x) = -1$, say $x = \tau$, whereas the other $N - 1$ ones give $f(x) = 1$. How many times of evaluations of f are required to determine the element τ for $f(\tau) = -1$? Through a conventional algorithm, one needs $O(N)$ trials to achieve this aim. How about the utility of quantum algorithm? The search problem can be rephrased in the quantum mechanical language: for a given unitary operator I_τ , that is sometimes called the *oracle operator*, and a set of state vectors (orthonormal basis): $\{|0\rangle, |1\rangle, \dots, |N - 1\rangle\}$, $I_\tau |x\rangle = |x\rangle$ for all states in the set except $I_\tau |x\rangle = -|x\rangle$ for $x = \tau$. How many queries of I_τ are required to determine $|\tau\rangle$? By Grover's algorithm [57, 58], one needs only $O(\sqrt{N})$ quantum mechanical steps to find the marked state $|\tau\rangle$ out. The first step of Grover's algorithm is to prepare a superposition state of all elements: $|s\rangle = 1/\sqrt{N} \sum_{x=0}^{N-1} |x\rangle$. Then apply the Grover kernel $G = -I_\eta I_\tau$ to $|s\rangle$, where I_η is a unitary operator and contains no bias against the marked state. After about $m = \pi\sqrt{N}/4$ repetitions, i.e., $G^m |s\rangle$, the probability to get $|\tau\rangle$ is close to one if N is large. Since every

single G involves one query of I_τ , $O(\sqrt{N})$ searching steps are required for a quantum search task. In what follows, we will investigate on the certain quantum search and the phase-error tolerance of Grover's algorithm. In the next chapter, we will demonstrate the one-way quantum computation experimentally by solving a quantum search problem.

9.2 Quantum searching with certainty

Grover's algorithm provides a high probability in finding the object only for a large N . The probability will be lower as N decreases. Grover [163], however, also proposed that the Walsh-Hadamard transformation used in the original version can be replaced by almost any arbitrary unitary operator and the phase angles of rotation can be arbitrarily used as well, instead of the original π -angles. The utility of the arbitrary phase angles in fact can provide the possibility for finding the marked item with certainty, no matter whether N is large or not, if these angles obey a so-called matching condition.

Some typical literatures concerning with the matching condition will be mentioned here. Long *et al.* [164, 165] have derived the relation $\phi = \theta$, where ϕ and θ are the phases used in the algorithm, using an $SO(3)$ picture. Høyer [166], on the other hand, has proved a relation $\tan(\phi/2) = \tan(\theta/2)(1 - 2/N)$, and claimed that the relation $\phi = \theta$ is an approximation to this case. Recently, a more general matching condition has been derived by Long *et al.* [167], also using the $SO(3)$ picture. In the last article, however, only the certainty for finding the marked state is ensured. In fact a phase angle appearing in the amplitude of the final state after searching will remain. If the final state should be necessary for a future application, i.e., if it should interact with other states, this phase angle will be important for quantum interferences, but it can not be given in the $SO(3)$ representation. We therefore intend to derive the matching condition in the $SU(2)$ picture. In addition, we will also give a more concise formula for evaluating the number of the iterations needed in the searching and deduce the final state in a complete form as $e^{i\delta} |\tau\rangle$, where $|\tau\rangle$ is the marked state. The optimal choice of the phase angles will be

discussed, too [168].

Suppose in a two-dimensional, complex Hilbert space we have a marked state $|\tau\rangle$ to be searched by successively operating a Grover's kernel G on an arbitrary initial state $|s\rangle$. The Grover kernel is a product of two unitary operators I_τ and I_η , given by

$$\begin{aligned} I_\tau &= I + (e^{i\phi} - 1) |\tau\rangle \langle \tau|, \\ I_\eta &= I + (e^{i\theta} - 1) U |\eta\rangle \langle \eta| U^{-1}, \end{aligned} \quad (9.1)$$

where U is an arbitrary unitary operator, $|\eta\rangle$ is another unit vector in the space, and ϕ and θ are two phase angles. It should be noted that the phases ϕ and θ actually are the differences $\phi = \phi_2 - \phi_1$ and $\theta = \theta_2 - \theta_1$, where ϕ_2 , ϕ_1 , θ_2 , and θ_1 , as depicted in Refs. [169, 170], denote the rotating angles to $|\tau\rangle$, the vector orthogonal to $|\tau\rangle$, $U|\eta\rangle$, and the vector orthogonal to $U|\eta\rangle$, respectively. The Grover kernel can be expressed in a matrix form as long as an orthonormal set of basis vectors is designated, so we simply choose

$$|I\rangle = |\tau\rangle \quad \text{and} \quad |II\rangle = (U|\eta\rangle - U_{\tau\eta}|\tau\rangle)/l, \quad (9.2)$$

where $U_{\tau\eta} = \langle \tau | U |\eta \rangle$ and $l = (1 - |U_{\tau\eta}|^2)^{1/2}$. Letting $U_{\tau\eta} = \sin(\beta)e^{i\alpha}$, we can write, from (9.2),

$$U|\eta\rangle = \sin(\beta)e^{i\alpha} |I\rangle + \cos(\beta) |II\rangle, \quad (9.3)$$

and the Grover kernel can now be written

$$\begin{aligned} G &= -I_\eta I_\tau \\ &= - \begin{bmatrix} e^{i\phi}(1 + (e^{i\theta} - 1) \sin^2(\beta)) & (e^{i\theta} - 1) \sin(\beta) \cos(\beta) e^{i\alpha} \\ e^{i\phi}(e^{i\theta} - 1) \sin(\beta) \cos(\beta) e^{-i\alpha} & 1 + (e^{i\theta} - 1) \cos^2(\beta) \end{bmatrix}. \end{aligned} \quad (9.4)$$

In the searching process, the Grover kernel is successively operated on the initial state $|s\rangle$. We wish that after, say, m iterations the operation the final state will be orthogonal

to the basis vector $|II\rangle$ so that the probability for finding the marked state $|\tau\rangle$ will exactly be unity. Alternatively, in mathematical expression, we wish to fulfill the requirement

$$\langle II | G^m |s\rangle = 0 , \quad (9.5)$$

since then

$$|\langle \tau | G^m |s\rangle| = |\langle I | G^m |s\rangle| = 1 . \quad (9.6)$$

The eigenvalues of the Grover kernel G are

$$\lambda_{1,2} = -e^{i(\frac{\phi+\theta}{2} \pm w)} , \quad (9.7)$$

where the angle w is defined by

$$\cos(w) = \cos\left(\frac{\phi - \theta}{2}\right) - 2 \sin\left(\frac{\phi}{2}\right) \sin\left(\frac{\theta}{2}\right) \sin^2(\beta) . \quad (9.8)$$

The normalized eigenvectors associated with these eigenvalues are computed:

$$|g_1\rangle = \begin{bmatrix} e^{-i\frac{\phi}{2}} e^{i\alpha} \cos(x) \\ \sin(x) \end{bmatrix} , |g_2\rangle = \begin{bmatrix} -\sin(x) \\ e^{i\frac{\phi}{2}} e^{-i\alpha} \cos(x) \end{bmatrix} . \quad (9.9)$$

In expression (9.9), the angle x is defined by

$$\sin(x) = \sin\left(\frac{\theta}{2}\right) \sin(2\beta) / \sqrt{l_m} ,$$

where

$$\begin{aligned} l_m &= (\sin(w) + \sin(\frac{\phi - \theta}{2}) + 2 \cos(\frac{\phi}{2}) \sin(\frac{\theta}{2}) \sin^2(\beta))^2 + (\sin(\frac{\theta}{2}) \sin(2\beta))^2 \\ &= 2 \sin(w) (\sin(w) + \sin(\frac{\phi - \theta}{2}) + 2 \cos(\frac{\phi}{2}) \sin(\frac{\theta}{2}) \sin^2(\beta)). \end{aligned}$$

The matrix G^m can be simply expressed by $G^m = \lambda_1^m |g_1\rangle \langle g_1| + \lambda_2^m |g_2\rangle \langle g_2|$, so we have

$$G^m = (-1)^m e^{im(\frac{\phi+\theta}{2})} \begin{bmatrix} e^{imw} \cos^2(x) + e^{-imw} \sin^2(x) & e^{-i\frac{\phi}{2}} e^{i\alpha} i \sin(mw) \sin(2x) \\ e^{i\frac{\phi}{2}} e^{-i\alpha} i \sin(mw) \sin(2x) & e^{imw} \sin^2(x) + e^{-imw} \cos^2(x) \end{bmatrix}. \quad (9.10)$$

The initial state $|s\rangle$ in this work is considered to be an arbitrary unit vector in the space and is given by



$$|s\rangle = \sin(\beta_0) |I\rangle + \cos(\beta_0) e^{iu} |II\rangle. \quad (9.11)$$

The requirement (9.5) implies that both the real and imagine parts of the term $\langle II | G^m |s\rangle$ are zero, so, as substituting (9.10) and (9.11) into (9.5), one will eventually obtain the two equations:

$$-\sin(mw) \sin(\frac{\phi}{2} - \alpha - u) \sin(2x) \sin(\beta_0) + \cos(mw) \cos(\beta_0) = 0, \quad (9.12)$$

$$\sin(mw) \cos(\frac{\phi}{2} - \alpha - u) \sin(2x) \sin(\beta_0) - \sin(mw) \cos(2x) \cos(\beta_0) = 0. \quad (9.13)$$

Equation (9.13), by the definition of the angle x , will reduce to the matching condition

$$(\sin(\frac{\phi - \theta}{2}) + 2 \cos(\frac{\phi}{2}) \sin(\frac{\theta}{2}) \sin^2(\beta)) \cos(\beta_0) = \sin(\frac{\theta}{2}) \sin(2\beta) \cos(\frac{\phi}{2} - \alpha - u) \sin(\beta_0), \quad (9.14)$$

which is identical to the relation derived by Long *et al.* [167]:

$$\tan\left(\frac{\phi}{2}\right) = \tan\left(\frac{\theta}{2}\right) \left(\frac{\cos(2\beta) + \sin(2\beta) \tan(\beta_0) \cos(\alpha + u)}{1 - \tan(\beta_0) \tan\left(\frac{\theta}{2}\right) \sin(2\beta) \sin(\alpha + u)} \right). \quad (9.15)$$

Equation (9.12), under the satisfaction of the matching condition (9.14), or (9.15), will reduce to a concise formula for evaluating the number of iterations m :

$$\cos(mw + \sin^{-1}(\sin(\beta_0) \sin\left(\frac{\phi}{2} - \alpha - u\right))) = 0. \quad (9.16)$$

By equation (9.16), one can compute the number m

$$m = \lceil f \rceil, \quad (9.17)$$

where $\lceil \cdot \rceil$ denotes the smallest integer greater than the quantity in it, and the function f is given by

$$f = \frac{\frac{\pi}{2} - \sin^{-1}(\sin(\beta_0) \sin\left(\frac{\phi}{2} - \alpha - u\right))}{\cos^{-1}(\cos\left(\frac{\phi - \theta}{2}\right) - 2 \sin\left(\frac{\phi}{2}\right) \sin\left(\frac{\theta}{2}\right) \sin^2(\beta))}. \quad (9.18)$$

It can also be shown that if the matching condition is fulfilled, then after m searching iterations the final state will be

$$G^m |s\rangle = e^{i\delta} |\tau\rangle = e^{i[m(\pi + \frac{\phi + \theta}{2}) + \Omega]} |\tau\rangle, \quad (9.19)$$

where the angle Ω is defined by

$$\Omega = \tan^{-1}(\cot\left(\frac{\phi}{2} - \alpha - u\right)). \quad (9.20)$$

The phase angle appearing in the amplitude of the final state will be important for quantum interferences if possibly the state should interact with other states in a future application, so we would had better remain it as the present form.

The matching condition (9.14), or (9.15), relates the angles ϕ , θ , β , β_0 , and $\alpha + u$ for finding a marked state with certainty. If β , β_0 and $\alpha + u$ are designated, then $\phi = \phi(\theta)$ is deduced by the matching condition. As $\phi(\theta)$ is determined, we then can evaluate by (9.18) the value of $f = f(\phi(\theta), \theta)$ and consequently decide by (9.17) the number of iterations m . The functions $\phi(\theta)$ and $f(\theta)$ for some particular designations of β , β_0 and $\alpha + u$ have been shown in Figs. 9.1 and 9.2. These examples have schematically depicted that theoretically we can establish a tabulated chart of possible choices between all of the phases for finding a marked state with certainty. It is worth noticing that as $\alpha + u = 0$ and $\beta = \beta_0$, the matching condition recovers $\phi = \theta$ automatically since then eq. (9.13) becomes an identity, and accordingly one has

$$f = \frac{\frac{\pi}{2} - \sin^{-1}(\sin(\frac{\phi}{2}) \sin(\beta))}{2 \sin^{-1}(\sin(\frac{\phi}{2}) \sin(\beta))}, \text{ for } \phi = \theta. \quad (9.21)$$

This is the case discussed in Ref. [165]; an example can be read by the straight line of unity slope for $\beta = \beta_0 = 10^{-4}$ and the corresponding f vs θ variation in Fig. 9.1. It can also be shown that the matching condition (9.14) will recover the relation considered by Høyer [166]:

$$\tan(\frac{\phi}{2}) = \tan(\frac{\theta}{2}) \cos(2\beta), \text{ for } \cos(\phi/2 - \alpha - u) = 0. \quad (9.22)$$

In Figs.9.1 and 9.2 we have shown by the cross marks some particular examples of this special case.

Observing Figs 9.1 and 9.2, one realizes that for every designation of β , β_0 and $\alpha + u$, the optimal choices for ϕ and θ is letting $\phi = \theta = \pi$, since then the corresponding f is minimum under the fact $df/d\theta = (\partial f/\partial\phi)(d\phi/d\theta) + \partial f/\partial\theta = 0$, for $\phi = \theta = \pi$. We thus denote the optimal value of m by

$$m_{op} = \lceil \min(f) \rceil = \left\lceil \frac{\frac{\pi}{2} - \sin^{-1}(\sin(\beta_0) \cos(\alpha + u))}{2\beta} \right\rceil. \quad (9.23)$$

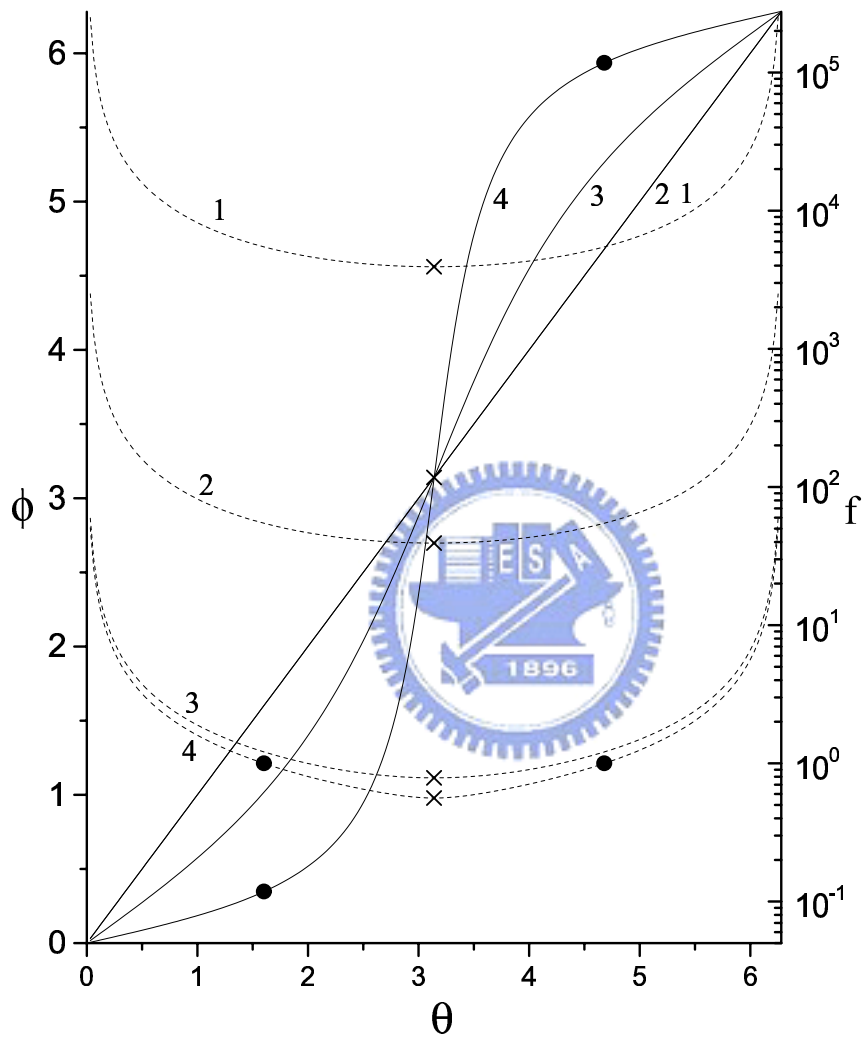


Figure 9.1: Variations of $\phi(\theta)$ (solid) and $f(\theta)$ (broken), for $\alpha + u = 0$, $\beta_0 = 10^{-4}$, and $\beta = 10^{-4}$ (1), 10^{-2} (2), 0.5 (3) and 0.7 (4), respectively. The cross marks denote the special case of Høyer [166], while the entire circles correspond to the optimal choices of ϕ_{op} and θ_{op} for $\alpha + u = 0$, $\beta_0 = 10^{-4}$ and $\beta = 0.7$. The solid straight line 1 corresponds the case $\phi = \theta$, while the solid curve 2 is only approximately close to the former.

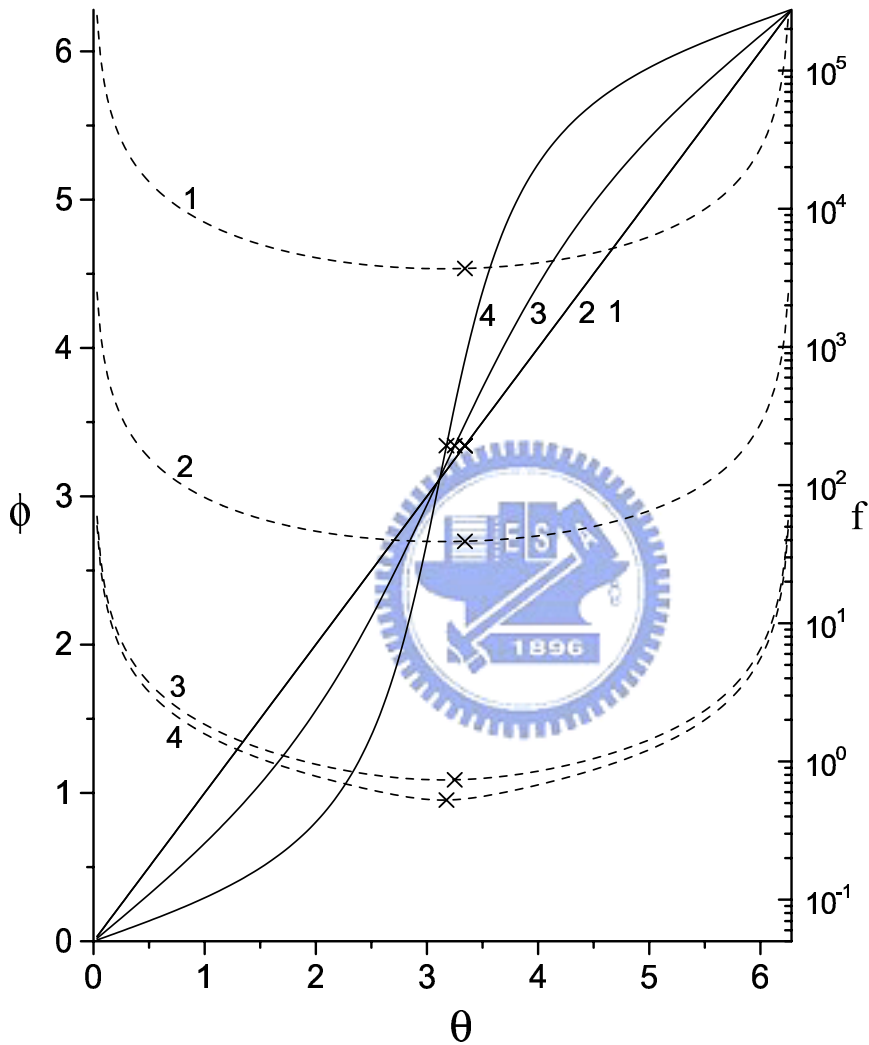


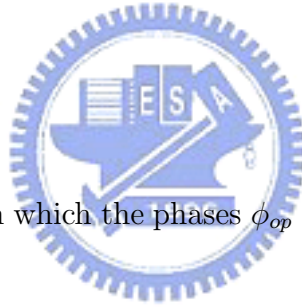
Figure 9.2: Variations of $\phi(\theta)$ (solid) and $f(\theta)$ (broken), for $\alpha + u = 0.1$, $\beta_0 = 0.1$, and $\beta = 10^{-4}$ (1), 10^{-2} (2), 0.5 (3) and 0.7 (4), respectively. The cross marks denote the special case of Høye [166]. The solid curves 1 and 2 are very close, and both of them are only approximately close to the line $\phi = \theta$.

With the choice of m_{op} , however, one need to modify the phases θ and $\phi(\theta)$ to depart from π so that the matching condition is satisfied again. For example, if $\alpha + u = 0$, $\beta_0 = 10^{-4}$ and $\beta = 0.7$ are designated, then the minimum value of f will be $\min(f) = 0.56$. So we choose $m_{op} = 1$ and the modified phases are $\theta_{op} = (1 \pm 0.490)\pi$ and $\phi_{op} = (1 \pm 0.889)\pi$, respectively. This example has been shown by the marked entire circles in Fig.1. It is worth noticing again that under the choice of m_{op} the modified ϕ and θ for the special case considered by Long [165] will be

$$\phi_{op} = \theta_{op} = \lceil \min(f) \rceil = 2 \sin^{-1} \left(\frac{\sin(\frac{\pi}{4m_{op}+2})}{\sin(\beta)} \right),$$

where

$$m_{op} = \left\lceil \frac{\frac{\pi}{2} - \beta}{2\beta} \right\rceil.$$



This is in fact a special case in which the phases ϕ_{op} and θ_{op} can be given by a closed-form formula.

9.3 An improved phase error tolerance in quantum search algorithm

Grover's quantum search algorithm [57, 58] is achieved by applying Grover kernel on an uniform superposition state, which is obtained by applying Walsh-Hadamard transformation on a initial state, in a specific operating steps such that the probability amplitude of marked state is amplified to a desired one. Grover's kernel is composed of phase rotations and Walsh-Hadamard transformations. The phase rotations include two kinds of operations : π -inversion of the marked state and π -inversion of the initial state. It has shown that the phases, π , can be replaced by two angles, ϕ and θ , under the phase matching criterion, which is the necessary condition for quantum searching with certainty. In other

words, the relation between ϕ and θ will affect the degree of success of quantum search algorithm. There have been several studies concern with the effect of imperfect phase rotations. In their paper [164], Long *et al.* have found that the tolerated angle difference between two phase rotations, δ , due to systematic errors in phase inversions, with a given expected degree of success P_{\max} , is about $2/\sqrt{NP_{\max}}$, where N is the size of the database. Høyer [166] has shown that after some number of iterations of Grover kernel, depending on N and unperturbed θ , it will give a solution with error probability $O(1/N)$ under a tolerated phase difference $\delta \sim O(1/\sqrt{N})$. The same result is also redrived by Biham *et al.* [171]. On the other hand, a near conclusion, $\delta \sim O(1/N^{2/3})$, is presented by Pablo-Norman and Ruiz-Altaba [172].

The result of Long *et al.* [164] is based on the approximate Grover kernel and an assumption: large N and small δ *et al.*. However, we found that the main inaccuracy comes from the approximate Grover kernel. Since all parameters in Grover kernel connect with each other exquisitely, any reduction to the structure of Grover's kernel would destroy this penetrative relation, so accumulative errors emerge from the iterations to a quantum search. Although this assumption lead their study to a proper result, it cannot be applied to general cases, e.g. any set of two angles in phase rotations satisfies phase matching condition [167, 168]. In what follows, we will get rid of the approximation to Grover kernel, then derive an improved criterion for tolerated error in phase rotation and the required number of qubits for preparing a database. Besides, a concise formula for evaluating minimum number of iterations to achieve a maximum probability will also be acquired. By this formula then evaluating the actual maximum probability, one can realize the derived criterion for tolerated error is near exactly [173].

Let the operator U is Walsh-Hadamard transformation W , the orthonormal set is

$$|I\rangle = |\tau\rangle \text{ and } |\tau_{\perp}\rangle = (W|\eta\rangle - W_{\tau\eta}|\tau\rangle)/l, \quad (9.24)$$

where $W_{\tau\eta} = \langle \tau | W | \eta \rangle$ and $l = (1 - |W_{\tau\eta}|^2)^{1/2}$. Furthermore, let $W_{\tau\eta} = \sin(\beta)$, we have

$$|s\rangle = W |\eta\rangle = \sin(\beta) |\tau\rangle + \cos(\beta) |\tau_{\perp}\rangle, \quad (9.25)$$

and the Grover kernel can now be written

$$\begin{aligned} G &= -I_{\eta} I_{\tau} \\ &= - \begin{bmatrix} e^{i\phi}(1 + (e^{i\theta} - 1) \sin^2(\beta)) & (e^{i\theta} - 1) \sin(\beta) \cos(\beta) \\ e^{i\phi}(e^{i\theta} - 1) \sin(\beta) \cos(\beta) & 1 + (e^{i\theta} - 1) \cos^2(\beta) \end{bmatrix}. \end{aligned} \quad (9.26)$$

After m number of iterations, the operator G^m can be expressed as

$$G^m = (-1)^m e^{im(\frac{\phi+\theta}{2})} \begin{bmatrix} e^{imw} \cos^2(x) + e^{-imw} \sin^2(x) & e^{-i\frac{\phi}{2}} i \sin(mw) \sin(2x) \\ e^{i\frac{\phi}{2}} i \sin(mw) \sin(2x) & e^{imw} \sin^2(x) + e^{-imw} \cos^2(x) \end{bmatrix}. \quad (9.27)$$

Then the probability of finding a marked state is

$$\begin{aligned} P &= 1 - |\langle \tau | G^m | s \rangle|^2 \\ &= 1 - (\cos(mw) \cos(\beta) - \sin(mw) \sin(\frac{\phi}{2}) \sin(2x) \sin(\beta))^2 \\ &\quad - \sin^2(mw) (\cos(\frac{\phi}{2}) \sin(2x) \sin(\beta) - \cos(2x) \cos(\beta))^2. \end{aligned} \quad (9.28)$$

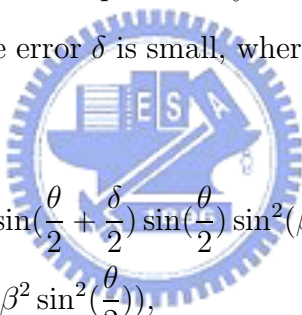
Moreover, by the equation $\partial P / \partial(\cos(mw)) = 0$, the minimum number of iterations for obtaining the maximum probability, $P_{\max}(\cos(m_{\min}w))$, is evaluated,

$$m_{\min}(\beta, \phi, \theta) = \frac{\cos^{-1}\left(\sqrt{\frac{b-2a}{2b}}\right)}{w}, \quad (9.29)$$

where

$$\begin{aligned}
 a &= \sin(2x) \cos(2\beta) + \cos(2x) \cos\left(\frac{\phi}{2}\right) \sin(2\beta), \\
 b &= (2 + \sin^2(2x) + (3 \sin^2(2x) - 2) \cos(4\beta) - 2 \sin^2(2x) \cos(\phi) \sin^2(2\beta)) \\
 &\quad + 2 \sin(4x) \cos\left(\frac{\phi}{2}\right) \sin(4\beta).
 \end{aligned}$$

For a sure-success search problem, the phase condition, $\phi = \theta$, provided iterations, $m_{\min} = (\pi/2 - \sin^{-1}(\sin(\phi/2) \sin(\beta)))/w$, is required. However, when effects of imperfect phase inversions are considered, the search is not certain, then the new condition to phase error, said $\delta = \phi - \theta$, and the size of database would be rederived in order to accomplish the search with a reduced maximum probability. Now, we suppose the database is large, i.e., if $\sin(\beta) \ll 1$, and a phase error δ is small, where $|\delta| \ll 1$, one will have the following approximation, viz.,



$$\begin{aligned}
 \cos(w) &= \cos\left(\frac{\delta}{2}\right) - 2 \sin\left(\frac{\theta}{2} + \frac{\delta}{2}\right) \sin\left(\frac{\theta}{2}\right) \sin^2(\beta) \\
 &\approx 1 - \left(\frac{\delta^2}{8} + 2\beta^2 \sin^2\left(\frac{\theta}{2}\right)\right), \\
 \sin(w) &= (1 - \cos^2(w))^{1/2} \\
 &\approx \frac{(\delta^2 + 16\beta^2 \sin^2(\frac{\theta}{2}))^{1/2}}{2}, \\
 \sin(2x) &= \frac{4\beta \sin(\frac{\theta}{2})}{(\delta^2 + 16\beta^2 \sin^2(\frac{\theta}{2}))^{1/2}}.
 \end{aligned}$$

The probability P (9.28) then has the approximation

$$\begin{aligned}
 P &\approx 1 - \cos^2(mw) \cos^2(\beta) - \sin^2(mw) \cos^2(2x) \\
 &= \sin^2(mw) \sin^2(2x),
 \end{aligned} \tag{9.30}$$

with a maximum value, by letting $\sin^2(mw) = 1$,

$$P_{\max} \approx \sin^2(2x) = \frac{16\beta^2 \sin^2(\frac{\theta}{2})}{\delta^2 + 16\beta^2 \sin^2(\frac{\theta}{2})} \tag{9.31}$$

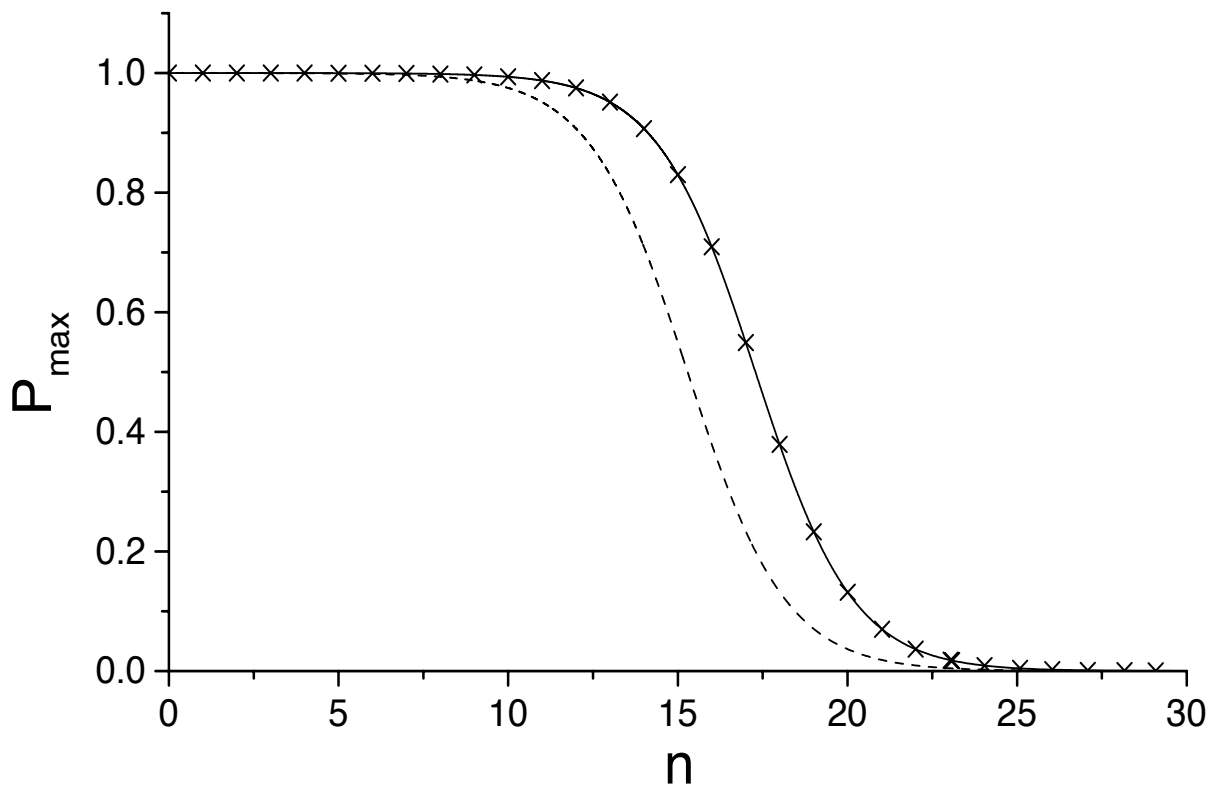


Figure 9.3: Variations of exact vaule of $P_{\max}(n)$ (cross marks), $16\beta^2 \sin^2(\frac{\theta}{2}) / (\delta^2 + 16\beta^2 \sin^2(\frac{\theta}{2}))$ (solid), and $4\beta^2 / (\delta^2 + 4\beta^2)$ (dash) for $\theta = \pi$, $\delta = 0.01$ where $\beta = \sin^{-1}(2^{-n/2})$.

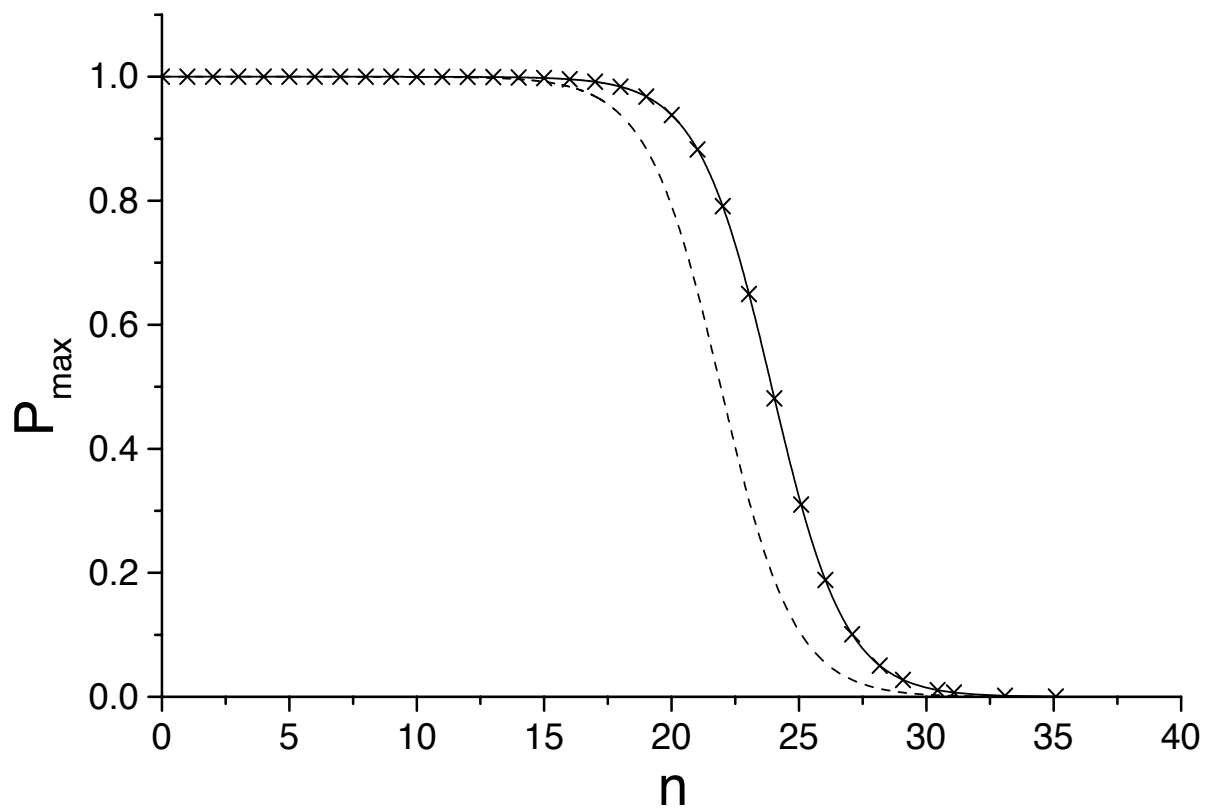


Figure 9.4: Variations of exact vaule of $P_{\max}(n)$ (cross marks), $\frac{16\beta^2 \sin^2(\frac{\theta}{2})}{\delta^2 + 16\beta^2 \sin^2(\frac{\theta}{2})}$ (solid), and $\frac{4\beta^2}{\delta^2 + 4\beta^2}$ (dash) for $\theta = \pi$, $\delta = 0.001$ where $\beta = \sin^{-1}(2^{-n/2})$.

The function (9.31) for two designations, $\delta = 0.01$ and $\delta = 0.001$, are depicted in Fig. 9.3 and Fig. 9.4 respectively.

Observing Fig. 9.3 and Fig. 9.4, one realizes the function (9.31) depicted by solid line coincides with the exact value, obtained by Eq. (9.28) and Eq. (9.29), shown by cross marks. On the contrary, the result of Long *et al.*,

$$P_{\max} \approx \frac{4\beta^2 \sin^2(\frac{\theta}{2})}{\delta^2 + 4\beta^2 \sin^2(\frac{\theta}{2})}, \quad (9.32)$$

is an underestimation depicted by dash lines.

9.4 On a family of quantum search algorithms robust against phase imperfections

Even in the case of large N , where high success rate in finding the marked state is expected by using the standard Grover's algorithm, inevitable noises including decoherence and gate inaccuracies can significantly affect the efficiency of the algorithm. To overcome such demerit we therefore should either apply the fault-tolerant computation [174] to reduce gate imperfections and decoherence, or limit the size of the quantum database to depress the effect of the uncertainty of the phase inversion operations. In another way, we can also, if possible, consider implementing a modified algorithm which is itself robust against phase imperfections and or decoherence. Recently, Hu [175] introduced an interesting family of algorithms for the quantum search. Although these algorithms are more complicated than the standard Grover's algorithm, they can be proved to be robust against imperfect phase inversions, so the limitation of the size of database can be greatly relieved. In what follows we therefore intend to analyze the algorithms introduced by Hu [175] in detail then show the robustness of the family in resisting the effect of imperfect phase inversions [176, 177].

If we denote the phase inversion of marked state $I_\tau = 1 + (e^{i\phi} - 1) |\tau\rangle \langle\tau|$ and the phase

inversion of the initial state $I_s = 1 + (e^{i\theta} - 1) |s\rangle \langle s|$, then the generalized Grover operator is given by $G = I_s I_\tau$ and in n iteration the unit probability for finding the marked state, viz., $|\langle \tau | G^n |s\rangle|^2 = 1$, is ensured if $\phi = \theta$. Instead of applying G^n on the initial state $|s\rangle$, Hu [175] presented and utilized the operators $A_{2n} = (I_s^\dagger I_\tau^\dagger I_s I_\tau)^n$ and $A_{2n+1} = G A_{2n}$ to accomplish a quantum search with certainty, and named the former the even member and the latter the odd member of the family $\{A_n, n = 1, 2, \dots\}$ because they require even ($2n$) and odd ($2n + 1$) oracle calls in computation, respectively. The arrangement $I_s^\dagger I_\tau^\dagger I_s I_\tau$ will be shown to have cancellation effect on phase errors in each iteration of the algorithm A_{2n} and A_{2n+1} and as a whole can ensure the robustness against imperfect phase inversion.

Consider a two-dimensional Hilbert space spanned by the marked state $|\tau\rangle$ and the state $|\tau_\perp\rangle$, which is orthogonal to $|\tau\rangle$. The initial state, as a uniform superposition of all states, then can be express by $|s\rangle = W |0\rangle = \sin(\beta) |\tau\rangle + \cos(\beta) |\tau_\perp\rangle$, where $\sin(\beta) \equiv \sqrt{M/N}$ and M is the number of the target states. The eigenvalues of the operator $I_s^\dagger I_\tau^\dagger I_s I_\tau$ are $\lambda_{1,2} = \cos(\omega) \pm i \sin(\omega)$ and the corresponding eigenvectors are computed

$$\begin{aligned} |\lambda_1\rangle &= \cos(x) |\tau\rangle + i \sin(x) e^{i(\frac{\phi}{2} - \gamma)} |\tau_\perp\rangle, \\ |\lambda_2\rangle &= i \sin(x) e^{-i(\frac{\phi}{2} - \gamma)} |\tau\rangle + \cos(x) |\tau_\perp\rangle, \end{aligned} \quad (9.33)$$

where the rotation x and the related parameters are defined by

$$\tan(x) = \frac{2r \sin(\frac{\phi}{2}) \sin(\frac{\theta}{2}) \sin(2\beta)}{\sin(\omega) + \sin^2(\frac{\theta}{2}) \sin(\phi) \sin^2(2\beta)}, \quad (9.34)$$

$$\cos(\omega) = 1 - 2 \sin^2(\frac{\theta}{2}) \sin^2(\frac{\phi}{2}) \sin^2(2\beta), \quad (9.35)$$

$$r e^{i\gamma} = \cos(\frac{\theta}{2}) + i \sin(\frac{\theta}{2}) \cos(2\beta). \quad (9.36)$$

Then in n iterations of the operator of $I_s^\dagger I_\tau^\dagger I_s I_\tau$ we will have $A_{2n} = (I_s^\dagger I_\tau^\dagger I_s I_\tau)^n = \lambda_1^n |\lambda_1\rangle \langle \lambda_1| + \lambda_2^n |\lambda_2\rangle \langle \lambda_2|$, which can be expressed in the following matrix form:

$$A_{2n} = \begin{bmatrix} \cos(n\omega) + i \sin(n\omega) \cos(2x) & \sin(2x) \sin(n\omega) e^{-i(\frac{\phi}{2} - \gamma)} \\ -\sin(2x) \sin(n\omega) e^{i(\frac{\phi}{2} - \gamma)} & \cos(n\omega) - i \sin(n\omega) \cos(2x) \end{bmatrix}, \quad (9.37)$$

where $\sin(2x)$ and $\cos(2x)$ can be computed in use of the definition (9.34) and given by

$$\sin(2x) = \left(\frac{1 - \sin^2(\frac{\theta}{2}) \sin^2(2\beta)}{1 - \sin^2(\frac{\theta}{2}) \sin^2(\frac{\phi}{2}) \sin^2(2\beta)} \right)^{1/2}, \quad (9.38)$$

$$\cos(2x) = \frac{\sin(\frac{\theta}{2}) \cos(\frac{\phi}{2}) \sin(2\beta)}{(1 - \sin^2(\frac{\theta}{2}) \sin^2(\frac{\phi}{2}) \sin^2(2\beta))^{1/2}}. \quad (9.39)$$

When the quantum search is carried out by using the even member A_{2n} , the component of the final state after n iterations of $(I_s^\dagger I_\tau^\dagger I_s I_\tau)$ in the basis state $|\tau_\perp\rangle$ is expressed by $\langle \tau_\perp | A_{2n} | s \rangle = RE_e + iIM_e$, and accordingly the exact success rate in finding the marked state $|\tau\rangle$ then is given by

$$p = 1 - |\langle \tau_\perp | A_{2n} | s \rangle|^2 = 1 - (RE_e^2 + IM_e^2), \quad (9.40)$$

where

$$RE_e = \cos(n\omega) \cos(\beta) - \sin(n\omega) \sin(2x) \cos\left(\frac{\phi}{2} - \gamma\right) \sin(\beta), \quad (9.41)$$

$$IM_e = -\frac{\sin(n\omega) \sin(\beta)}{(1 - \sin^2(\frac{\theta}{2}) \sin^2(\frac{\phi}{2}) \sin^2(2\beta))^{1/2}} \sin\left(\frac{\theta + \phi}{2}\right). \quad (9.42)$$

It is clear that when $IM_e = 0$, one obtains the n -independent phase matching condition, $\phi = -\theta$, for A_{2n} , and the success rate then becomes

$$p = 1 - RE_e^2 = 1 - \cos^2(n\omega - \alpha), \quad (9.43)$$

where $\alpha = \sin^{-1}(\sin(\beta) \cos(\phi/2 + \gamma))$. The 100% success rate for the search problem can be achieved as by letting $\cos(n\omega - \alpha) = 0$. For a search with certainty, since n is a positive integer, one therefore has to expect the iteration number given by

$$n_e(\theta, \beta) = \lceil f_e(\theta, \beta) \rceil, \quad (9.44)$$

and the function $f_e(\theta, \beta)$ is given by

$$f_e(\theta, \beta) = \frac{\frac{\pi}{2} + \alpha(\theta, \beta)}{\omega(\theta, \beta)}. \quad (9.45)$$

Given β , the function f_e has its minimal value as $\theta = \pi$ (and $\phi = -\pi$ thereby), as if minimal oracle calls are demanded in the computation, we should have the optimal phase θ_{op} associated with

$$f_e(\theta_{op}, \beta) = [f_e(\pi, \beta)]. \quad (9.46)$$

For example, if given $\beta = 1$, we have $[f_e(\pi, 1)] = 1$, and the optimal phase angle $\theta_{op} = \pi \pm 1.304$ follows in the algorithm using the even member A_{2n} . In usual operation, however, the quantum database is large, i.e., $\sin(\beta) \ll 1$, and the phase $\theta = \pi$ and $\phi = -\pi$ are fixed, then the required iterations are estimated by $n \sim \pi/8\beta$ and by (9.46) the maximal success rate will be approximately evaluated

$$p_{\max} \sim 1 - \beta^2, \text{ for } \theta = \pi,$$

which is the same result obtained as if the standard Grover algorithm is implemented. That is, as the phase $\theta = \pi$ is fixed, the present algorithm (A_{2n}) is equivalent to the standard algorithm (G^m) with even oracle calls required in the computation. Nevertheless, since in a real operation, imperfections in the phase inversions are inevitable. In what follows, we will show that the present algorithm is robust against small phase imperfections in a quantum computation and provides a maximal success rate that is similar to the one given above.

In the absence of decoherence and error correction, we considered constant phase errors causing the phase ϕ and θ to be $\phi = \pi + \phi_e$ and $\theta = \pi + \theta_e$, where $|\phi_e| \ll 1$ and $|\theta_e| \ll 1$. By introducing the constant phase imperfections, one then have the following

approximations, when $\beta \ll 1$,

$$\begin{aligned}\sin(2x) &\sim 1 - \frac{1}{2}\beta^2\phi_e^2, \cos(2x) \sim \beta\phi_e, \\ \cos\left(\frac{\phi}{2} - \gamma\right) &\sim -1 + \frac{1}{8}(\theta_e - \phi_e)^2, \sin\left(\frac{\phi}{2} - \gamma\right) \sim \frac{1}{2}(\theta_e - \phi_e), \\ \omega &\sim 4\beta\left(1 - \frac{1}{8}(\theta_e^2 + \phi_e^2) + \frac{4}{3}\beta^2\right).\end{aligned}$$

Then, since the errors are unknown in advance of the computation, the iteration number is also considered to be $n \sim \pi/8\beta$, and we thus have $\cos(n\omega) \sim \pi(\theta_e^2 + \phi_e^2)/16 - 2\pi\beta^2/3$ and $\sin(n\omega) \sim 1$. The approximation of RE_e and IM_e accordingly are evaluate by

$$\begin{aligned}RE_e &\sim \beta + \frac{\pi}{16}(\theta_e^2 + \phi_e^2) - \frac{2}{3}\pi\beta^2, \\ IM_e &\sim -\frac{1}{2}\beta(\theta_e + \phi_e).\end{aligned}\tag{9.47}$$

The maximal success rate, in uses of expression (9.40)-(9.42), now is approximately derived by

$$p_{\max} \sim 1 - \beta^2 - (\text{H.O.T.}),\tag{9.48}$$

where H.O.T. represents high order terms higher than second-degree in the small parameters β, θ_e and ϕ_e . Expression (9.48) clearly tells that the reduction of the probability due to the introduction of the phase errors in fact can almost be neglected. Then, through it, we can see that the present algorithm is robust against systematic phase imperfections.

The analysis of the algorithm using the odd member A_{2n+1} can be undertaken by the same procedure as in analyzing the even member. In this case, we have

$$p_{\max} = 1 - (RE_o^2 + IM_o^2),\tag{9.49}$$

where

$$\begin{aligned}
 RE_o &= \cos(nw) \left[\cos\left(\frac{\theta - \phi}{2}\right) - 4 \sin\left(\frac{\theta}{2}\right) \sin\left(\frac{\phi}{2}\right) \sin^2(\beta) \right] \cos(\beta) \\
 &+ \sin(nw) \left\{ \cos(2x) \left[\sin\left(\frac{\theta - \phi}{2}\right) - 4 \sin\left(\frac{\theta}{2}\right) \sin\left(\frac{\phi}{2}\right) \sin^2(\beta) \right] \cos \beta \right. \\
 &- \left. \sin(2x) \left[\cos\left(\gamma + \frac{\theta}{2}\right) + 4 \sin(\gamma) \sin\left(\frac{\theta}{2}\right) \cos^2(\beta) \right] \sin \beta \right\}, \\
 IM_o &= \cos(\beta) \sin\left(\frac{\theta - \phi}{2}\right) \left(\cos(nw) - \sin(nw) \frac{\cos(2x) \sin\left(\frac{\phi}{2}\right)}{\cos\left(\frac{\phi}{2}\right)} \right). \tag{9.50}
 \end{aligned}$$

Letting $IM_o = 0$, one has the phase matching condition, $\phi = \theta$, for A_{2n+1} . The 100% success rate then can be ensured when the iteration steps at $n_o(\theta, \beta) = \lceil f_o(\theta, \beta) \rceil$, where

$$\begin{aligned}
 &f_o(\theta, \beta) \\
 = &\frac{\frac{\pi}{2} - \cos^{-1}\left(\frac{\cos(\beta)(1 - 4 \sin^2(\frac{\theta}{2}) \sin^2(\beta)) \sqrt{1 - \sin^4(\frac{\theta}{2}) \sin^2(2\beta)}}{\sqrt{1 - \sin^2(\frac{\theta}{2}) \sin^2(2\beta)}}\right)}{\omega(\theta, \beta)}. \tag{9.51}
 \end{aligned}$$

Note that in this case the inequality $1 - 4 \sin^2(\theta/2)^2 \geq 0$ should be demanded since then the meaningful requirement $f_o \geq 0$ can then be fulfilled. Given β , the function $f_o(\theta, \beta)$ also has its minimal value at $\theta = \pi$ (then $\phi = \pi$), as the optimal choice of the phase θ_{op} should be estimated by

$$f_o(\theta_{op}, \beta) = \lceil f_o(\theta, \beta) \rceil, \tag{9.52}$$

when minimal oracle calls are demanded in a search with certainty. For $\beta = 1$, the choice of the phase should be $\theta_{op} = \phi_{op} = \pi \pm 1.870$, for example. The standard Grover algorithm with odd oracle calls can be recovered when $\theta = \phi = \pi$ is fixed. In usual operations, when phase imperfections are introduced, i.e., as $\theta = \pi + \theta_o$ and $\phi = \pi + \phi_o$, where both θ_o and ϕ_o are small errors in the phases, they also produce almost negligible reductions in the success rate as given by an expression like Eq. (9.48).

9.5 Hamiltonian and measuring time for analog quantum search

Several researchers have proposed other ways to solve the quantum search problem, such as the *analog analogue* version of the Grover's algorithm [178–180] and the adiabatic evolution to quantum search [181–183]. The former is to be considered in this work. It is proposed that the quantum search computation can be accomplished by controlled Hamiltonian time evolution of a system, obeying the Schrödinger equation

$$i \frac{d|\Psi(t)\rangle}{dt} = H |\Psi(t)\rangle, \quad (9.53)$$

where the constant $\hbar = 1$ is imposed for convenience. Farhi and Gutmann [178] presented the time-independent Hamiltonian $H_{fg} = E_{fg}(|w\rangle\langle w| + |s\rangle\langle s|)$, where $|w\rangle$ is the marked state and $|s\rangle$ denotes the initial state. Later, Fenner [179] proposed another Hamiltonian $H_f = E_f i(|w\rangle\langle s| - |s\rangle\langle w|)$. Recently, Bae and Kwon [180] further derived a generalized quantum search Hamiltonian

$$H_g = E_{fg}(|w\rangle\langle w| + |s\rangle\langle s|) + E_f(e^{i\phi}|w\rangle\langle s| + e^{-i\phi}|s\rangle\langle w|), \quad (9.54)$$

where ϕ is an additional phase to the Fenner Hamiltonian. Unlike the Grover algorithm, which operates on a state in discrete time, a quantum search Hamiltonian leads to the evolution of a state in continuous time, so the 100% probability for finding the marked state can be guaranteed in the absence of all kinds of imperfection occurring in a quantum operation. Both the Hamiltonian H_{fg} and H_f can help to find the marked state with 100% success. However, Bae and Kwon [180] addressed that the generalized Hamiltonian H_g can accomplish the search with certainty only when $\phi = n\pi$ is imposed, where n is arbitrary integer. In this work, however, we will show that the generalized Hamiltonian H_g can be derived by an analytical method, which is distinct to the one implemented by Bae and Kwon [180], and the same method will lead to arbitrary chosen phase ϕ , depending on

when the measurement on the system is undertaken and how large the system energy gap is provided. Since Hamiltonian-controlled system is considered, the energy-time relation will play an essential role in the problem. Therefore, the evaluation of the measuring time for the quantum search becomes crucially important. In this study, we will derive the general Hamiltonian for the time-controlled quantum search system first. Then the exact time for measuring the marked state will be deduced. Finally, the role played by the phase ϕ in the quantum search will be discussed, and both the measuring time and the system energy gap as variations with ϕ will be given [184].

Suppose that a two-dimensional, complex Hilbert space is spanned by the orthonormal set $|w\rangle$, which is the marked state, and $|w_\perp\rangle$, which denotes the unmarked one. An initial state $|s\rangle = |\Psi(0)\rangle$ is designed to evolve under a time-independent quantum search Hamiltonian given by

$$H = E_1 |E_1\rangle \langle E_1| + E_2 |E_2\rangle \langle E_2|, \quad (9.55)$$

where E_1 and E_2 are two eigenenergies of the quantum system, $E_1 > E_2$, and $|E_1\rangle$ and $|E_2\rangle$ are the corresponding eigenstates satisfying the completeness condition $|E_1\rangle \langle E_1| + |E_2\rangle \langle E_2| = \mathbf{1}$. The eigenstates can be assumed by

$$\begin{aligned} |E_1\rangle &= e^{i\alpha} \cos(x) |w\rangle + \sin(x) |w_\perp\rangle, \\ |E_2\rangle &= -\sin(x) |w\rangle + e^{-i\alpha} \cos(x) |w_\perp\rangle. \end{aligned} \quad (9.56)$$

where x and α are two parameters to be determined later based on the required maximal probability for measuring the marked state. By the assumptions given in (9.56), the Hamiltonian can be written in the matrix form

$$H = \begin{bmatrix} E_p + E_o \cos(2x) & E_o \sin(2x) e^{i\alpha} \\ E_o \sin(2x) e^{-i\alpha} & E_p - E_o \cos(2x) \end{bmatrix}. \quad (9.57)$$

where $E_p = (E_1 + E_2)/2$ is the mean of eigenenergies and $E_o = (E_1 - E_2)/2$ represents half

of the system energy gap. The major advantage of using the controlled Hamiltonian time evolution is that the marked state can always be searched with certainty in the absence of quantum imperfections. The crucial key of the present problem in turn is to decide when to measure the marked state by the probability of unity. So in what follows we will in detail deduce the relation between all the unknown appearing in the system and then evaluate the exact measuring time for finding the marked state with certainty.

The time evolution of the initial state is given by $|\Psi(t)\rangle = e^{-iHt} |s\rangle$. Therefore, the probability of finding the marked state will be $P = |\langle w | e^{-iHt} |s\rangle|^2 = 1 - |\langle w_\perp | e^{-iHt} |s\rangle|^2$. Without loss of generality, let us consider the problem of searching one target from N unsorted items. The general form of the initial state considered in this study is given by

$$|s\rangle = e^{iu} \sin(\beta) |w\rangle + \cos(\beta) |w_\perp\rangle, \quad (9.58)$$

where $\sin(\beta) \equiv 1/\sqrt{N}$ and u denotes the relative phase between the two components in the initial state. Note that the relative phase u may arise from a phase decoherence or an intended design during the preparation of the initial state. Now, because of $e^{-iHt} = e^{-iE_1t} |E_1\rangle \langle E_1| + e^{-iE_2t} |E_2\rangle \langle E_2|$, using the expressions given in (56) and (58), we can deduce

$$\begin{aligned} \langle w_\perp | e^{-iHt} |s\rangle &= e^{-iE_p t} ((\cos(\beta) \cos(E_o t) - \sin(\alpha - u) \sin(2x) \sin(\beta) \sin(E_o t)) \\ &\quad + i(\cos(2x) \cos(\beta) - \cos(\alpha - u) \sin(2x) \sin(\beta)) \sin(E_o t)). \end{aligned} \quad (9.59)$$

To accomplish the quantum search with maximal probability, the time-independent term $(\cos(2x) \cos(\beta) - \cos(\alpha - u) \sin(2x) \sin(\beta))$ in (9.59) must vanish and thus the unknown x can be determined by

$$\cos(2x) = \frac{\sin(\beta) \cos(\alpha - u)}{\cos(\gamma)}, \text{ or } \sin(2x) = \frac{\cos(\beta)}{\cos(\gamma)}, \quad (9.60)$$

where γ is defined by $\sin(\gamma) = \sin(\beta) \sin(\alpha - u)$. The probability for finding the marked

state then becomes

$$\begin{aligned}
 P &= 1 - |\langle w_\perp | e^{-iHt} |s\rangle|^2 \\
 &= 1 - \frac{\cos^2(\beta)}{\cos^2(\gamma)} \cos^2(E_0 t + \gamma).
 \end{aligned} \tag{9.61}$$

Usually, if the size of database N is large, then $\gamma \ll 1$ and the marked state $|w\rangle$ will be measured at $t = \pi/(2E_o)$ by a probability $p = 1 - \tan^2 \gamma \sim 1$, according to (9.61). Expression (9.61) also indicates that, by letting $\cos^2(E_0 t + \gamma) = 0$, we can measure the marked state with unit probability, no matter how large N is, at the time instants

$$t_j = \frac{(2j - 1)\pi/2 - \sin^{-1}(\sin(\beta) \sin(\alpha - u))}{E_o}, \quad j = 1, 2, \dots \tag{9.62}$$

In what follows, let us only focus on the first instant $t_1 = (\pi/2 - \sin^{-1}(\sin(\beta) \sin(\alpha - u)))/E_o$. It is clear that a larger E_o , or equivalently a larger system energy gap, will lead to a shorter time for measuring the marked state with certainty. Meanwhile, as can be seen in (9.61), the probability for measuring the marked state varies with time as a periodic function whose frequency is the Bohr frequency E_o/π , so a larger E_o will also result in a more difficult control on the measuring time. In other words, the measuring time should be controlled more precisely for a higher Bohr frequency in the state evolution since then a small error in the measuring time will cost a serious drop of the probability. However, the energy gap E_o depends on the size of database N , as will be mentioned later.

With the relations shown in (9.60), the present Hamiltonian now can be written by

$$H = \begin{bmatrix} E_p + E_o \frac{\sin(\beta) \cos(\alpha - u)}{\cos(\gamma)} & E_o \frac{\cos(\beta)}{\cos(\gamma)} e^{i\alpha} \\ E_o \frac{\cos(\beta)}{\cos(\gamma)} e^{-i\alpha} & E_p - E_o \frac{\sin(\beta) \cos(\alpha - u)}{\cos(\gamma)} \end{bmatrix}, \tag{9.63}$$

which is represented in terms of the energies E_p and E_o and the phase α . Alternatively,

if we let

$$\begin{aligned} E_{fg} &= \frac{(E_p - E_o \frac{\sin(\beta) \cos(\alpha-u)}{\cos(\gamma)})}{\cos^2(\beta)}, \\ E_f e^{i(\phi-u)} &= \frac{E_o}{\cos(\gamma)} e^{i(\alpha-u)} - E_{fg} \sin(\beta), \end{aligned} \quad (9.64)$$

or inversely,

$$\begin{aligned} E_p &= E_{fg} + E_f \cos(\phi - u) \sin(\beta), \\ E_o &= ((E_f \cos(\phi - u) + E_{fg} \sin(\beta))^2 \\ &\quad + E_f^2 \sin^2(\phi - u) \cos^2(\beta))^{\frac{1}{2}}, \end{aligned} \quad (9.65)$$

then the Hamiltonian can also be expressed by

$$H = \begin{bmatrix} E_{fg}(1 + \sin^2(\beta)) + 2E_f \cos(\phi - u) \sin(\beta) & e^{iu}(E_f e^{i(\phi-u)} + E_{fg} \sin(\beta)) \cos(\beta) \\ e^{-iu}(E_f e^{-i(\phi-u)} + E_{fg} \sin(\beta)) \cos(\beta) & E_{fg} \cos^2(\beta) \end{bmatrix}, \quad (9.66)$$

which in turn is represented in terms of the energies E_{fg} and E_f and the phase ϕ . The Hamiltonian shown in (9.66) in fact can be expressed as $H_g = E_{fg}(|w\rangle\langle w| + |s\rangle\langle s|) + E_f(e^{i\phi}|w\rangle\langle s| + e^{-i\phi}|s\rangle\langle w|)$, which is exactly of the same form as the Bae and Kwon Hamiltonian H_g shown in (9.54). However, Bae and Kwon [180] only consider the case $u = 0$. In both the presentations (9.63) and (9.66) of the Hamiltonian H , the corresponding measuring time for finding the marked state $|w\rangle$ with certainty is at

$$\begin{aligned} t_1 &= \frac{\frac{\pi}{2} - \sin^{-1}(\sin(\beta) \sin(\alpha - u))}{E_o} \\ &= \frac{\frac{\pi}{2} - \sin^{-1}\left(\frac{E_f \sin(\beta) \sin(\phi-u)}{((E_f \cos(\phi-u) + E_{fg} \sin(\beta))^2 + E_f^2 \sin^2(\phi-u))^{\frac{1}{2}}}\right)}{((E_f \cos(\phi - u) + E_{fg} \sin(\beta))^2 + E_f^2 \sin^2(\phi - u) \cos^2(\beta))^{\frac{1}{2}}}. \end{aligned} \quad (9.67)$$

Equation (9.67) indicates that when the phase difference $\alpha - u$, or $\phi - u$, is imposed and the energy gap E_o or the energies E_f and E_{fg} are provided, the measurement at

the end of a search should be undertaken at the instant t_1 . To discuss further, we first consider the case $u = 0$, i.e., the case where neither phase decoherence nor intended relative phase is introduced in the preparation of the initial state $|s\rangle$. If $\phi = n\pi$, or $\alpha = n\pi$, is imposed, then the present Hamiltonian reduces to that considered by Bae and Kwon [180] to serve for a search with certainty when the measurement is undertaken at $t_1 = \pi/(2E_o) = \pi/(2|(-1)^n E_f + E_{fg} \sin(\beta)|)$. If $E_f = 0$, or if $E_o = E_{fg} \sin(\beta)$ and $\alpha = 0$, is imposed, then the present Hamiltonian reduces to the Farhi and Gutmann Hamiltonian H_{fg} , which serves for a search with certainty at $t_1 = \pi/(2E_o) = \pi/(2E_{fg} \sin \beta)$. Further, when $E_{fg} = 0$ and $\phi = \pi/2$, or $E_p = 0$ and $\alpha = \pi/2$ is chosen, the present Hamiltonian will reduce to the Fenner Hamiltonian H_f associated with the measuring time $t_1 = (\pi - 2\beta)/(2E_o) = (\pi - 2\beta)/(2E_f \cos \beta)$. In general, the phase ϕ , or α , in fact can be imposed *arbitrary* for a search with certainty as the condition $u = 0$ is imposed.

However, if inevitable phase decoherence in the preparation of the initial state $|s\rangle$ is considered, then the phase u must be assumed to be arbitrary. Accordingly, the probability for finding the marked state will not be unity at all. For example, if following Bae and Kwon [180] by letting $t_1 = \pi/(2E_o)$, then we only have a probability for finding the marked state given by

$$p = 1 - \frac{\cos^2(\beta) \sin^2(\beta) \sin^2(u)}{1 - \sin^2(\beta) \sin^2(u)}. \quad (9.68)$$

It is easy to show that the probability shown in (9.68) is always greater than or equal to the lower bound $p_{min} = 1 - \sin^2(\beta) = 1 - 1/N$. Of course, if the nonzero phase u is introduced by an intended design, not an inevitable phase decoherence, then a search with certainty can be accomplished for an arbitrary ϕ , or α , when associated with the measuring time shown in (9.67). For example, if $u = \pi/2$ is the phase designated, the ideal measuring time should be $t_1 = (\pi - 2\beta)/(2E_o)$, which is the same as the Fenner's t_1 . Again if the phase decoherence is introduced into the system and changes the phase from $\pi/2$ to an undesired u , then one eventually obtains a poor probability $p = 1 - (1 + \sin^2(u) - 2 \sin(u)) \sin^2(\beta)$.

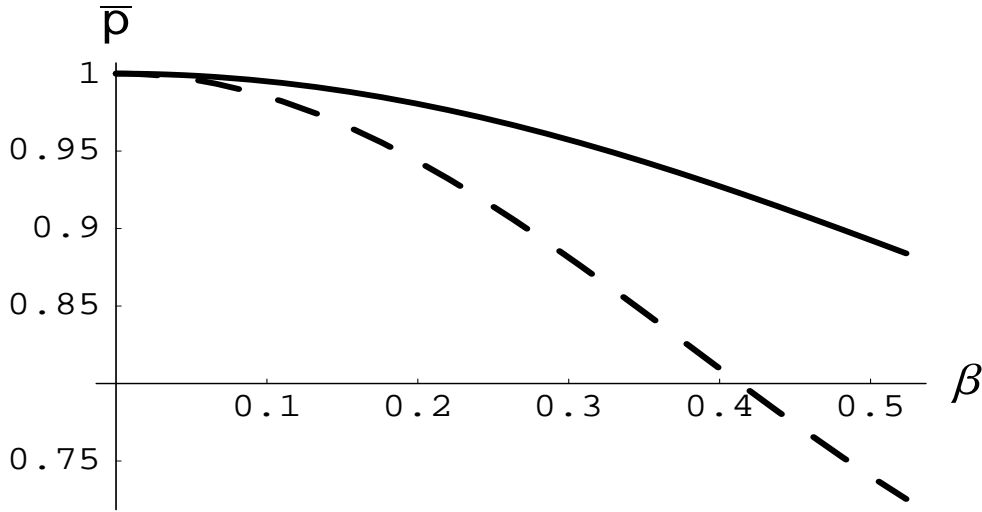


Figure 9.5: The variation of $\bar{p}(\beta)$ for cases of Bae-Kwon(solid), Farhi-Gutmann(solid), and Fenner(broken) at the specific measuring times, $t_{1,BK} = t_{1,FG} = \pi/(2E_o)$ and $t_{1,F} = (\pi - 2\beta)/(2E_o)$.

Moreover if the phase error occurs randomly in a quantum database, then we cannot be sure when to take a measurement, and the probability for finding the marked state even drops off seriously in some cases. For investigating the effect of the random uncontrollable parameter u on p at a fixed measuring time, we average over all possible values of $p(\beta, u)$ about all arbitrary values of phase parameter u . Fig. 9.5 shows the variation of the mean probability \bar{p} with β for cases of Bae-Kwon, Farhi-Gutmann and Fenner at the specific measuring times, $t_{1,BK} = t_{1,FG} = \pi/(2E_o)$ and $t_{1,F} = (\pi - 2\beta)/(2E_o)$, those Hamiltonian suggest in such a case. The same character of their proposals is that \bar{p} is sensitive to a phase decoherence as the database is small. The mean success probabilities of Bae-Kwon and Farhi-Gutmann are the same and always greater than the one of Fenner. Then the Hamiltonians presented by Bae and Kwon, and Farhi and Gutmann are more robust against the phase decoherence than the one proposed by Fenner especially for low values of N .

Now we proceed to give a brief review on the comparison between E_{fg} and E_f , which has been discussed in Ref. [185], and to recall the implication behind the analog quantum

search first presented by Farhi and Gutmann [178]. Suppose there is a $(N - 1)$ -fold degeneracy in a quantum system and its Hamiltonian is read as $H_0 = E |w\rangle \langle w|$, then our assignment is to find the unknown state $|w\rangle$. Since one does not yet know what $|w\rangle$ is, it is natural to add a well known Hamiltonian, $H_D = E |s\rangle \langle s|$, such that the initial state of the system $|s\rangle$ can be drove into $|w\rangle$. The total Hamiltonian therefore becomes $H = H_0 + H_D = E(|w\rangle \langle w| + |s\rangle \langle s|)$, which is just the Hamiltonian of Farhi and Gutmann [178] H_{fg} . It can be simplified under the large database limit,

$$H_{fg} \approx E(|w\rangle \langle w| + |s\rangle \langle s|) + E \sin(\beta)(|w\rangle \langle s| + |s\rangle \langle w|). \quad (9.69)$$

From it one can realize that the driving Hamiltonian induces transitions between $|w\rangle$ and $|s\rangle$ with a mixing amplitude $O(E \sin(\beta))$, which causes $|s\rangle$ to evolve to $|w\rangle$. By Eq. (9.65), thus it is rational to assume $E_f \sim E_{fg} \sin(\beta)$, and therefore the energy gap E_o should be proportional to $\sin \beta$, or $1/\sqrt{N}$. The measuring time then is easily found to be $t_1 \propto \sqrt{N}$ from Eq. (9.67). However, if consider the case $E_f \gg E_{fg}$, like the extreme situation considered by Fenner [179], then we encounter with $E_o \sim E_f \cos(\phi - u)$ and accordingly the measuring time t_1 is independent of the size of database N . Therefore, in an usual case the assumption $E_f \sim E_{fg} \sin(\beta)$ is reasonable.

An interesting phenomenon occurs when the critical condition $E_f = E_{fg} \sin(\beta)$ is considered. Fig. 9.6 shows the variations of t_1 and E_o with the phase difference $\phi - u$ in such a case. It is observed that when $\phi - u = \pm\pi$ the energy gap E_o becomes zero and then the eigenstates of the quantum search system correspond to the common eigenvalue $E = E_1 = E_2$ and become degenerate. In such case, the Hamiltonian becomes proportional to the identity $\mathbf{1}(= |w\rangle \langle w| + |w_\perp\rangle \langle w_\perp|)$. Therefore, the initial state $|s\rangle$ does not evolve at all and the probability for finding the marked state $|w\rangle$ indeed is the initial one, viz., $p = \sin^2(\beta) = 1/N$, which can also be deduced using Eq. (61). In other words, the quantum search system is totally useless as long as $\phi - u = \pm\pi$ is imposed under the critical condition $E_f = E_{fg} \sin(\beta)$. When $\phi - u \neq \pm\pi$, both t_1 and E_o are finite, as

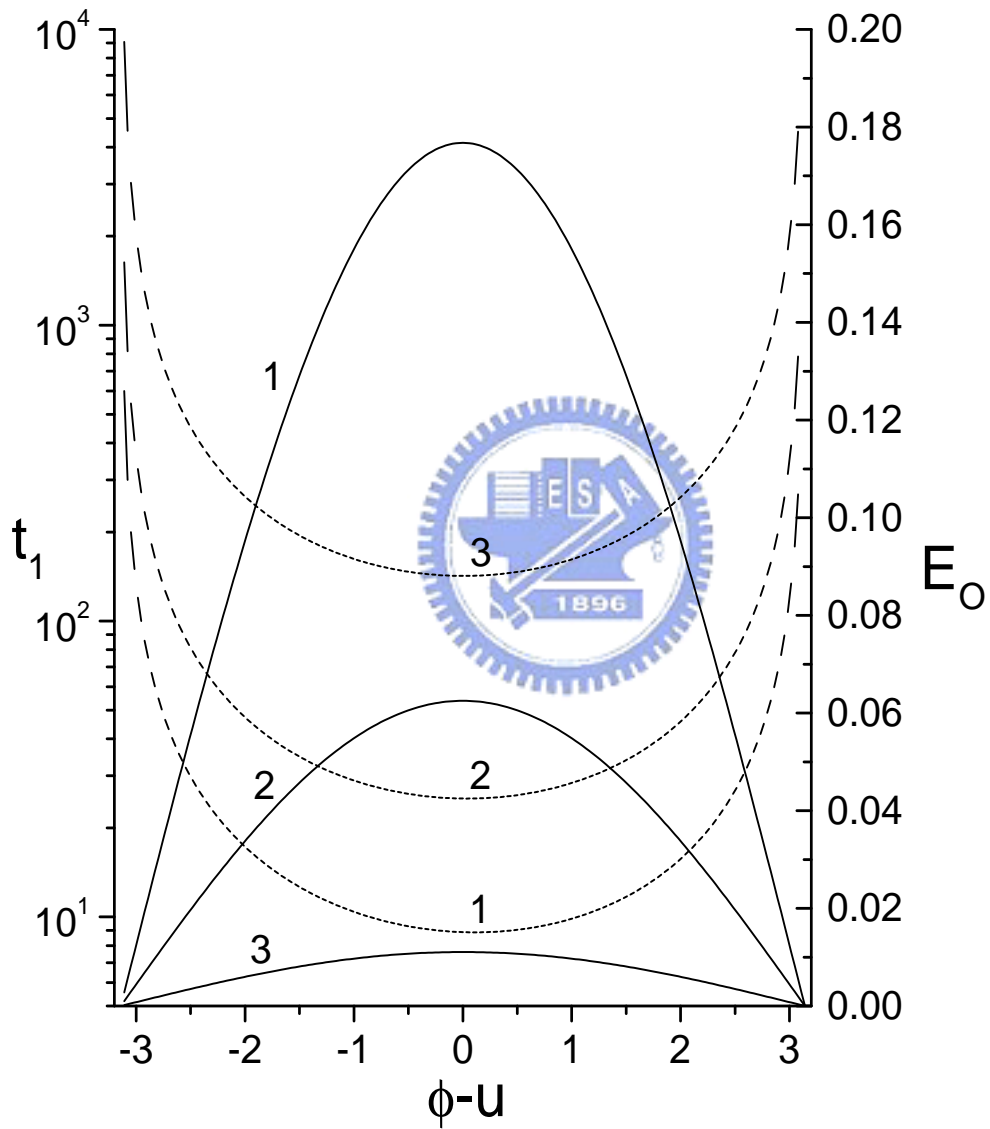


Figure 9.6: Variations of $t_1(\phi - u)$ (broken) and $E_o(\phi - u)$ (solid), for $\beta = 0.085$ (1), $\beta = 0.031$ (2), and $\beta = 0.0055$ (3).

can be seen from Fig. 9.6, and therefore the quantum search system becomes efficient again and is capable of finding the marked state with certainty, especially when the phase difference is imposed around $\phi - u = 0$. As a conclusion, for an efficient, useful quantum search system, the critical condition mentioned above should be avoided and in fact the reasonable condition $E_f \sim E_{fg} \sin(\beta)$ is recommended to be imposed.



Chapter 10

Experimental generation of hyperentangled photons and experimental realization of one-way quantum computing



10.1 Introduction

Cluster states have recently received enormous attentions in the field of quantum information and are important for one-way universal quantum computing [31–33]. Moreover, with highly robustness they are also essential for quantum error correction codes and quantum communication protocols [187, 188]. Many efforts have been stepped toward generating and characterizing cluster states in linear optics [52, 53, 99, 189–192]. Recently the principal feasibility of one-way quantum computing model has been experimentally demonstrated through 4-photon cluster state successfully [52, 53, 62].

In this chapter we show an experimental realization of one-way quantum computing with a 2-photon 4-qubit cluster state. We develop and employ a bright cluster state source which produces a 2-photon state entangled both in polarization and spacial modes.

The Grover's search algorithm is demonstrated with highly performances. The genuine four-partite entanglement and high fidelity of better than 88% for this cluster state are characterized and verified by measurement of an optimal entanglement witness with two local measurement settings. Inheriting the intrinsic two-photon character, compare with the one using multi-photon, our scheme promises a brighter source in quantum computing by more than 4 orders of magnitude, which offers a significantly high efficiency for optical quantum computing. It thus provides a simple and fascinating alternative to complement the usual multi-photon cluster state [54].

10.2 Photon source for polarization entanglement

First, we will give an introduction to the photon source used for creation of polarization entangled photons. We use parametrically driven nonlinear media to generate nonclassical light via a type-I spontaneous parametric down-conversion (SPDC) process [98]. Photons from the pump beam are converted into two photons that emitted from the beta-barium borate (BBO) crystal along different directions. The emitted photons, say signal and idler photons respectively, satisfy phase matching conditions:

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i, \quad (10.1)$$

for energy conservation, where ω_p , ω_s , and ω_i denote the frequencies of the pump, signal, and idler respectively, and

$$\hbar\mathbf{k}_p = \hbar\mathbf{k}_s + \hbar\mathbf{k}_i, \quad (10.2)$$

for momentum conservation, where \mathbf{k}_p , \mathbf{k}_s , and \mathbf{k}_i represent the respective wave vectors. Since the constrain of phase matching conditions, the signal and idler photon emitted from the crystal on opposite sides of concentric cones centered on the direction of the pump beam. The signal and idler photons possess the same polarization but are orthogonal

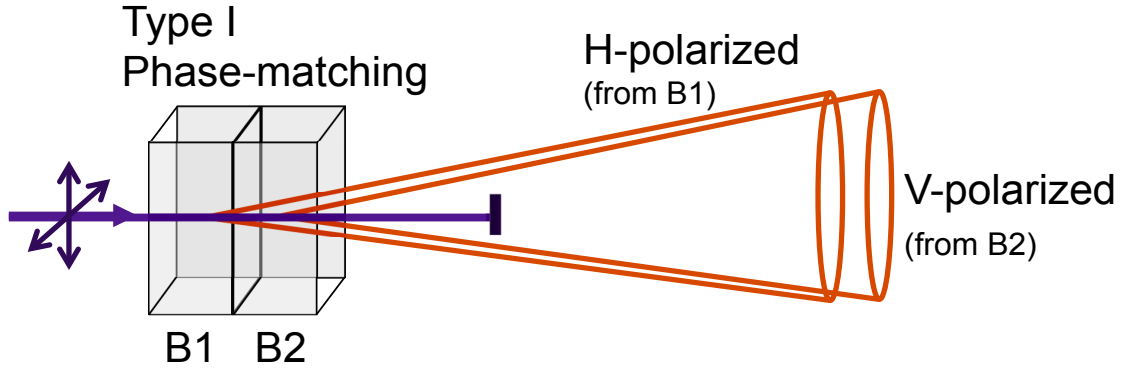


Figure 10.1: Polarization photon source with two-crystal geometry BBO crystals

to that of the pump beam. This process can be described by the following interaction Hamiltonian

$$H_I = \hbar\gamma a_s^\dagger a_i^\dagger + \text{H.c.}, \quad (10.3)$$

where $\gamma \propto \eta_p \chi^{(2)}$, η_p denotes the amplitude of the classical coherent field and $\chi^{(2)}$ is the second-order nonlinear susceptibility of the BBO crystal, and a_s^\dagger and a_i^\dagger represent the creation operators of the signal and idler beams respectively.

We use the nonlinear media with two-crystal geometry as shown in Fig. 10.1 to create polarization photons [98]. The BBO crystals with the type-I phase-matching condition are adjacent and relatively thin, and they are oriented with their optic axes aligned in perpendicular planes. With the type-I phase-matching, a pump beam with vertical polarization will produce horizontally polarized photon pairs, and this process of down conversion occurs only in the first crystal (see Fig. 10.2). Using a horizontally polarized pump beam, down conversion process will only in the second crystal and vertically polarized photon pairs are created (see Fig. 10.3).

If a geometry condition of the two BBO crystals is imposed on the system [98]:

$$\theta_c \frac{L}{D} \ll 1, \quad (10.4)$$

where θ_c is the opening angle of the cone, D is the pump beam diameter, and L is the

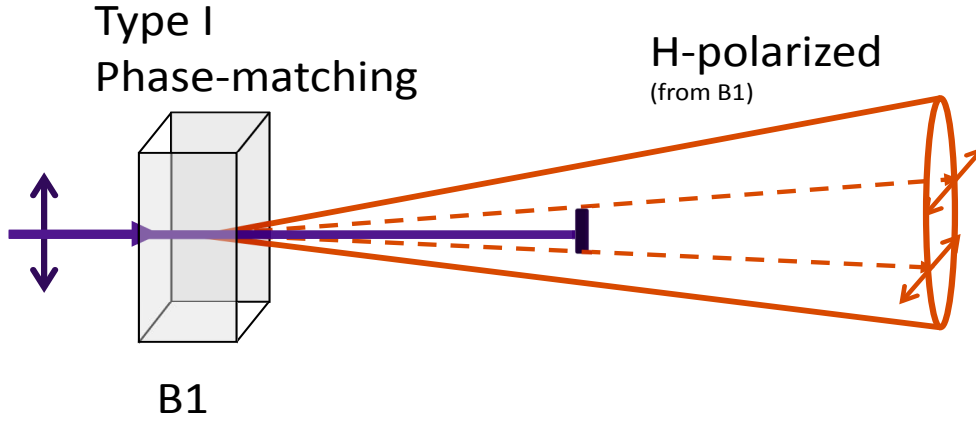


Figure 10.2: Polarization photons emitted from the first BBO crystal

crystal thickness, the high spatial overlap of the cones of down conversion produced by a 45° pump beam will induce a coherent two-down-conversion process. This implies that the emitted pair of photons with the spatial modes that are indistinguishable for the two crystals is in the state

$$|\Phi(\phi)\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 |H\rangle_2 + e^{i\phi} |V\rangle_1 |V\rangle_2), \quad (10.5)$$

where H and V denote horizontal and vertical polarization, respectively, and the subscripts 1 and 2 denote two distinct spatial modes. The relative phase between horizontal and vertical components of the state vector can be adjusted by (a) tilting the BBO crystals, by (b) using birefringent crystal on one of the output beams for phase shift, or by (c) changing the relative phase between the vertical and horizontal components of the pump beam.

10.3 Experimental generation of two-photon four-qubit hyperentangled states

To experimentally realize the single-element quantum search on a one-way quantum computer, we use the technique developed in previous experiments [102] with a type-I SPDC

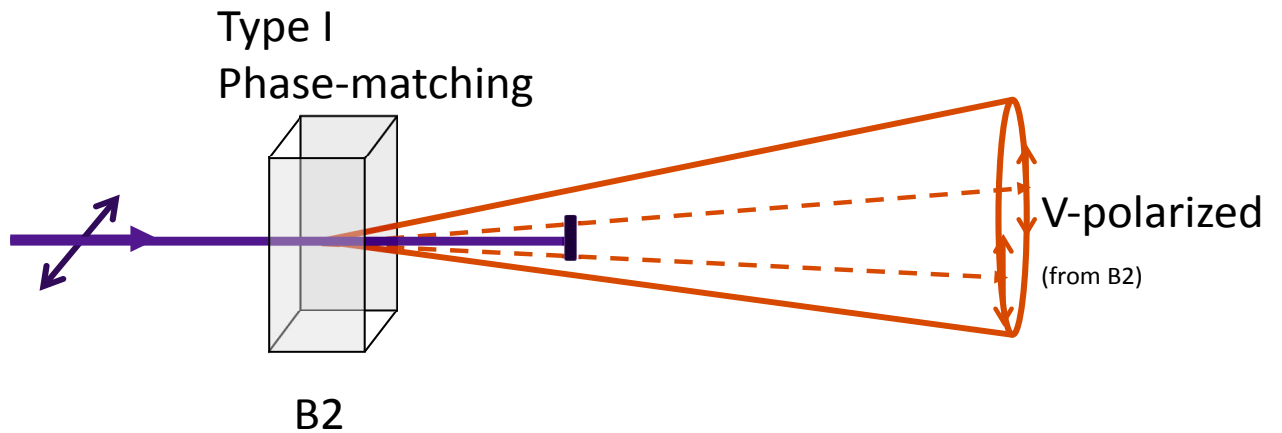


Figure 10.3: Polarization photons emitted from the second BBO crystal

source [98] to generate a two-photon four-qubit cluster state that is equivalent to the four-qubit box cluster state up to a local transformation, that is depicted in Fig. 10.4.

By pumping a two-crystal structured BBO by a ultraviolet (UV) pulse in a double pass configuration, one polarization entangled photon pair is generated by a type-I SPDC source with two possibilities in the forward direction and in the backward direction, respectively, to perform the preparation of 2-photon 4-qubit cluster state. The UV pulsed laser with a central wavelength of 355 nm has pulse duration of 5 ps, a repetition rate of 80 MHz, and an average pumping power of 200mW. Two quarter-wave plates (QWPs) are tilted along their optic axis to vary relative phases between polarization components to attain two desired possibilities for entangle pair creation. Concave mirror and prism are mounted on translation stages to optimize interference and overlapping on two beam splitters ($BS_{1,2}$) or two polarizing beam splitters ($PBS_{1,2}$) for achieving the target cluster state. Half-wave plates (HWPs) together with polarizing beam splitters (PBS) and 8 single-photon detectors (D1-D8) are used for polarization analysis of the output state. Finally, we observe a cluster state generation rate of about 1.2×10^4 per second behind 3 nm filters (IF) of central wavelength 710 nm.

A pulse of UV light passes twice through two contiguous BBO with optic axes aligned in perpendicular planes to produce one polarization entangled photon pair, with one

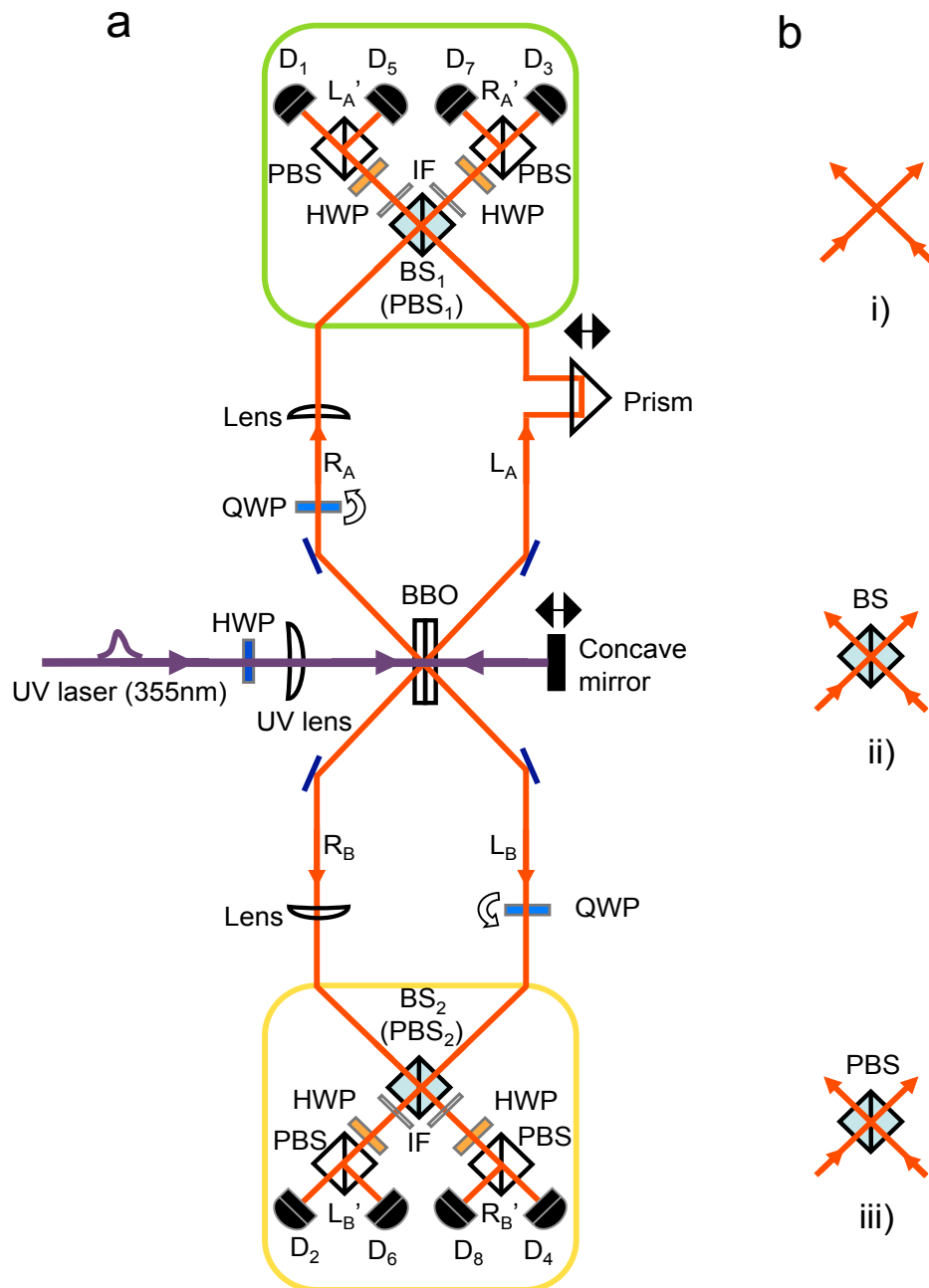


Figure 10.4: Schematic of experimental setup.

possibility in the forward direction of generating a state

$$|F\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B) |L\rangle_A |L\rangle_B, \quad (10.6)$$

on spacial (path) modes $L_{A,B}$, and another possibility in the backward direction of producing a state

$$|B\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |H\rangle_B - |V\rangle_A |V\rangle_B) |R\rangle_A |R\rangle_B, \quad (10.7)$$

on spacial modes $R_{A,B}$, where $|H\rangle$ ($|V\rangle$) stands for photons with horizontal (vertical) polarization. The states $|F\rangle$ and $|B\rangle$ can be a coherent superposition $|F\rangle + e^{i\theta} |B\rangle$ through perfect temporal overlaps of modes R_A and L_A and of modes R_B and L_B . By properly adjusting the distance between the concave mirror and the crystal, so that $\theta = 0$, the generated state is exactly the desired 2-photon 4-qubit cluster state

$$|C_4\rangle = \frac{1}{2}(|0000\rangle_{1234} + |0011\rangle_{1234} + |1100\rangle_{1234} - |1111\rangle_{1234}), \quad (10.8)$$

if we identify photon A to be qubits 2,3 and photon B to be qubits 1,4 and encode logical qubits as $|H(V)\rangle_B \leftrightarrow |0(1)\rangle_1$, $|H(V)\rangle_A \leftrightarrow |0(1)\rangle_2$, $|L(R)\rangle_A \leftrightarrow |0(1)\rangle_3$, $|L(R)\rangle_B \leftrightarrow |0(1)\rangle_4$. We observe a cluster state generation rate about 1.2×10^4 per second for 200mw UV pump, which is 4 order of magnitude more than the usual 4-photon cluster state production [52, 53, 190], and the lower bound for fidelity of experimental generations of $|C_4\rangle$ is $F \geq 0.883 \pm 0.002$ [54], that is better than the ones in [52, 53, 190] where fidelities are about 0.63 [52, 53] and 0.74 [190], respectively. The lower bound for fidelity is determined through an optimal entanglement witness with the following form:

$$\mathcal{W} = 2I - \frac{1}{2}(X_1 X_2 Z_4 + X_1 X_2 Z_3 + Z_2 X_3 X_4 + Z_1 X_3 X_4 + Z_1 Z_2 + Z_3 Z_4), \quad (10.9)$$

and by $F \geq \frac{1}{2}(1 - \langle \mathcal{W} \rangle_{\text{exp}})$ [72]. The experimental values of the observables of the witness

| Observable | Value | Observable | Value |
|-------------|---------------------|-------------|---------------------|
| $X_1X_2Z_4$ | 0.9070 ± 0.0036 | $Z_2X_3X_4$ | 0.9071 ± 0.0037 |
| $X_1X_2Z_3$ | 0.9076 ± 0.0035 | $Z_1X_3X_4$ | 0.8911 ± 0.0040 |
| Z_3Z_4 | 0.9812 ± 0.0016 | Z_1Z_2 | 0.9372 ± 0.0030 |

Table 10.1: Experimental values of all the observable on the cluster state $|C_4\rangle$ for the entanglement witness \mathcal{W} measurement. Each experimental value corresponds to measure in an average time of 1 sec and considers the Poissonian counting statistics of the raw detection events for the experimental errors.

is shown in Table 10.1. It is worth noting that \mathcal{W} is equivalent to the witness \mathcal{W}_{R_4} under a swap between operators 2 and 3 and a exchange of X and Z . See (3.18).

10.4 Experimental demonstration of quantum search algorithm with an one-way quantum computer

10.4.1 One-way quantum computation

If we have a four-element database, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and in which only one item satisfying $I_{jk}|jk\rangle = -|jk\rangle$, $j, k \in \{0, 1\}$ and otherwise $I_{jk}|j'k'\rangle = |j'k'\rangle$, $j' \neq j, k' \neq k$ where I_{jk} is the oracle operator corresponding to the database, one can utilize the quantum logic circuit depicted in Fig. 10.5 to search $|jk\rangle$ with certainty and then identify I_{jk} by just querying *one* oracle. The oracle operator can be designed by four settings: $(\alpha, \beta) = (\pi, \pi), (\pi, 0), (0, \pi), (0, 0)$, that correspond to I_{00}, I_{01}, I_{10} , and I_{11} respectively. For instance, if $(\alpha, \beta) = (\pi, \pi)$ is set in the quantum logic circuit and the superposition state of the four elements $|s\rangle = |+\rangle|+\rangle$, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, is prepared as the input of the circuit, the output state will be $|00\rangle$.

One-way quantum computer can simulate the quantum logic circuit for sigle-element quantum search. To simulate a computation task on a one-way quantum computer, one has to prepare a cluster state with a specific type of entangled feature associated with the computation. A cluster state can be schematically described by an array of nodes (vertexes) connected with lines. Each node is initially in the state of $|+\rangle$. Every

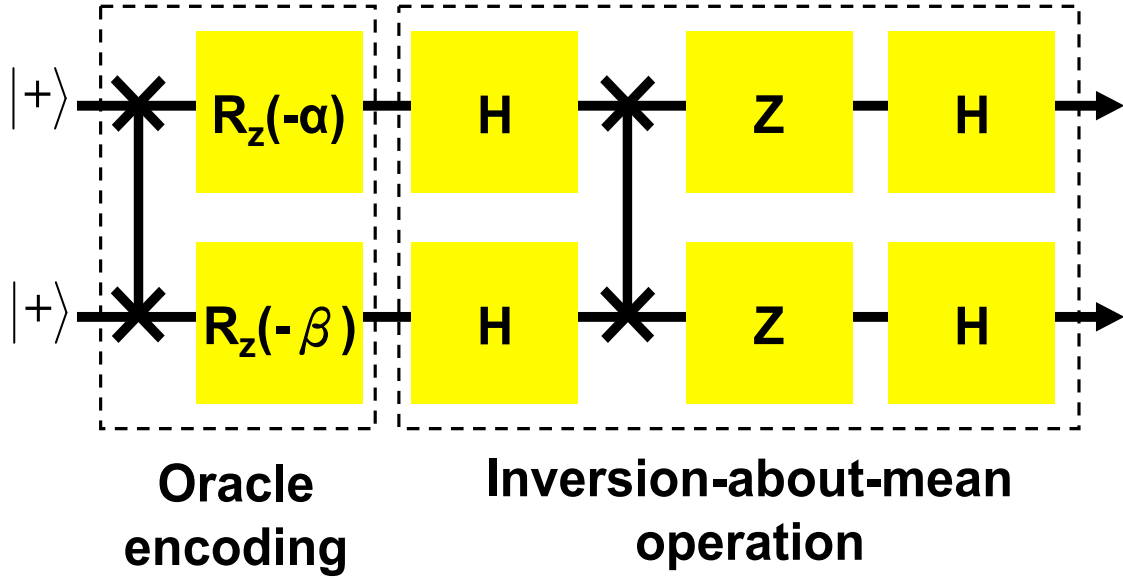


Figure 10.5: Quantum circuit for realization of quantum search algorithm.

connected line between nodes experiences a controlled-phase (CPhase) gates acting as $|j\rangle |k\rangle \rightarrow (-1)^{jk} |j\rangle |k\rangle$. The scenario of one-way implementation consists four steps as follows:

1. Prepare a 4-qubit box cluster state:

$$\begin{aligned}
 |R_4\rangle = & \frac{1}{2}(|0\rangle_1 |0\rangle_2 |+\rangle_3 |+\rangle_4 + |0\rangle_1 |1\rangle_2 |-\rangle_3 |-\rangle_4 \\
 & + |1\rangle_1 |0\rangle_2 |-\rangle_3 |-\rangle_4 + |1\rangle_1 |1\rangle_2 |+\rangle_3 |+\rangle_4),
 \end{aligned} \tag{10.10}$$

where $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ and the subindex denotes the number of particle. It is schematically represented in Fig. 10.6.

2. Take local measurements on the second and the third qubits in the bases $B_2(\alpha) = \{|\alpha_+\rangle, |\alpha_-\rangle\}$ and $B_3(\beta) = \{|\beta_+\rangle, |\beta_-\rangle\}$ respectively, where $|\alpha(\beta)_\pm\rangle = (|0\rangle \pm e^{i\alpha(\beta)} |1\rangle)/\sqrt{2}$. The outcome of measurement $|\alpha(\beta)_+\rangle$ is denoted by $s_{2(3)} = 0$ and $|\alpha(\beta)_-\rangle$ is denoted by $s_{2(3)} = 1$. The state of the remaining subsystem composed of the first and the third qubits is then equivalent to the output state of the quantum circuit shown in Fig. 10.7 when $|+\rangle |+\rangle$ is fed as an input.

3. Take local measurements on the first and the fourth qubits in the bases $\{|\pi_+\rangle, |\pi_-\rangle\}$,

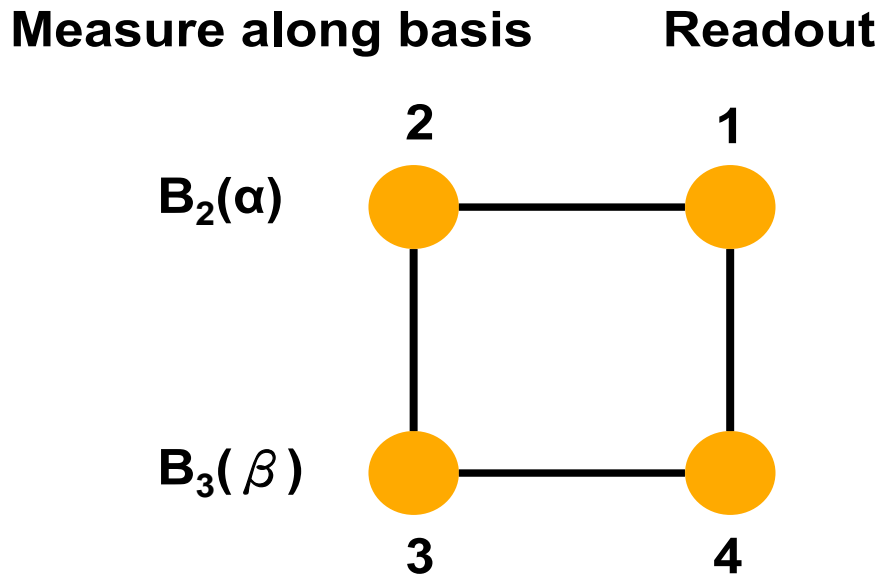


Figure 10.6: Box cluster state.

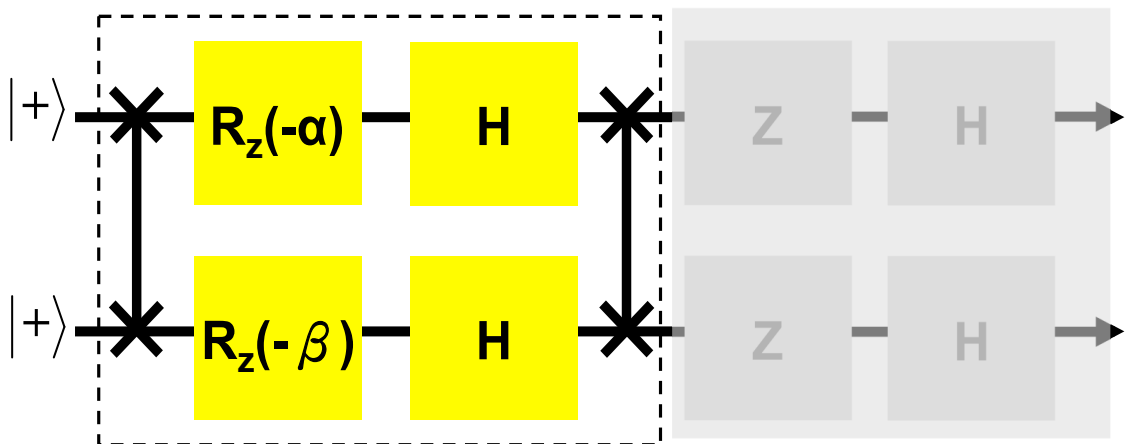


Figure 10.7: Quantum circuit involved an action of oracle for quantum search.

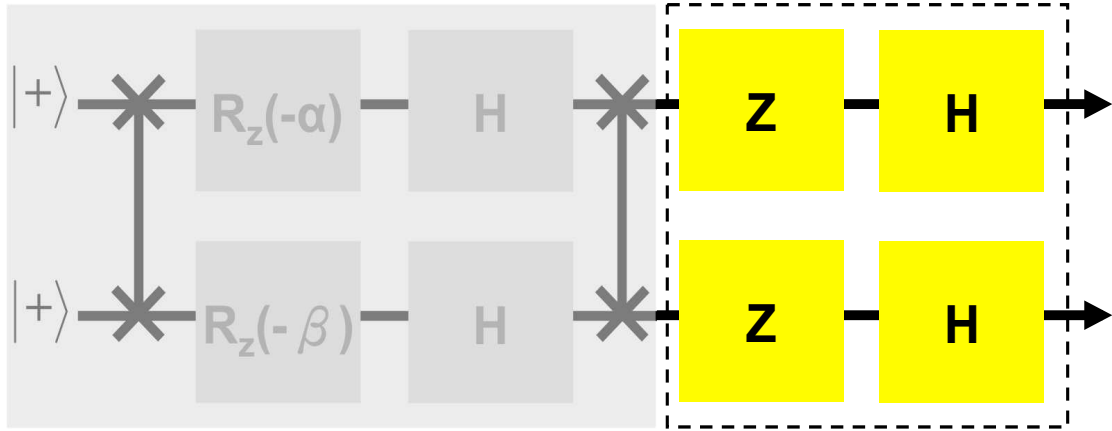


Figure 10.8: Quantum circuit composed of four local operations for the step 3 in one way realization.

which is equivalent to apply local operations depicted in Fig. 10.8 below to the output state of the circuit in the step 2. Similarly, the outcome of measurement corresponding to the state $|\alpha_+\rangle_{1(4)}$ is denoted by $s_{1(4)} = 0$ and $|\alpha_-\rangle_{1(4)}$ is denoted by $s_{1(4)} = 1$.

4. Refer to $(s_3 + s_4 = s_{34}, s_1 + s_2 = s_{12})$, one then can identify the oracle, I_{jk} , where $j = s_{34}$ and $k = s_{12}$.

10.4.2 Experimental realization of one-way quantum search

The state $|C_4\rangle$ is very useful for our experimental demonstration because $|C_4\rangle$ is equivalent to the four-qubit box cluster state up to four-qubit local unitary operations. To give a concrete demonstration, we experimentally mark the element $|00\rangle$ in qubits 2, 3 and make the final readout measurements on qubits 1, 4 all along basis $B(\pi)$. By noting the fact that the state Eq. (10.8) differs from the box cluster state up to a H transformation on every qubit and a swap between qubits 2 and 3, this amounts to measure along the $\{|V\rangle, |H\rangle\}$ basis for the polarization in each output arm after PBS_1 and PBS_2 . The output of the algorithm is two bits $(s_3 \oplus s_4, s_1 \oplus s_2)$ in lab basis by feed-forwarding outcomes of qubits 2,3. The experimental result of this example is shown in Fig. 10.9.

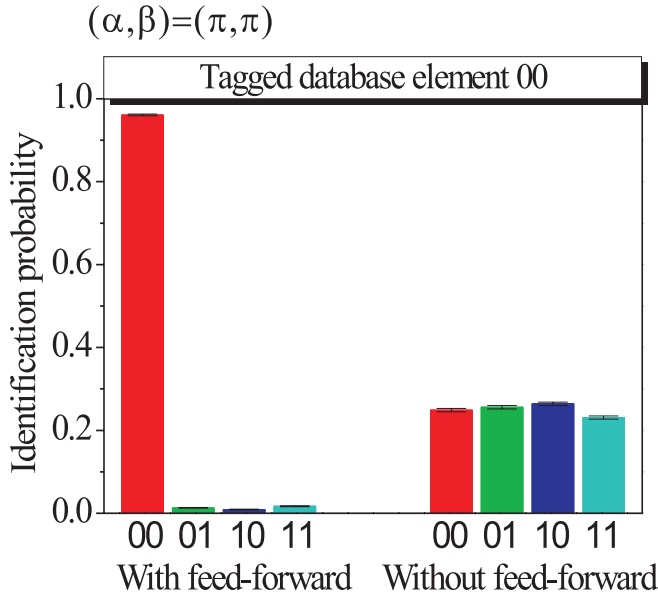


Figure 10.9: A successful identification probability of $(96.1 \pm 0.2)\%$ is achieved deterministically with feed-forward, while it is $(24.9 \pm 0.4)\%$ without feed-forward. This depicts that our source of cluster state is ideally suited for such a sort of algorithm's implementation.

10.5 Conclusion

We have developed a scheme for preparation of a two-photon four-qubit cluster state. With such a source, we have designed and demonstrated the first proof-of-principle experimental realization of one-way quantum computing. The excellent quality of the state with fidelity better than 88% is characterized by an optimal witness without using of a full state tomography. Moreover, high count rates of the state creation enable more efficient quantum computing by 4 orders of magnitude than previous methods. We have thus achieved implementation of Grover's algorithm with a successful probability of about 96%. In addition, non-trivial two-qubit quantum gates such as the CPhase gate are implemented with high fidelities through the approach developed. Refer to [54] for detailed discussions.

Chapter 11

Summary and Outlook

11.1 Summary

In this thesis we have presented novel approaches to correlation structure of multipartite entanglement, entanglement detection, entanglement generation, entanglement purification, quantum error corrections, quantum search algorithm, and, furthermore, experimental advance towards one-way quantum computation. Our research has covered several important subjects involved in the field of quantum information and quantum computation and mainly associates with the key processes of quantum information processing.

Through the correlation criteria of multipartite entanglement, one can construct robust entanglement witness operators to detect many-qubit stabilizer, four-qubit singlet, three-qubit W, generalized many-qubit GHZ, two-qudit Bell, two-qudit singlet, four-ququat supersinglet, many-qudit GHZ states with fewer local measurement settings. The entangled states under study are all important for entanglement-based quantum information processing. In addition to detections of entanglement, the criteria proposed help to analyze the correlation structures of Bell inequalities and to find their connections with entanglement witness operators.

An idea of hybrid maps is proposed to establish standard entanglement purification protocols which guarantee to purify any distillable state to a desired maximally entangled

pure state all by the standard purification local operations and classical communications. The protocols proposed in this work, in which two state transformations are used, perform better than the IBM and Oxford protocols in the sense that they require fewer operation times in yielding a same amount of the desired pure state. One of the proposed protocols in this work can even lead to a higher improved output yield when it is combined with the hashing protocol, as compared with the combined algorithm consisting of the Oxford and the hashing protocol.

Simpler encoding and decoding networks are necessary for more reliable quantum error-correcting codes. The simplification of the encoder-decoder circuit for a perfect five-qubit quantum error-correcting code can be derived analytically if the quantum error-correcting code is converted from its equivalent one-way entanglement purification protocol. In our study, the analytical method to simplify the encoder-decoder circuit is introduced and a circuit that is as simple as the existent simplest circuits is presented as an example. The encoder-decoder circuit presented here involves nine single- and two-qubit unitary operations, only six of which are controlled-NOT gates.

A study on the cause of multi-particle entanglement is also presented in this thesis. We show how dot-like single quantum well excitons, which are coupled to single-mode cavity photon, evolve into maximally entangled state as a series of conditional measurements are taken on the cavity field state. Generation of multi-particle entangled states is derived analytically. Application to quantum teleportation is also pointed out, and may be achieved with current technologies.

We have analyzed the quantum search algorithm in detail. First, a general quantum search algorithm with arbitrary unitary transformations and an arbitrary initial state is considered in this work. To search a marked state with certainty, we have derived, using an $SU(2)$ representation: (1) the matching condition relating the phase rotations in the algorithm, (2) a concise formula for evaluating the required number of iterations for the search, and (3) the final state after the search, with a complex phase in its amplitude. Moreover, the optimal choices and modifications of the phase angles in the Grover kernel

are also studied. As the matching condition in Grover search algorithm is transgressed due to inevitable errors in phase inversions, it gives a reduction in maximum probability of success. With a given degree of maximum success, we have derived the generalized and improved criterion for tolerated error and corresponding size of quantum database under the inevitable gate imperfections. The vanished inaccuracy to this condition has also been shown. A concise formula for evaluating minimum number of iterations is also presented. Furthermore, a family of algorithms is recently addressed for sure-success quantum search problems. When the phase inversion operations of these algorithms are identical to those of the standard Grover algorithm, we found that this family of algorithms is of robustness against inevitable phase imperfections. Finally, an analog analogue of Grover's quantum search algorithm was studied. A generalized Hamiltonian driving the evolution of quantum state in the analog search system was derived. Equations relating all parameters considered in the present problem were given according to the required maximal probability for finding the marked state. By these equations, both the measuring time and the system energy gap suitable for a quantum search with or without certainty can thus be evaluated. It was shown that in an efficient quantum search computation, the measuring time should be proportional to the square root of the size of database.

We perform the first experimental realization of one-way quantum computation on a 2-photon four-qubit cluster state that is entangled both in polarization and spatial modes. Through solving a quantum search problem, the experiment illustrates a high-speed quantum computation in one-way realization. The experimental demonstration shows the hyper-entangled cluster states can provide an ideal source for rapidly and precisely optical quantum information processing.

11.2 Outlook

Distinct correlation properties of entanglement pay the way for novel models of information and computation and reveal the fundamental features of quantum phenomenon. We

have seen in the thesis that the correlation criteria proposed provide a way to analyze the correlation structure of multipartite entanglement. In our preliminary result, the criteria can be used to construct Bell inequalities for three four-level systems, which shows that there may exist a family of Bell inequalities for many qudits where each member is comprised of correlators. Furthermore, how to detect genuine multipartite entanglement that are inherent in many-qudit singlet and valence-bound solid states is still open. These entangled states are crucial for quantum information and computation. Then one of our future works is to design a method based on correlators to investigate on the structures of these states. As for entanglement purification, improvement of purification yield will be the next topic. Since the standard protocol for purifying entangled qubit pairs relies on successful controlled-NOT operations and on certain results of measurements, designations of new models that can be achieved deterministically or in a more deterministic way will be helpful for raising the yield of purification. The number of controlled-NOT gates also affects the complexity of an encoder-decoder circuit to perform the five-qubit, single-error correction protocol. The simplest circuit consists of six controlled-NOT gates and three single-qubit operations presented in this thesis and proposed by Braunstein and Smolin might not be improved further. A more convincing proof will be given in the future work. As for generation of entangled pairs or multipartite entangled qubits, preparation of remote entangled states by controlling a media system with a high generation of yield is crucial. How to control the third quantum system in an experiment reliably as the case discussed in the thesis will be investigated elsewhere. For generating entangled photons with SPDC sources, investigations on the quality of entangled photons and coincidence detections are also the future topics for entanglement generations.

Quantum correlations provide novel ways of communications with high security, e.g., the Ekert protocol for key distribution. However, it is worth discussing whether entanglement is necessary for quantum communication. In Ref. [193], it has shown that the Ekert protocol [29] based on maximally entangled qubits is equivalent to the scheme of Bennett and Brassard [34] using on nonorthogonal states. It implies that in some quantum commu-

nication tasks utilization of entanglement is not the only method for reliable achievement [194]. Since entanglement can be replaced by separable quantum systems, the processes required for entangled states, e.g., entanglement purification, can be replaced by simple single-qubit operations. We propose an example for quantum secret sharing to discuss it further. With a simple protocol proposed, we show that secret sharing tasks can be performed without assistance of entanglement.

A sender, called Sophie, wants to share a confidential message with her friends Alice and Bob. Instead of giving the whole message to Alice and Bob, Sophie splits the message into two pieces and prepares to send each individual one to Alice and Bob respectively. The hope of Sophie is that her confidential message can be determined faithfully only when Alice and Bob combine their individual pieces. For protecting the security of the message from selfish actions of any eavesdroppers or dishonest party, Sophie realizes that she cannot send the individual messages to Alice and Bob directly without invoking any secret-sharing protocols.

Quantum mechanics specifies that quantum states can exist in multiple eigenstates simultaneously, i.e., superposition, and measurement of a variable will yield one of the eigenvalues corresponding to the observable with a specific probability and makes a collapse of the state vector. Furthermore, quantum states can not be cloned perfectly, and through unitary operations, they can be transformed coherently. An utilization of these quantum mechanical features of physical states and associated operations is sufficient to realize our protocol. In the scenario of quantum secret sharing, Sophie wants Alice to possess a state $|s_a\rangle$ and Bob to possess another one $|s_b\rangle$. Each party has no information about the state of the other party, and Alice and Bob can share the state $|s_a\rangle \otimes |s_b\rangle$ only when they combine their own states $|s_a\rangle$ and $|s_b\rangle$. Let us assume that $s_{a(b)} \in \{0, 1\}$ and $\{|0\rangle, |1\rangle\}$ are eigenstates of Pauli matrix σ_z . A quantum state can be changed from $|0\rangle_a \otimes |0\rangle_b$ to $|s_a\rangle \otimes |s_b\rangle$ by applying unitary transformations to $|0\rangle_a \otimes |0\rangle_b$:

$$|s_a\rangle \otimes |s_b\rangle = U_D U_C |0\rangle_a \otimes |0\rangle_b, \quad (11.1)$$

where U_C and U_D are unitary operators. It is worth noting two points involved in the state evolution:

(1) If a specific U_C is chosen by Sophie for the state transformation, the operator U_D should be consequently fixed for $|s_a\rangle \otimes |s_b\rangle$.

(2) We assume that Alice and Bob know that $|s_a\rangle \otimes |s_b\rangle$ evolves from $|0\rangle_a \otimes |0\rangle_b$. However, since they have no information about both $|s_a\rangle$ and $|s_b\rangle$ before secret sharing, giving them only the operator U_C or U_D cannot help them to figure $|s_a\rangle \otimes |s_b\rangle$ out with certainty unless one provides them both U_C and U_D .

With these two facts, a simple protocol is designed to satisfy the needs of Sophie. Firstly, Sophie can randomly choose a U_C from a set of operators and apply it to $|0\rangle_a \otimes |0\rangle_b$, and then she send each individual qubit to Alice and Bob. It is clear that U_C is unknown to both Alice and Bob. When both of Alice and Bob have received the qubits, according the operator U_C chosen, Sophie announce which U_D should be used by Alice and Bob. In an ideal situation where any eavesdropper and cheat are excluded from considerations, Alice and Bob can reconstruct the state $|s_a\rangle$ and $|s_b\rangle$ with certainty if they follow Sophie's instruction for U_D . When considering eavesdropping, if any selfish actions of eavesdroppers or dishonest party change Sophie's preparation $U_C |0\rangle_a \otimes |0\rangle_b$ in transit, the subsequent operation U_D shall not transfer the qubits to $|s_a\rangle \otimes |s_b\rangle$ and then the message can not be reconstructed with certainty. This effect on the secret states can be utilized to expose eavesdroppers. For instance, in our protocol $|0\rangle_a \otimes |1\rangle_b$ and $|1\rangle_a \otimes |0\rangle_b$ represent the logical bits 0 and 1 respectively, whereas the states $|0\rangle_a \otimes |0\rangle_b$ and $|1\rangle_a \otimes |1\rangle_b$ are used to detect eavesdroppers, which means that Sophie shall be aware of eavesdroppers when she find that the result of combination of Alice and Bob is $|0\rangle_a \otimes |0\rangle_b$ or $|1\rangle_a \otimes |1\rangle_b$ and is not consistent with her designation of $|s_a\rangle \otimes |s_b\rangle$.

With the idea introduced above, the quantum secret-sharing protocol is specified by six steps:

S1. Sophie randomly choose two local unitary operators C_a and C_b , where $C_a, C_b \in$

$\{X_+, X_-, Y_+, Y_-\}$ and

$$\begin{aligned} X_+ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, & X_- &= \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \\ Y_+ &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, & Y_- &= \frac{1}{\sqrt{2}} \begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}, \end{aligned} \quad (11.2)$$

and applies C_a and C_b to the states $|0\rangle_a$ and $|0\rangle_b$ respectively, i.e., she prepares a product state $|\Psi\rangle = |\Psi_a\rangle \otimes |\Psi_b\rangle$, where $|\Psi_{a(b)}\rangle = C_{a(b)}|0\rangle_{a(b)}$.

S2. Sophie sends the qubits $|\Psi_a\rangle$ and $|\Psi_b\rangle$ to Alice and Bob respectively.

S3. Through classical communication, Sophie confirms that both parties have received the qubits.

S4. Sophie announce which kinds of operators, say D_a and D_b , should be used by Alice and Bob to reconstruct a secret state $|s\rangle = |s_a\rangle \otimes |s_b\rangle$. The set of operators (C_a, C_b) chosen in **S1** restricts the choices of local operators in this step. If $C_{a(b)} \in \{U_+, U_-\}$ where $U = X$ or Y , $D_{a(b)}$, the operator applied by Alice (Bob), should also be in the set of operator $\{U_+, U_-\}$. The type $+$ or $-$ for U_+ and U_- depends on the choice of Sophie. When Sophie has made her decision, she broadcast the choices of D_a and D_b in public. The designation of (s_a, s_b) depends on Sophie's message for sharing. To share a logical bit 0 or 1 with Alice and Bob, her designation is $(s_a = 0, s_b = 1)$ or $(s_a = 1, s_b = 0)$ respectively. Furthermore, Sophie can design $(s_a = 0, s_b = 0)$ or $(s_a = 0, s_b = 1)$ to examine whether Alice and Bob inform her of their results faithfully (refer to **S6**).

S5. First, Alice and Bob have to transform their qubits by D_a and D_b respectively. When the transformations are performed, they measure their qubits in the respective orthonormal bases $\{|0\rangle_a, |1\rangle_a\}$ and $\{|0\rangle_b, |1\rangle_b\}$ and eventually get the output states $|s'_a\rangle$ and $|s'_b\rangle$. In an ideal situation without eavesdropping, they have $s'_a = s_a$ and $s'_b = s_b$ with certainty. Then, they combine their results of measurement and have $s'_a s'_b$.

S6. Alice and Bob identify whether their combined message is even: $s'_a s'_b \in \{00, 11\}$ or odd: $s'_a s'_b \in \{01, 10\}$. If the message is even, both of them should inform Sophie of this

result via classical communication. If $s'_a s'_b = 01(10)$, they share a bit 0 (1) with Sophie and keep a secret.

With the above protocol, quantum secret sharing can be achieved without entanglement. A detailed discussion of the security of the proposed protocol will be given elsewhere [195]. In addition to quantum communication, it has been shown that sophisticated quantum search can be performed without entanglement and the quantum interference alone suffices to reduce the complexity of query requirement [196]. The experimental demonstrations by optical implementation is reported in Ref. [197]. It would be interesting and important to find other quantum mechanical procedures that require no entanglement source or generate no multipartite correlations of quantum states at any time step.



Appendix A

Tightness of Bell inequalities

Every tight Bell inequality fulfills the following conditions [115]:

Condition 1. All the generators of the convex polytope must belong either to the half-space or to the hyperplane.

Condition 2. There must be $4d(d-1)$ linear independent generators among the ones that belong to the hyperplane.

On the other hand, non-tight Bell inequalities satisfy only the first condition. Then, we will examine the proposed Bell inequality by these conditions for tightness. Since we have proven that the proposed Bell inequality fulfills the first condition in the third section. Then we proceed to consider the second condition for the Bell inequality. All the generators of the convex polytope are written as

$$\mathbf{G} = \left| v_1^{(1)}, v_2^{(1)} \right\rangle \oplus \left| v_1^{(1)}, v_2^{(2)} \right\rangle \oplus \left| v_1^{(2)}, v_2^{(1)} \right\rangle \oplus \left| v_1^{(2)}, v_2^{(2)} \right\rangle, \quad (\text{A.1})$$

which can also be represented as the following form by the defined variables shown in Eq. (2.57):

$$\begin{aligned} & \left| v_1^{(1)}, \chi_{11} - v_1^{(1)} \right\rangle \oplus \left| v_1^{(1)}, -\chi_{12} - v_1^{(1)} \right\rangle \\ & \oplus \left| v_1^{(1)} - \chi_{11} - \chi_{21} - 1, \chi_{11} - v_1^{(1)} \right\rangle \\ & \oplus \left| v_1^{(1)} + \chi_{12} + \chi_{22}, -\chi_{12} - v_1^{(1)} \right\rangle, \end{aligned} \quad (\text{A.2})$$

APPENDIX A. TIGHTNESS OF BELL INEQUALITIES

where $|\tilde{v}_1^{(r)}, \tilde{v}_2^{(t)}\rangle = |\tilde{v}_1^{(r)} \bmod d\rangle \otimes |\tilde{v}_2^{(t)} \bmod d\rangle$. The generators which satisfy $C_{\Psi_{1,LR}}^{(d)} = 2$ are the ones with the variables belonging to the class (i) discussed after Eq. (2.59) in the third section. Thus, the generators contained in the hyperplane are shown as:

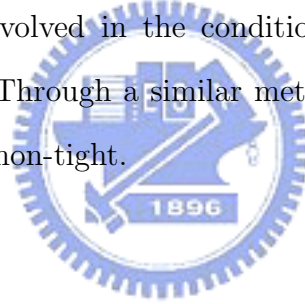
$$|v, -v\rangle \oplus |v, -v\rangle \oplus |v-1, -v\rangle \oplus |v-1, -v\rangle, \quad (\text{A.3})$$

$$|v, -v\rangle \oplus |v, -v\rangle \oplus |v, -v\rangle \oplus |v, -v\rangle, \quad (\text{A.4})$$

$$|v, -v\rangle \oplus |v, 1-v\rangle \oplus |v-1, -v\rangle \oplus |v-1, -v\rangle, \quad (\text{A.5})$$

$$|v, -1-v\rangle \oplus |v, -v\rangle \oplus |v, -1-v\rangle \oplus |v, -v\rangle, \quad (\text{A.6})$$

for $v \in \{0, 1, \dots, d-1\}$. The total number of linear independent generators is $4d$ which is smaller than $4d(d-1)$ involved in the condition of tightness. Then the proposed Bell inequality is non-tight. Through a similar method shown above, one can prove the inequality: $C_{\Psi_{2,LR}}^{(d)} \leq 2$, is non-tight.



Appendix B

Entanglement witnesses of stabilizer states

In order to prove that \mathcal{W}_ϕ is a witness for detecting truly multipartite entanglement, we show a comparison between \mathcal{W}_ϕ and \mathcal{W}_ϕ^p : if a state ρ satisfies $\text{Tr}(\mathcal{W}_\phi\rho) < 0$, it also satisfies $\text{Tr}(\mathcal{W}_\phi^p\rho) < 0$, i.e., $\mathcal{W}_\phi - \gamma_\phi\mathcal{W}_\phi^p \geq 0$ where γ_ϕ is some positive constant [72]. The related parameters utilized to prove the witness operators have been summarized in the following table.

Table B.1: The parameters involved in the proofs of entanglement witnesses and their robustness to noise. Robustness of entanglement witnesses. The robustness to noise can be determined by the noise tolerance: $p_{\text{noise}} < \delta_{\text{noise}}$, is such that $\rho = p_{\text{noise}}/2^N\mathbf{1} + (1 - p_{\text{noise}})|\phi\rangle\langle\phi|$, where p_{noise} describes the noise fraction, is identified as a truly multipartite entanglement.

| W_ϕ | δ_{noise} | γ_ϕ | α_ϕ^p |
|--------------------|--|--------------------|-----------------|
| W_{L_N} | $(4 - (\frac{3}{2\sqrt{2}})^{\delta[\lceil\frac{N}{2}\rceil-1, \lfloor\frac{N}{2}\rfloor]}(\frac{4}{2^{N/2}}))^{-1}$ | $\gamma_1\gamma_2$ | 1/2 |
| W_{GHZ_N} | $(3 - \frac{4}{2^n})^{-1}$ | $\gamma_1\gamma_2$ | 1/2 |
| W_{R_4} | 1/3 | $\gamma_1\gamma_2$ | 1/2 |

Appendix C

Entanglement witnesses of entangled qudits

To prove that \mathcal{W}_ϕ is a witness, we have to show the following comparison between \mathcal{W}_ϕ and \mathcal{W}_ϕ^p : if a state ρ satisfies $\text{Tr}(\mathcal{W}_\phi\rho) < 0$, it also satisfies $\text{Tr}(\mathcal{W}_\phi^p\rho) < 0$, i.e., $\mathcal{W}_\phi - \gamma_\phi\mathcal{W}_\phi^p \geq 0$ where γ_ϕ is some positive constant [72]. The table shown below summarizes the related parameters utilized to prove that the proposed operators are indeed entanglement witnesses for detecting many-qudit entanglement

Table C.1: Summaries of α_ϕ for \mathcal{W}_ϕ , the parameters α_ϕ^p and γ_ϕ , which are utilized to prove \mathcal{W}_ϕ , and δ_{noise} involved in robustness of the entanglement witness operator proposed.

| $ \phi\rangle$ | $ s\rangle$ | $ S\rangle$ | $ \Psi_{4\times 4}\rangle$ | $ \Psi_{N\times 3}\rangle$ |
|-------------------------|-------------------------------------|---------------------------------------|--|--|
| α_ϕ | $0.5 \langle \widehat{C}_s \rangle$ | $0.806 \langle \widehat{C}_S \rangle$ | $0.6 \langle \widehat{C}_\Psi \rangle$ | $0.6 \langle \widehat{C}_{\Phi_N} \rangle$ |
| α_ϕ^p | $1/d$ | $1/4$ | $1/4$ | $1/3$ |
| γ_ϕ | -1.55 | -1.92 | -1.81 | $\sum_{k=0}^{N-2} 2^k$ |
| δ_{noise} | 0.5 | 0.194 | 0.4 | 0.4 |

Bibliography

- [1] Charles H. Bennett and David P. DiVincenzo, *Nature* **404**, 247 (2000).
- [2] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information* (Springer, Berlin, 2000).
- [3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, September 2000).
- [4] N. D. Mermin, *Quantum Computer Science: An Introduction* (Cambridge University Press, September, 2007).
- [5] J. S. Bell, *Physics* (Long Island City, N.Y.) **1**, 195 (1964).
- [6] J. S. Bell, *Speakable and unspeakable in quantum mechanics* (Cambridge University Press, July 29, 1988).
- [7] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47** , 777 (1935).
- [8] A. Peres, *Quantum Theory: Concepts and Methods* , (Springer, September 1995).
- [9] N. Bohr, *Phys. Rev.* **48**, 696 (1935).
- [10] E. Schrödinger, *Die Naturwissenschaften* **23** , 807 (1935).
- [11] D. Bohm, *Quantum theory* (Prentice-Hall, New-York, 1951).

BIBLIOGRAPHY

- [12] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981); A. Aspect, P. Grangier, and G. Roger, *ibid* **49**, 91 (1982); A. Aspect, P. Grangier, and G. Roger, *ibid* **49**, 1804 (1982).
- [13] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
- [14] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [15] M. Seevinck and G. Svetlichny, Phys. Rev. Lett. **89**, 060401 (2002).
- [16] S. M. Roy and V. Singh, Phys. Rev. Lett. **67**, 2761 (1991); M. Ardehali, Phys. Rev. A **46**, 5375 (1992); S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992); A. V. Belinskii and D. N. Klyshko, Phys. Usp. **36**, 653 (1993); N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998); R. F. Werner and M. M. Wolf, Phys. Rev. A **64**, 032112 (2001); M. Żukowski and Č. Brukner, Phys. Rev. Lett. **88**, 210401 (2002); Kai Chen, Sergio Alberverio, and Shao-Ming Fei, Phys. Rev. A **74**, 050101 (2006).
- [17] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
- [18] W. Son, J. Lee, and M. S. Kim, Phys. Rev. Lett. **96**, 060406 (2006).
- [19] N. J. Cerf, S. Massar, and S. Pironio, Phys. Rev. Lett. **89**, 080402 (2002).
- [20] A. Mair *et al.*, Nature **412**, 313 (2001).
- [21] L. Neves *et al.*, Phys. Rev. Lett. **94**, 100501 (2005); M. N. O’Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, *ibid* **94**, 220501 (2005); G. Lima *et al.*, Phys. Rev. A **73**, 032340 (2006).
- [22] R.T. Thew *et al.*, Quant. Inf. Comput. **4**, 093 (2004); N. K. Langford *et al.*, Phys. Rev. Lett. **93**, 053601 (2004).

BIBLIOGRAPHY

- [23] S. Grblacher *et al.*, *New J. Phys.* **8**, 75 (2006).
- [24] T. Durt, Nicolas J. Cerf, N. Gisin, and Marek Żukowski, *Phys. Rev. A* **67**, 012311 (2003); T. Durt, D. Kaszlikowski, J. L. Chen, and L. C. Kwek, *ibid* **69**, 032313 (2004).
- [25] N. Gisin and A. Peres, *Phys. Lett. A* **162**, 15 (1992).
- [26] D. Kaszlikowski *et al.*, *Phys. Rev. Lett.* **85**, 4418 (2000).
- [27] D. Kaszlikowski *et al.*, *Phys. Rev. A* **65**, 032118 (2002).
- [28] J. Lee, S. W. Lee, and M. S. Kim, *Phys. Rev. A* **73**, 032316 (2006).
- [29] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [30] C. H. Bennett *et al.*, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [31] H.J. Briegel and R. Raussendorf, *Phys. Rev. Lett.* **86**, 910 (2001).
- [32] R. Raussendorf and H.J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [33] R. Raussendorf, D.E. Browne, and H.J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [34] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
- [35] D. Gottesman and I. Chuang, *Nature* **402**, 390 (1999).
- [36] E. Knill, R. Laflamme, and G. J. Milburn, *Nature* **409**, 46 (2001).
- [37] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [38] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
- [39] D. Boschi *et al.*, *Phys. Rev. Lett.* **80**, 1121 (1998).
- [40] D. Bouwmeester *et al.*, *Nature* **390**, 575 (1997).

BIBLIOGRAPHY

- [41] A. Furusawa *et al.*, Science **282**, 706 (1998).
- [42] M. A. Nielsen *et al.*, Nature **396**, 52 (1998).
- [43] Z. Zhao *et al.*, Nature **430**, 54 (2004).
- [44] Q. Zhang *et al.*, Nat. Phys. **2**, 678 (2006).
- [45] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
- [46] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).
- [47] B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **66**, 052307 (2002).
- [48] H.J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5392 (1998).
- [49] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).
- [50] D. Deutsch, Proc. R. Soc. London Ser. A **425**, 73 (1989).
- [51] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).
- [52] P. Walther *et al.*, Nature **434**, 169 (2005).
- [53] R. Prevedel *et al.*, Nature **445**, 65 (2007).
- [54] K. Chen *et al.*, Phys. Rev. Lett. **99**, 120503 (2007).
- [55] D. Deutsch and R. Jozsa, Proc. R. Soc. London Ser. A **439**, 553 (1992).
- [56] P. W. Shor, in Proceedings of 35th Annual Symposium on Foundation of Computer Science, (IEEE, Los Alamitos, CA, 1994).
- [57] L. K. Grover, in Proceedings of 28th Annual ACM Symposium on the Theory of Computation, (ACM Press, New York, 1996)
- [58] L. K. Grover, Phys. Rev. Lett. **79**, 325(1997).

BIBLIOGRAPHY

- [59] C.H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, *SIAM J. Comput.* **26**,1510 (1997).
- [60] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, *Fortsch. Phys.-Prog. Phys.*, **46**, 493 (1998).
- [61] C. Zalka, *Phys. Rev. A*, **60**, 2746 (1999).
- [62] M.S. Tame *et al.*, *Phys. Rev. Lett.* **98**, 140501 (2007).
- [63] C. Y. Lu *et al.*, *Phys. Rev. Lett.* **99**, 250504 (2007); B. P. Lanyon *et al.*, *ibid* **99**, 250505 (2007).
- [64] H. B.-Pasquinucci and A. Peres, *Phys. Rev. Lett.* **85**, 3313 (2000).
- [65] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [66] D. Bruß and C. Macchiavello, *Phys. Rev. Lett.* **88**, 127901 (2002).
- [67] M. Fitzi, N. Gisin, and U. Maurer, *Phys. Rev. Lett.* **87**, 217901 (2001).
- [68] Časlav Brukner, Marek Żukowski, and Anton Zeilinger, *Phys. Rev. Lett.* **89**, 197901 (2001).
- [69] A. Cabello, *Phys. Rev. Lett.* **89**, 100402 (2002).
- [70] M. Bourennane *et al.*, *Phys. Rev. Lett.* **92**, 087902 (2004).
- [71] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1996); B. M. Terhal, *ibid* **271**, 319 (2000); M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, *Phys. Rev. A* **62**, 052310 (2000).
- [72] G. Tóth and O. Gühne, *Phys. Rev. Lett.* **94**, 060501 (2005); G. Tóth and O. Gühne, *Phys. Rev. A* **72**, 022340 (2005).
- [73] C. M. Li *et al.*, *Phys. Rev. A* **76**, 032313 (2007).

BIBLIOGRAPHY

- [74] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [75] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).
- [76] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).
- [77] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, *Phys. Rev. Lett.* **77**, 198, (1996).
- [78] E. Knill and R. Laflamme, *Phys. Rev. A* **55**, 900 (1997).
- [79] P. Shor, *Phys. Rev. A* **52**, 2493 (1995).
- [80] A. M. Steane, *Phys. Rev. Lett.* **77**, 793 (1996).
- [81] J. W. Pan *et al.*, *Nature* **410**, 1067 (2001).
- [82] A. Miyake and H. J. Briegel, *Phys. Rev. Lett.* **95**, 220501 (2005).
- [83] C. Kruszynska *et al.*, *Phys. Rev. A* **74**, 052316 (2006).
- [84] Y. W. Cheong *et al.*, *Phys. Rev. A* **76**, 042314 (2007).
- [85] D. Leibfried *et al.*, *Nature* **438**, 639 (2005).
- [86] C. W. Chou *et al.*, *Nature* **438**, 828 (2005).
- [87] Y. A. Chen *et al.*, *Nat. Phys.* **4**, 103 (2008).
- [88] H. Haffner *et al.*, *Nature* **438**, 643 (2005).
- [89] Yu. A. Pashkin *et al.*, *Nature* **421**, 823 (2003).
- [90] T. Yamamoto *et al.*, *Nature* **425**, 941 (2003).

BIBLIOGRAPHY

- [91] I. Chiorescu *et al.*, Science **299**, 1869 (2003).
- [92] D. P. DiVincenzo and D. Loss, Superlatt. Micro. **23**, 419 (1998).
- [93] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
- [94] N. Gisin and R. Thew, Nat. Photonics **1**, 165 (2007).
- [95] P. Kok *et al.*, Rev. Mod. Phys. **79**, 135 (2007).
- [96] J. L. O'Brien, Science **318**, 156 (2007).
- [97] P. G. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995).
- [98] P. G. Kwiat *et al.*, Phys. Rev. A **60**, 773 (1999).
- [99] C. Y. Lu *et al.*, Nat. Phys. **3**, 91 (2007).
- [100] S. Groblacher *et al.*, Nature **446**, 871 (2007).
- [101] C. Simon and J. W. Pan, Phys. Rev. Lett. **89**, 257901 (2002).
- [102] T. Yang *et al.*, Phys. Rev. Lett. **95**, 240406 (2005).
- [103] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989); W. Tittel *et al.*, Phys. Rev. A **59**, 4150 (1999).
- [104] R. T. Thew *et al.*, Phys. Rev. A **66**, 062304 (2002); I. Marcikic *et al.*, Nature **421**, 509 (2003).
- [105] R. T. Thew *et al.*, Phys. Rev. Lett. **93**, 010503 (2004).
- [106] J. T. Barreiro *et al.*, Phys. Rev. Lett. **95**, 260501 (2005).
- [107] P. G. Kwiat and H. Weinfurter, Phys. Rev. A **58**, 2623 (1998).
- [108] Z. B. Chen Phys. Rev. A **73**, 050302 (2006).
- [109] L. B. Fu, Phys. Rev. Lett. **92**, 130404 (2004).

BIBLIOGRAPHY

- [110] G. A. Durkin and C. Simon, Phys. Rev. Lett. **95**, 180402 (2005).
- [111] C. M. Li and D. S. Chuu (unpublished).
- [112] C. M. Li, D. S. Chuu, and Y. N. Chen (unpublished).
- [113] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989); D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
- [114] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).

[115] L. Masanes, Quant. Inf. Comp. **3**, 345 (2003).

[116] One can rephrase the function $g^{(rt)}(\eta)$ as

$$g^{(rt)}(\eta) = 2 \left\{ \frac{\sin\left[\left(d - \frac{1}{2}\right) \frac{2\pi\eta_{rt}}{d}\right]}{2 \sin\left(\frac{2\pi\eta_{rt}}{2d}\right)} - \frac{1}{2} \right\}, \quad (\text{C.1})$$

where $\eta_{rt} = \eta + \nu + \nu_{rt}$. Then using the formula about series of cosine helps us to simplify the function further by

$$\begin{aligned} g^{(rt)}(\eta) &= \sum_{n=1}^{d-1} 2 \cos(2\pi n \eta_{rt} / d) \\ &= \sum_{n=1}^{d-1} \omega^{\eta_{rt} n} + \omega^{-\eta_{rt} n}, \end{aligned} \quad (\text{C.2})$$

where $\omega = \exp(i2\pi/d)$. Since $\sum_{\eta=0}^{d-1} \omega^{\eta_{rt} n} = \sum_{\eta=0}^{d-1} \omega^{-\eta_{rt} n} = 0$ for $\nu + \nu_{rt} \neq 0$, we conclude $\sum_{\eta=0}^{d-1} g^{(rt)}(\eta) = 0$.

- [117] D. Gottesman, Ph. D. thesis, California Institute of Technology, Pasadena, CA, 1997.
- [118] Y. Y. Liao, Y. N. Chen, C. M. Li, and D. S. Chuu, J. Phys. B: At. Mol. Opt. Phys. **39**, 421 (2006).

BIBLIOGRAPHY

- [119] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, Phys. Rev. Lett. **95**, 120405 (2005).
- [120] L. Y. Hsu, Phys. Rev. A **73**, 042308 (2006).
- [121] C. M. Li (unpublished).
- [122] M. Hein, J. Eisert, and H. J. Briegel, Phys. Rev. A **69**, 062311 (2004).
- [123] H. Weinfurter and M. Żukowski, Phys. Rev. A **64**, 010102 (2001); M. Eibl *et al.*, Phys. Rev. Lett. **90**, 200403 (2003).
- [124] C. M. Li and D. S. Chuu (unpublished).
- [125] K. L. Chung and F. Aitsahlia, *Elementary Probability Theory* (Springer-Verlag New York Inc., 2006).
- [126] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [127] E. Maneva and J. Smolin, LANL e-print quant-ph/0003099.
- [128] N. Metwally, Phys. Rev. A **66**, 054302 (2002).
- [129] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Phys. Rev. A **67**, 022310 (2003).
- [130] J. Y. Hsieh, C. M. Li, and D. S. Chuu, Phys. Lett. A **8**, 80 (2006).
- [131] C. Macchiavello, Phys. Lett. A **246**, 385 (1998).
- [132] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997); M. Horodecki, P. Horodecki, and R. Horodecki, *ibid* **80**, 5239 (1998).
- [133] N. Gisin, Phys. Lett. A **328**, 94 (2004).
- [134] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

BIBLIOGRAPHY

- [135] P. Badziag, M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A. **62**, 012311 (2000).
- [136] A. Ekert and C. Macchiavello, Phys. Rev. Lett. **77**, 2585 (1996).
- [137] D. Gottesman, Phys. Rev. A **54**, 1826 (1996).
- [138] A. R. Calderbank, E. M. Rains, P. W. Shor, and N.J.A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
- [139] S. L. Braunstein and J. A. Smolin, Phys. Rev. A **55**, 945 (1997).
- [140] E. Knill, R. Lafamme, R. Matrtinez, and C. Negrevergne, Phys. Rev. Lett. **86**, 5811 (2001).
- [141] J. Y. Hsieh, C. M. Li, and D. S. Chuu, New J. Phys. **8**, 80 (2006).
- [142] A. M. Steane, Phys. Rev. Lett. **76**, 793 (1996).
- [143] J. Y. Hsieh and C. M. Li, LANL e-print quant-ph/0405038.
- [144] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A **54**, 1034 (1996).
- [145] W. H. Zuerk, Rev. Mod. Phys. **75**, 715 (2003).
- [146] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).
- [147] S. Bose, I. Fuentes-Guridi, P. L. Knight, and V. Vedral, Phys. Rev. Lett. **87**, 050401 (2001); R. W. Rendell and A. K. Rajagopal, Phys. Rev. A **67**, 062110 (2003).
- [148] D. Braun, Phys. Rev. Lett. **89**, 277901 (2002); Y. N. Chen, D. S. Chuu, and T. Brandes, Phys. Rev. Lett. **90**, 166802 (2003); M. Paternostro, W. Son, and M. S. Kim, Phys. Rev. Lett. **92**, 197901 (2004); Y. N. Chen, T. Brandes, C. M. Li, and D. S. Chuu, Phys. Rev. B **69**, 245323 (2004).
- [149] M. Plenio, S. F. Huelga, A. Beige, and P. L. Knight, Phys. Rev. A **59**, 2468 (1999).

BIBLIOGRAPHY

- [150] C. Cabrillo, J.I. Cirac, P. Garcia-Fernandez, and P. Zoller, Phys. Rev. A **59**, 1025 (1999); X. X. Yi, C. S. Yu, L. Zhou, and H. S. Song, Phys. Rev. A **68**, 052304 (2003).
- [151] H. Nakazato, T. Takazawa, and K. Yuasa, Phys. Rev. Lett. **90**, 060401 (2003); H. Nakazato, M. Unoki, and K. Yuasa, Phys. Rev. A **70**, 012303 (2004); G. Compagno, A. Messina, H. Nakazato, A. Napoli, M. Unoki, and K. Yuasa, *ibid* **70**, 052316 (2004).
- [152] L. A. Wu, D. A. Lidar, S. Schneider, Phys. Rev. A **70**, 032322 (2004).
- [153] C. M. Li, Y. N. Chen, C. W. Luo, J. Y. Hsieh, and D. S. Chuu, Int. J. Quantum Inf. **3**, Issue 1 supp., 111 (2005).
- [154] C. M. Li, Y. N. Chen, C. W. Luo, and D. S. Chuu (unpublished).
- [155] M. Plenio and P.L. Knight, Rev. Mod. Phys. **70**, 101 (1998).
- [156] Actually, the pulse E field is the "THz radiation" which could be easily generated from GaAs semiconductor or several nonlinear crystals such as GaSe.
- [157] Q. Wu and X. C. Zhang, Appl. Phys. Lett. **71**, 1285 (1997).
- [158] J. H. Reina and N. F. Johnson, Phys. Rev. A **63**, 012303 (2001); F. de Pasquale *et al.*, Phys. Rev. Lett. **93**, 120502 (2004); O. Sauret *et al.*, Phys. Rev. B **69**, 035332 (2004).
- [159] Y. N. Chen, C. M. Li, T. Brandes, and D. S. Chuu, New J. Phys. **7**, 172 (2005).
- [160] R. G. DeVoe and R. G. Brewer, Phys. Rev. Lett. **76**, 2049 (1996).
- [161] S. Bose *et al.*, Phys. Rev. Lett. **83**, 5158 (1999).
- [162] S. J. van Enk *et al.*, Phys. Rev. Lett. **78**, 4293 (1997). E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
- [163] L. K. Grover, Phys. Rev. Lett. **80**, 4329 (1998).
- [164] G. L. Long, Y. S. Li, W. L. Zhang, and C. C. Tu, Phys. Rev. A, **61**, 042305 (2000).

BIBLIOGRAPHY

- [165] G. L. Long, Phys. Rev. A, **64**, 022307 (2001).
- [166] P. Høyer, Phys. Rev. A, **62**, 052304 (2000).
- [167] G. L. Long, L. Xiao, and Y. Sun, e-print quant-ph/0107013.
- [168] J. Y. Hsieh and C. M. Li, Phys. Rev. A **65**, 052322 (2002).
- [169] A. Galindo, M. A. Martín-Delgado, Phys. Rev. A, **62**, 062303 (2000).
- [170] C. M. Li, C. C. Hwang, J. Y. Hsieh, and K. S. Wang, Phys. Rev. A, **65**, 034305 (2002).
- [171] E. Biham, O. Biham, D. Biron, M. Grassl, D. Lidar, and D. Shapira, Phys. Rev. A **63**, 012310(2000).
- [172] B. Pablo-Norman and M. Ruiz-Altaba, Phys. Rev. A **61**, 012301 (2000).
- [173] J. Y. Hsieh, C. M. Li, and D. S. Chuu, Chinese J. Phys. **42**, 585 (2004).
- [174] J. Preskill, Proc. R. Soc. London, Ser A **454**, 385 (1998).
- [175] C. R. Hu, Phys. Rev. A **66**, 042301 (2002).
- [176] J. Y. Hsieh, C. M. Li, and D. S. Chuu, Int. J. Quantum Inf. **2**, 285 (2004).
- [177] C. M. Li, J. Y. Hsieh, and D. S. Chuu, Chinese J. Phys. **45**, 637 (2007).
- [178] E. Farhi and S. Gutmann, Phys. Rev. A **57**, 2403(1998).
- [179] S. A. Fenner, e-print quant-ph/0004091.
- [180] J. Bae and Y. Kwon, Phys. Rev. A **66**, 012314(2002).
- [181] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, e-print quant-ph/0001106.
- [182] W. van Dam, M. Mosca, and U. Vazirani, in Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science (IEEE Computer Society Press, New York, 2001), pp. 279–287.

BIBLIOGRAPHY

- [183] J. Roland and N.J. Cerf, Phys. Rev. A **65**, 042308 (2002).
- [184] J. Y. Hsieh, C. M. Li, and D. S. Chuu, J. Phys. Soc. Jpn. **74**, 2945 (2005).
- [185] L. K. Grover and A. M. Sengupta, Phys. Rev. A, **65**, 032319(2002).
- [186] J. Roland and N. J. Cerf, Phys. Rev. A **68**, 062311(2003).
- [187] D. Schlingemann and R. F. Werner, Phys. Rev. A **65**, 012308 (2002).
- [188] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
- [189] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
- [190] N. Kiesel *et al.*, Phys. Rev. Lett. **95**, 210502 (2005).
- [191] P. Walther, M. Aspelmeyer, K.J. Resch, and A. Zeilinger, Phys. Rev. Lett. **95**, 020403 (2005).
- [192] T.P. Bodiya and L. M. Duan, Phys. Rev. Lett. **97**, 143601 (2006).
- [193] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [194] L. Y. Hsu and C. M. Li, Phys. Rev. A **71**, 022321 (2005).
- [195] C. M. Li, J. Y. Hsieh, and D. S. Chuu (unpublished).
- [196] David A. Meyer, Phys. Rev. Lett. **85**, 2014 (2000).
- [197] P. Londero *et al.*, Phys. Rev. A **69**, 010302 (2004).