UNIVERSITY OF CALGARY

Verifiable Relativistic Quantum Communication

by

Yadong Wu

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN PHYSICS AND ASTRONOMY

CALGARY, ALBERTA

NOVEMBER, 2019

Abstract

Quantum summoning retrieves quantum information prepared at some point in spacetime at another point, which is randomly chosen from a set of points. This thesis presents an efficient quantum summoning protocol based on a quantum error-correcting code, along with encoding and decoding methods. This protocol reduces space complexity as well as gate complexity of encoding compared to previous best results. Our throughout study of quantum summoning paves the way for investigating relativistic quantum cryptography with quantum summoning as a primitive.

This thesis also studies a relativistic continuous-variable quantum secret sharing protocol in non-inertial frame, which includes the effect of acceleration of quantum shares in spacetime. By formulating the relativistic effect as a Gaussian lossy channel, we analyze how the fidelity of quantum secret sharing protocol is affected by this relativistic effect. This investigation relaxes the common assumption of secret sharing in inertial frames and this framework can be applied to other relativistic quantum communication protocols.

To efficiently verify bosonic quantum channels, I propose a framework of verification of quantum channels plus average-fidelity witness. For both multi-mode Gaussian unitary channels and single-mode amplifying channels, I present efficient verification protocols utilizing only two-mode squeezed vacuum states and homodyne detections. Our work is significant in verification of quantum components in continuous-variable quantum information processing.

Preface

The results reported in this thesis are published in peer-reviewed journals. The content of these articles are used in my thesis either verbatim or with some modifications as required. My publications are

NJP19 Ya-Dong Wu, Barry C. Sanders, “Efficient verification of bosonic quantum channels via benchmarking", New Journal of Physics **21**, 073026 (21 pp.), 2019.

NJP18 Ya-Dong Wu, Abdullah Khalid, Barry C. Sanders, “Efficient Code for Relativistic Quantum Summoning", New Journal of Physics **20**, 063052 (18 pp.), 2018.

PRD17 Mehdi Ahmadi, Ya-Dong Wu, Barry C. Sanders,“Relativistic (2,3)-threshold quantum secret sharing", Physical Review D **96**, 065018 (10 pp.), 2017.

The materials taken from these papers and the modifications made for this thesis are listed below:

- In Chapter 1, sections 1.2, 1.3 and 1.4 are taken verbatim the introduction sections of [NJP19], [NJP18], and [PRD17], respectively.
- Subsections 2.2.4, 2.2.5 and 2.2.6 are taken mostly verbatim from Sec. II. B, II. C and II. D of [NJP18], respectively.
- Subsections 2.3.5 and 2.4.5 contain two figures published in [PRD17].
- Sections 3.1 and 3.2 are taken verbatim from Sec. II A and Sec. III of [NJP18], respectively.

- Chapter 4 is taken mostly verbatim from [NJP18] except Sec. 4.2, which is new material written for this thesis.
- Chapter 5 is taken mostly verbatim from [PRD17] except some notations are changed.
- Sections 6.2 and 6.3 are taken verbatim from Secs. II B and II C of [NJP19], respectively.
- Chapter 7 is taken verbatim from Secs. III, IV, V and IV of [NJP19].

Acknowledgements

I would like to thank my supervisor Barry C. Sanders, who gave me the chance to come to Calgary to pursue a PhD degree in physics. Thanks for his patient guidance and insightful comments for my work. Also great thanks for his financial support for me to attend international conferences as well as visiting USTC Shanghai Institute.

I want to thank Gilad Gour, Christoph Simon, as well as Alexander Lvovsky for their serving in my supervisory committee. Also thanks to David Feder for his work as an examiner in my candidacy exam. Thanks to all of them for their great work. Their strict requirements helped me to build broad background knowledge on quantum information.

Great thanks to Mehdi Ahmadi, from whom, I learned relativistic quantum information. Thanks to Abdullah Khalid, who helped me with scientific writing and had many discussions with me. I also want to thank Dominic Berry, Dong-Xiao Quan, Masoud Habibi Davijani, Yunlong Xiao, Jiawei Ji, Nana Liu and Si-Hui Tan for inspiring discussions with me and insightful comments on my work.

I want to say thanks to my friends and colleagues in both Calgary and Shanghai. Thanks to my parents and my wife for their support.

Table of contents

List of figures and illustrations

List of tables

List of symbols, abbreviations and glossaries

Symbol or abbreviation	Definition
$\mathbb{R}$	Real number
$\mathbb{C}$	Complex number
$\mathbb{Z}_2$	$\{0,1\}$
GF(2)	Galois field consisting of $\mathbb{Z}_2$
$\mathscr{H}$	Hilbert space
$\mathscr{L}$	Space of linear transformations
ρ	Density operators or density matrices
N	Number of causal diamonds
$\tilde{N}$	$2\left\lceil\frac{N}{2}\right\rceil$
Q	Number of qubits to summon one qubit
$\mathcal{E}$	Quantum channel
$\mathcal{E}_c$	Canonical form of a single-mode Gaussian channel
$\mathcal{C}_\mathcal{E}$	Choi matrix of quantum channel $\mathcal{E}$
$F(\rho,\sigma)$	Fidelity between two states ρ and σ
$\bar{F}_\mathcal{E}$	Average fidelity of channel $\mathcal{E}$
$F_\mathrm{E}(\mathcal{E})$	Entanglement fidelity of channel $\mathcal{E}$
$\mathbb{1}$	Identity operator or identity matrix
$\lvert\Phi^+\rangle$	Maximally-entangled state
$\mathscr{I}$	Isometry
U	Unitary operation
$\lVert\ \rVert_1$	Schatten1-norm
$\lVert\ \rVert$	Euclidean norm
$\lVert\ \rVert_\infty$	Schatten ∞-norm or operator norm
$\lVert\ \rVert_\diamond$	Diamond norm
CZ	Controlled-Z gate
H	Hadamard gate
$\mathcal{G}_n$	n-qubit Pauli group
Ξ	Set of correctable Pauli operators
$\{\lvert\bar{i}\rangle\}$	Orthonormal basis of code space
$[[n,k,d]]$	n physical qubits encoding k logical qubits with distance d
$\boldsymbol{H}$	Parity check matrix
$\boldsymbol{G}$	Generator matrix
$\mathcal{C}$	Linear code
$\mathcal{S}$	Stabilizer group

$C(\mathcal{S})$	Centralizer of $\mathcal{S}$ in Pauli group
(k,n)-threshold	Secret is encode into n shares, at least k shares are authorized to decode the secret
$[a,b]$	$ab-ba$
$\hat{a}$	Annihilation operator
$\hat{a}^\dagger$	Creation operator
$\hat{q}$	Position operator
$\hat{p}$	Momentum operator
$\langle O \rangle$	Mean value of observable O
$\lvert 0 \rangle_{\mathscr{F}}$	Vacuum state
$\lvert n \rangle_{\mathscr{F}}$	Fock state
$\hat{n}$	Photon number operator
$\bar{n}$	Mean photon number
$\rho_T(\bar{n})$	Thermal state with mean photon number $\bar{n}$
$\mathcal{H}$	Hamiltonian
ω	Frequency in inertial frame
ω'	Rindler coordinate frequency
$\tilde{\omega}$	Proper frequency during acceleration
$\boldsymbol{k}$	Wave number
$D(\boldsymbol{\alpha})$	Weyl displacement operator
χ_ρ	Characteristic function of ρ
$\mathscr{W}_\rho$	Wigner function of ρ
P_ρ	P-function of ρ
Q_ρ	Q-function of ρ
$\hat{\boldsymbol{x}}$	$\{\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_m, \hat{p}_m\}$
$\bar{\boldsymbol{x}}$	$\langle \hat{\boldsymbol{x}} \rangle$
$\boldsymbol{V}$	Covariance matrix
$\boldsymbol{\Omega}$	$\bigoplus^m \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$
$HW(m)$	Heisenberg-Weyl group on m-mode phase space
$Sp(2m,\mathbb{R})$	$2m$-dimensional real symplectic group
$\mathscr{R}$	Minimal rank of a single-mode Gaussian channel
ζ	Transmissivity of a single-mode Gaussian channel
$\hat{q}^{(0)}$	Position operator of vacuum state
$\hat{p}^{(0)}$	Momentum operator of vacuum state
g_{ab}	Metric tensor
χ	Rindler coordinate position
η	Rindler coordinate time
c	Speed of light
a	Proper acceleration
a_c	Proper acceleration at the center of cavity
τ	Proper time
L	Proper length of cavity
L'	Rindler coordinate length of cavity
$\Box$	d'Alembert operator

$\phi_k, k \in \mathbb{N}$	Mode functions
h	$a_{\mathrm{c}}L$
u	$\frac{\tilde{\omega}\tau}{2\pi k}$
$F^{(0)}$	Zeroth-order coefficient of F in terms of h
$F^{(2)}$	Second-order coefficient of F in terms of h
$\diamondsuit_i$	ith Causal diamond
y_i	ith Request point
z_i	ith Reveal point
$\prec$	Causally preced
$\succ$	Causally succeed
Σ	Spacetime region
$\mathscr{G}$	Graph
V	Set of vertices
E	Set of edges
K_n	n-vertex complete graph
2^{E_k}	Power set of the set of edges in K_n
$\mathscr{E}$	Binary linear space comprising all the elements in 2^{E_k}
e_{ij}	Edge connecting vertices v_i and v_j
$\boldsymbol{A}_i$	Binary vector represented by star graphs
$\boldsymbol{T}_{ijk}$	Binary vector represented by triangular graphs
Π	Performance operator
$1/\lambda$	Variance of Gaussian distribution of amplitude
$\|\alpha\rangle$	Coherent state with amplitude $\alpha \in \mathbb{C}$
$\|\boldsymbol{\alpha}\rangle$	$\|\alpha_1\rangle \otimes \|\alpha_2\rangle \otimes \cdots \otimes \|\alpha_m\rangle$
$\boldsymbol{S}$	Symplectic transformation on phase space
$\boldsymbol{d}$	Displacement vector on phase space
$U_{\boldsymbol{S},\boldsymbol{d}}$	Gaussian unitary operation characterized by $\boldsymbol{S}$ and $\boldsymbol{d}$
S_κ	Two-mode squeezing operation $\mathrm{e}^{\frac{\kappa}{2}\left(\hat{a}_1\hat{a}_2+\hat{a}_1^\dagger\hat{a}_2^\dagger\right)}$
$\|\kappa\rangle_{\mathrm{TMSV}}$	$S_\kappa \|0\rangle_{\mathscr{F}}$
ε	Estimation error bound
δ	Maximal failure probability
ρ_{p}	Prepared state
ρ_{t}	Target state
W	Fidelity witness
$\mathcal{W}(\rho_{\mathrm{p}})$	Mean value of W on state ρ_{p}
$\bar{F}_{\max}$	Maximal achievable average fidelity
$\mathcal{W}(\mathcal{E})$	Mean value of $W_{\mathrm{A}'\mathrm{R}}$ on state $\mathcal{E} \otimes \mathcal{I}(\|\Psi\rangle\langle\Psi\|)$
F_{t}	Fidelity threshold
$\bar{F}_{\mathrm{t}}$	Average-fidelity threshold
$\mathfrak{g}$	Amplification gain
CP	Complex projective
POVM	Positive operator-valued measure
CPTP	Completely positive and trace-preserving
QEC	Quantum error correction

CWS	Codeword stabilized
CSS	Calderbank-Shor-Steane
CNOT	Controlled-not
QSS	Quantum secret sharing
CV	Continuous-variable
SPDC	Spontaneous parametric down-conversion
TMSV	Two-mode squeezed vacuum
BBB	Basic building block
SPAM	State-preparation and measurement
TEM	Transverse electromagnetic

Chapter 1

Introduction

1.1 Research Problems and Objects

In quantum information, we usually ignore the spacetime structure where quantum information processing tasks are performed, which is fine in most cases, as we usually consider quantum information processing on earth and the spatial scale of experimental settings is not huge. However, to understand quantum information problems in subtle spacetime structures [55, 51], we have to consider spacetime structure. The first step before considering subtle spacetime structure is to investigate quantum information processing in Minkowski spacetime. One fundamental question is how quantum information is flowed in Minkowski spacetime. Quantum teleportation [14], together with quantum error correction [46] or quantum secret sharing [27] implies that quantum information does not have to follow a specific trajectory in spacetime, whereas can be delocalized in spacetime, flowing along multiple trajectories and later localized again at a point in spacetime [52].

Quantum summoning [65, 52] is an operational quantum task to investigate where and when quantum information can be distributed in Minkowski spacetime. The conditions for the accomplishment of quantum summoning implies the limitations of distribution of quantum information in spacetime. To fully understand the distribution of quantum information in spacetime from an operational perspective, we are interested in investigating what is the most efficient encoding and

decoding method for quantum summoning. We aim to construct a more efficient encoding and decoding approach for quantum summoning than previous results.

During the distribution of quantum information in spacetime, relativistic effects may introduce decoherence into the quantum information. How relativistic effects affect the evolution of quantum information depends on how quantum information is encoded in physical systems [94]. For instance, the relativistic non-inertial motion between a measurement device and a quantum system can affect the quantum information detected by the measurement device, as shown by Unruh effect [33, 114]. Here we are interested in how relativistic effects affect localized quantum information. We aim to solve the relativistic effects on continuous-variable quantum secret sharing protocols in non-inertial frames.

The above relativistic effects on quantum information can be formulated as noisy quantum channels. These noisy channels reduce the fidelity of quantum communication in spacetime. One natural problem is how to characterize these noisy quantum channels. The most common way, up to now, is quantum-process tomography [76], which is, however, quite resource-consuming. Furthermore, to realize quantum supremacy, verification of reliable quantum devices is significant. Although in last decade, partial quantum characterization approaches, like fidelity estimation [41, 31] and randomized benchmarking [81], have been proposed, these methods cannot be readily adapted to verification of continuous-variable quantum channels [116], where quantum information is encoded in infinite-dimensional Fock space. We aim to construct an efficient and feasible verification method for verification of bosonic quantum channels.

1.2 Quantum summoning

Quantum summoning is the task of encoding and transmitting quantum information to a configuration of spacetime causal diamonds such that the quantum information can be reconstructed in any one of these causal diamonds [65, 52, 54, 2]. Quantum summoning cannot be guaranteed to work for every configuration of causal diamonds because quantum information cannot be

copied [93, 120, 34, 91] or transmitted superluminally [120]. Summoning is only possible for a configuration of causal diamonds if every pair of diamonds is causally related, where two diamonds are causally related if the earliest point of one can communicate with the latest point of the other [52]. We aim to construct efficient protocols for summoning quantum information in any configuration of N pairwise-related causal diamonds.

A variety of work has been done on summoning ever since Kent introduced this task and presented a no-summoning theorem [65]. Hayden and May [52] showed that quantum summoning can be reduced to the primitives of quantum secret sharing [27, 47, 83] and teleportation [14, 117]. They exploited a codeword-stabilized (CWS) quantum code [30] to design a summoning protocol that is efficient in the sense that the number of qubits used by the code is polynomial in N. Hayden et al. [54] interpreted quantum summoning as superposition of quantum information in delocalized spacetime regions, also called "spacetime replication of quantum information". They proposed an efficient protocol to perform this task for continuous-variable quantum information, as well as showing that optical circuits can be used to realize summoning experimentally. In 2016, Adlam and Kent proposed a summoning task with multiple summonses and provided a protocol, which employs teleportation, to accomplish this task for the configuration being an ordered set of causal diamonds [2].

Our protocol for summoning quantum information uses a Calderbank-Shor-Steane (CSS) code [22, 108]

$$\left[\left[\binom{\tilde{N}}{2}, 1, \frac{\tilde{N}}{2}\right]\right], \tilde{N} = 2\left\lceil \frac{N}{2} \right\rceil \in 2\mathbb{Z}, \tag{1.1}$$

that encodes one qubit into $\binom{\tilde{N}}{2}$ physical qubits, with the restriction that $\tilde{N}$ is even. We calculate that this CSS code distance $\frac{\tilde{N}}{2}$, and this code is constructed from the relation between graphs and linear algebra [35, 19]. Our code is a qubit version of the homological continuous-variable quantum error-correcting code [54] and corrects erasure errors that occur in summoning.

We provide a procedure to construct the encoding and decoding circuits for our CSS code for any even positive integer $\tilde{N}$. The number of qubits Q used by our protocol is reduced by a factor of two compared to the previous best [52], and the number of quantum gates is reduced

from $O\left(N^3\right)$ [52] to $O\left(N^2\right)$. Our decoding procedure has gate complexity $O(N)$. Our results are significant in that we complete the quantum summoning protocol [65, 52, 54] by providing both encoding and decoding schemes, explain how to utilize quantum error correction for summoning, analyze quantum resources, and demonstrate improved efficiency for our protocol.

1.3 Relativistic quantum secret sharing

In (k,n)-threshold quantum secret sharing, the dealer encodes a quantum secret in n quantum systems (or quantum shares), which he then distributes to n players. Each player receives exactly one share, where any subsets of k or more players form the access structure to retrieve the secure key while any subsets of fewer than k players; i.e., the adversarial structure, cannot learn any information whatsoever about the key. Continuous-variable threshold quantum secret sharing still faces the challenge that information about the quantum secret can be leaked into the adversarial structure [113, 69]. Various models of secret sharing exist with quantum or classical channels that can be public or private and a graph-state formalism was proposed to unify these models [83]. Here we consider the scenario wherein the dealer shares quantum channels with each player, and also the players share quantum channels between each other, which is known as the quantum-quantum case [83].

We focus on a relativistic variant of a $(2,3)$-threshold quantum secret sharing protocol which is the smallest-sized non-trivial protocol. We take into account the relativistic motion of the quantum shares in Minkowski spacetime during the distribution and collaboration and how it influences the success of the protocol. In the relativistic protocol, similar to the non-relativistic case [27], a dealer encodes the quantum secret into several quantum shares and distributes them to all the players. The players are located at different regions in the Minkowski spacetime and the dealer and the players are all stationary. Under such circumstances, during the dealer's distribution, the quantum shares experience non-uniform motion, as they are transmitted to spacetime points in the future light cone

of the dealer (Fig. 5.4). Then, a subset of players within the access structure collaborate to retrieve the quantum secret by sharing their shares. However, to reach the same spacetime point, the shares go through phases of accelerating and decelerating motion while being transmitted. We analyze the possible collaboration scenarios between the players; i.e., Players 1 and 2 collaborate (Fig. 5.6) or Players 2 and 3 collaborate (Fig. 5.9). In each scenario, we investigate how the non-inertial motion of the shares affects the fidelity of the quantum secret sharing protocol.

In $(2,3)$-threshold quantum secret sharing, the dealer encodes the quantum secret in three quantum shares in a localized manner, hence, we need to be able to analyze the effect of relativity on such systems. The relativistic effects on the state of localized quantum systems has been studied using different setups [21, 42, 37, 38, 5, 101, 36]. We find the framework of accelerating cavities a suitable choice for this purpose, as it can be adapted to study the effect of non-uniform motion on localized quantum fields [21, 42]. Accelerating cavities have been employed in the past to study the relativistic effects on quantum clocks [74], quantum teleportation [42], and to estimate proper acceleration [4, 3] to name a few. However, we develop a different approach from the previous studies for accelerating cavities; we formulate the evolution of the quantum field inside an accelerating cavity as a bosonic quantum Gaussian channel which we then use to include the effects of non-uniform motion of the quantum shares. Furthermore, this approach enables us to compute physical quantities, such as the average number of produced thermal particles and transmissivity of the relativistic channel.

1.4 Quantum verification

Progress in optical quantum computing [84, 10, 109] demands efficient schemes to verify performance of optical quantum processes, which would serve as components and devices for the quantum system. Characterization by quantum process tomography [26, 96, 32, 9, 90, 76, 99] could

serve as a means for gathering sufficient assessment data to be used for verification, but, unfortunately, quantum process tomography is inefficient: the sampling overhead scales exponentially with system size, with system size being logarithmic in Hilbert space dimension corresponding to how much quantum information (e.g., number of qubits) required to describe the system. Direct fidelity estimation [41, 31] provides a way to partially characterize quantum channels with less overhead, but its adaption to bosonic channels requires measuring the Wigner function of output states at each phase-space point, and hence is not feasible due to the non-compactness of phase space. Randomized benchmark [81, 82, 115, 98] provides a scalable method to evaluate the average performance of Clifford gates; however, its adaption to bosonic channels is not readily obtained because Gaussian unitary operations, as continuous-variable analog of Clifford gates, do not form an exact unitary 2-design [127]. We aim to devise efficient and experimentally feasible verification schemes for bosonic channels.

Quantum-state verification is widely studied [11, 50, 110, 44, 92, 126]. Reliable and efficient verification schemes [11] for both bosonic Gaussian pure states and pure states generated by photon-number state inputs, linear optical interferometers, and photon number detections has been generalized to non-Gaussian cubic phase states [75]. These verification approaches have been adapted to benchmarking continuous-variable (CV) quantum gates [40]. On the other hand, a series of quantum-process benchmark approaches for bosonic channels have been explored [24, 23, 124, 12]. An alternative approach benchmarks the average fidelity of bosonic quantum processes over all coherent states by preparing a two-mode squeezed vacuum state and measuring a single observable [12].

An experimentally appealing adaptation [40] of recent verification schemes [11, 75] only estimates average fidelity over a finite-dimensional subspace chosen by selecting a finite set of coherent states. This subspace selection cannot assess quantum-channel performance over the entire infinite-dimensional Hilbert space $\mathscr{H}$. In contrast, the alternative scheme [12] is challenged by experimental limitations: online squeezing, which squeezes *any* state known or unknown [125, 86], and quantum memories [80, 103]. Here we combine the favorable features of the state verifica-

tion approach [11] and the unified quantum-benchmark approach [12] to develop our verification schemes for bosonic channels.

We formulate quantum-channel verification as an adversarial game between a technology-limited verifier and an untrusted, powerful prover who has significant but bounded quantum technology. Our average-fidelity witness issues a certificate that contains a tight lower bound of the average fidelity of the quantum channel. We develop a general framework for verification of optimal quantum channels, and, as examples of this framework, we present reliable and experimentally feasible verification schemes for both multi-mode Gaussian unitary channels and single-mode amplification channels. Both schemes can be implemented by preparing two-mode squeezed vacuum states and applying local homodyne detections, and the sample complexities for both two schemes scale polynomially with all channel-specification parameters. Thus, our results provide experimentally feasible tests of quantum components in bosonic quantum systems.

1.5 Overviews of chapters

In chapter 2, I review background on quantum information theory, including elementary quantum information, quantum error correction, Gaussian quantum information as well as relativistic quantum information, which lay the foundation for investigation in following chapters. Chapter 3 reviews quantum summoning, including original quantum summoning protocol and generalized summoning protocols. In chapter 4, I present our results on efficient code for quantum summoning. We propose a protocol based on a quantum error-correcting code to summon single qubits, which consumes fewer resources than previous best results, plus encoding and decoding circuits. In chapter 5, we develop a non-inertial quantum secret sharing protocol, including the relativistic effects during the distribution of quantum shares. Specifically, we investigate how the fidelity of a $(2, 3)$ quantum secret sharing protocol is affected by acceleration effects on quantum shares. Chapter 6 reviews several partial characterization approaches for quantum systems, including fidelity estimation, verification and benchmarking. Chapter 7 presents a general framework for verification

of quantum channels plus an average-fidelity witness, which yields a tight lower bound of average fidelity. For multi-mode Gaussian unitary channels and single-mode amplifying channels, we present feasible and reliable verification protocols, where sample complexities scale polynomially with all channel parameters. Chapter 8 is the conclusion of this thesis and outlook.

Chapter 2

Background

2.1 Elements in quantum information

This section briefly reviews some basic knowledge and essential results in quantum information theory. In Subsec. 2.1.1, I present the basic concepts of density matrix, positive operator-valued measure (POVM) and quantum no-cloning theorem. Subsection 2.1.2 explains the definition of quantum channels and various representations of quantum channels. Subsection 2.1.3 reviews trace distance and fidelity of quantum states and average fidelity of quantum channels. Most content in this section can be found in Refs. [88, 118].

2.1.1 Quantum states, measurements and no-cloning theorem

Given a d-dimensional Hilbert space $\mathscr{H}$, a quantum pure state is represented by a vector $|\psi\rangle \in \mathscr{H}$[1]. A general quantum state is represented by a density matrix $\rho \in \mathscr{L}(\mathscr{H})$, where $\mathscr{L}(\mathscr{H})$ denotes the space of linear transformations on $\mathscr{H}$, such that ρ is positive semi-definite and $\mathrm{tr}(\rho) = 1$.

[1] Precisely speaking, one pure state is a point in a complex projective space.

Any measurement on state ρ can be represented by a POVM $\{M_i\}$, where for each i,

$$M_i \geq \mathbf{0}, \tag{2.1}$$

and

$$\sum_i M_i = \mathbb{1}. \tag{2.2}$$

Each M_i corresponds a different measurement outcome labeled by i, and the probability to obtain measurement outcome i is

$$p_i = \mathrm{tr}(M_i \rho). \tag{2.3}$$

It is easy to check that the total probability sum equals one due to Eq. (2.2). When $\{M_i\}$ are orthogonal from each other, the associated measurement is called a projective measurement.

A special property of quantum information, which is different from classical information is the quantum no-cloning theorem: an unknown quantum state cannot be copied. No-cloning theorem can be easily proved using proof of contradiction. Suppose there is a unitary operation U on $\mathscr{H}^{\otimes 2}$ such that $\forall |\psi\rangle \in \mathscr{H}$,

$$U |\psi\rangle |\mathrm{anc}\rangle = |\psi\rangle |\psi\rangle, \tag{2.4}$$

where $|\mathrm{anc}\rangle$ is an ancillary qudit. Then for $|\phi\rangle \neq |\psi\rangle$, Eq. (2.4) yields

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2, \tag{2.5}$$

which indicates that $|\phi\rangle$ and $|\psi\rangle$ must be orthogonal. Thus, the assumption in Eq. (2.4) is not true, and an unknown quantum state cannot be copied.

This subsection briefly reviews the mathematical concepts of quantum states and quantum measurements as well as the quantum no-cloning theorem. The next subsection explains quantum channels, which includes quantum measurements as a special case.

2.1.2 Quantum channels

In this section, I first explain that a quantum channel is a completely positive and trace-preserving (CPTP) map. Then I show three different representations of quantum channels.

A quantum channel $\mathcal{E}$ is a linear map

$$\mathcal{E} : \mathscr{L}(\mathscr{H}) \mapsto \mathscr{L}(\mathscr{H}). \tag{2.6}$$

$\mathcal{E}$ should map a density matrix to another density matrix, i.e., for any positive semi-definite matrix ρ with trace one, $\mathcal{E}(\rho)$ is also positive semi-definite and has trace one. This means that $\mathcal{E}$ is positive and trace-preserving. Furthermore, $\mathcal{E}$ is completely positive, which means that for any positive-semidefinite matrix $\rho' \in \mathscr{L}(\mathscr{H}^{\otimes 2})$, $\mathcal{E} \otimes \mathbb{1}(\rho')$ is positive-semidefinite as well. Thus, a quantum channel $\mathcal{E}$ is a CPTP map.

There are several different parametrization methods or representations for a quantum channel. The first is Choi-Jamiołkowski isomorphism. Given a maximally entangled state

$$|\Phi^+\rangle = \sum_{i=0}^{d-1} |i\rangle |i\rangle , \tag{2.7}$$

the density matrix

$$\mathcal{C}_{\mathcal{E}} \coloneqq \mathcal{E} \otimes \mathbb{1}(|\Phi^+\rangle \langle\Phi^+|) \in \mathscr{L}(\mathscr{H}^{\otimes 2}) \tag{2.8}$$

is called the Choi matrix of $\mathcal{E}$. Choi-Jamiołkowski isomorphism claims that there is a one-to-one correspondence between any quantum channel $\mathcal{E}$ and its Choi matrix $\mathcal{C}_{\mathcal{E}}$. This isomorphism provides a duality between quantum channels and quantum states.

The second representation is Kraus representation. A quantum channel can be represented by a linear mapping

$$\rho \to \sum_i V_i \rho V_i^\dagger , \tag{2.9}$$

where for each i, $V_i^\dagger V_i \geq 0$ and $\sum_i V_i^\dagger V_i = \mathbb{1}$. Actually, $\left\{ V_i^\dagger V_i \right\}_i$ is a POVM. Using the definitions

of POVM, one can see that the linear mapping in Eq. (2.9) is indeed a CPTP map.

The third representation is Stinespring dilation. Any quantum channel $\mathcal{E} : \mathscr{L}(\mathscr{H}_{\mathrm{A}}) \mapsto \mathscr{L}(\mathscr{H}_{\mathrm{A}'})$ can be dilated to an isometry

$$\mathscr{I} : \mathscr{H}_{\mathrm{A}} \mapsto \mathscr{H}_{\mathrm{A}'\mathrm{E}} \tag{2.10}$$

$$\mathscr{I}_{\mathrm{A}\to\mathrm{A}'\mathrm{E}}(|\psi\rangle) = \sum_i V_i |\psi\rangle \otimes |i\rangle\,, \tag{2.11}$$

where E denotes environment and $\{|i\rangle\}_i$ span an orthonormal basis of $\mathscr{H}_{\mathrm{E}}$. It is easy to check that $\mathrm{tr}_{\mathrm{E}}\,\mathscr{I}(\rho)$ yields the linear mapping in Eq. (2.9). As an isometry can be further extended to a unitary transformation from $\mathscr{H}_{\mathrm{AE}}$ to $\mathscr{H}_{\mathrm{A}'\mathrm{E}}$, a quantum channel can be realized by a unitary evolution by tracing out the corresponding environment.

This subsection has reviewed the concepts of quantum channels and three different representation of quantum channels. Choi-Jamiołkowski isomorphism is used for benchmarking bosonic channels in Sec. 6.3 and Stinespring dilation is mentioned when discussing Gaussian channels in Subsec. 2.4.4.

2.1.3 Distance measures

In this subsection, I explain two main distance measures for quantum states, one is fidelity, and the other is trace distance. From these two distance measures for quantum states, I further explain the induced distance measures for quantum channels.

The Schatten 1-norm of an operator M on $\mathscr{H}$ is

$$\|M\|_1 \coloneqq \mathrm{tr}\,|M|, \tag{2.12}$$

where $|M| \coloneqq \sqrt{M^\dagger M}$ is non-negative. Given two density operators ρ_1 and ρ_2, the fidelity between them is

$$F(\rho_1,\rho_2) \coloneqq \|\sqrt{\rho_1}\sqrt{\rho_2}\|_1^2. \tag{2.13}$$

If one of the two states is pure, for instance, $\rho_1 = |\psi\rangle\langle\psi|$, then Eq. (2.13) is simplified to

$$F(\rho_1, \rho_2) = \langle\psi|\rho_2|\psi\rangle. \tag{2.14}$$

$F(\rho_1, \rho_2)$ equals one if and only if $\rho_1 = \rho_2$, and equals zero if and only if ρ_1 and ρ_2 have mutually orthogonal supports.

As fidelity does not satisfy the triangular inequality, it is not a norm distance. The trace distance between these two density operators is

$$\|\rho_1 - \rho_2\|_{\mathrm{tr}} \coloneqq \frac{1}{2}\|\rho_1 - \rho_2\|_1 . \tag{2.15}$$

The relation between fidelity and trace distance is indicated by the following bounding relation

$$1 - \sqrt{F(\rho_1, \rho_2)} \leq \frac{1}{2}\|\rho_1 - \rho_2\|_1 \leq \sqrt{1 - F(\rho_1, \rho_2)}. \tag{2.16}$$

The relation implies that if $F(\rho_1, \rho_2)$ is ε-close to 1, then $\|\rho_1 - \rho_2\|_1$ is bounded above by $2\sqrt{\varepsilon}$. Reversely, if $\|\rho_1 - \rho_2\|_1$ is bounded above by ε, $F(\rho_1, \rho_2)$ must be ε-close to 1.

The trace-distanced induced norm distance between quantum channels $\mathcal{E}$ and $\mathcal{E}'$ is diamond norm

$$\left\|\mathcal{E} - \mathcal{E}'\right\|_\diamond \coloneqq \sup_{|\phi\rangle \in \mathscr{H}^{\otimes 2}} \|\mathcal{E}_1 \otimes \mathcal{I}(|\phi\rangle\langle\phi|) - \mathcal{E}_2 \otimes \mathcal{I}(|\phi\rangle\langle\phi|)\|_1 , \tag{2.17}$$

where $\mathcal{I}$ is an identity channel. Although diamond norm is a norm distance to quantify the difference between two quantum channels, optimization over the Hilbert space is usually analytically challenging. A more useful quantity, especially in experiments, is average fidelity. The average fidelity of $\mathcal{E}$, with respect to a unitary operation U, is

$$\bar{F}_{\mathcal{E}} \coloneqq \int_{\mathscr{H}} \mathrm{d}\psi \, \langle\psi| U^\dagger \mathcal{E}(|\psi\rangle\langle\psi|) U |\psi\rangle , \tag{2.18}$$

where $\mathrm{d}\psi$ is a Haar measure on $\mathscr{H}$. Although average fidelity is not a norm distance, it is common

in experiments to use average fidelity to benchmark the average performance of a quantum gate [68, 25].

A closely related definition is entanglement fidelity that is the fidelity to preserve a maximally entangled state

$$F_{\mathrm{E}}(\mathcal{E}) \coloneqq \langle\Phi^+| U^\dagger \otimes \mathbb{1}\mathcal{E} \otimes \mathcal{I}(|\Phi^+\rangle\langle\Phi^+|)U \otimes \mathbb{1} |\Phi^+\rangle . \tag{2.19}$$

Average fidelity and entanglement fidelity are related via [87]

$$\bar{F}_{\mathcal{E}} = \frac{dF_{\mathrm{E}}(\mathcal{E}) + 1}{d+1}. \tag{2.20}$$

Eq. (2.20) indicates that if we know either average fidelity or entanglement fidelity, we obtain the other.

In this section, I have reviewed basic concepts in quantum information theory including quantum states, POVM, quantum channels, and distance measures. These concepts appear in lots of parts of this thesis.

2.2 Quantum error correction

This section reviews quantum error correction (QEC) theory starting from criteria of QEC in Subsec. 2.2.1 and code distance in Subsec. 2.2.2. Then I review CSS codes in Subsec. 2.2.3 and the formalism of stabilizer code in Subsec. 2.2.4. From Subsec. 2.2.1 to Subsec. 2.2.4, I mainly follow the content in [97]. I explain basic algebraic graph theory in Subsec. 2.2.5 for the sake of the CSS code in Subsection. 4.3. Finally, I review CWS code in Subsec. 2.2.6 and quantum secret sharing in Subsec. 2.2.7 as particular quantum error-correcting codes.

2.2.1 Criteria of QEC

Suppose an orthonormal set of basis $\{|\bar{i}\rangle\}$ spans the code space $\mathscr{H}$, and Ξ is the set of Pauli operators, which the code can correct. The necessary and sufficient conditions for the code to be

enable to correct any error in Ξ is

$$\forall P_a, P_b \in \Xi, \langle \bar{i} | P_a^\dagger P_b | \bar{j} \rangle = C_{ab} \delta_{ij}, \tag{2.21}$$

where C_{ab} is a Hermitian matrix, and δ_{ij} is the Kronecker delta function.

The condition (2.21) implies two conditions. The first is

$$\text{For } i \neq j, \forall P_a, P_b \in \Xi, \langle \bar{i} | P_a^\dagger P_b | \bar{j} \rangle = 0. \tag{2.22}$$

This must be satisfied, as otherwise, the orthogonality of the codes is destroyed and hence information is damaged by errors. The second is that

$$\forall P_a, P_b \in \Xi, \langle \bar{i} | P_a^\dagger P_b | \bar{i} \rangle = C_{ab} \tag{2.23}$$

is independent of i. This must be true, because otherwise, by finding error operator P_a, we get encoded quantum information. But obtaining this unknown quantum information implies that the information has been disturbed, which is not supposed to be.

There is a special class of quantum error-correcting codes, called non-degenerate codes. An $P_a \in \Xi$ maps the code space $\mathcal{C}$ to a space $P_a\mathcal{C}$. In non-degenerate codes, all the spaces $P_a\mathcal{C}$ are orthogonal to each other. Thus, the equivalent condition to correct quantum errors in non-degenerate codes, is

$$\forall P_a, P_b \in \Xi, \langle \bar{i} | P_a^\dagger P_b | \bar{j} \rangle = \delta_{ab} \delta_{ij}. \tag{2.24}$$

The quantum error-correcting codes, which do not satisfy Eq. (2.24), are degenerate codes. In this case, the Hermitian matrix C_{ab} is not diagonal. But by applying singular value decomposition, we can find a unitary matrix U to diagonalize C_{ab}, that is $C = UDU^\dagger$, where D is a diagonal matrix. By defining

$$F_c = \sum_a U_{ca} P_a, \tag{2.25}$$

we have

$$\langle \bar{i} | F_a^\dagger F_b | \bar{j} \rangle = D_{ab} \delta_{ij}. \tag{2.26}$$

Thus, in the rotated basis $\left\{ \sum_a U_{ca} P_a^\dagger \right\}$, quantum errors can still be diagonalized.

2.2.2 Distance

We usually use three parameters $[[n,k,d]]$ to describe a quantum error-correcting code, where n is the number of physical qubits, k is the number of encoded qubits, and d is the distance of the code. To explain the code distance, let us first introduce the weight of a Pauli operator. Denote the n-qubit Pauli group as $\mathcal{G}_n$. Given a Pauli operator $g \in \mathcal{G}_n$, the weight of g is the number of nontrivial single-qubit Pauli operators, i.e., X, Y, Z, in the tensor product. For example, the weight of a three-qubit Pauli operator $X \otimes Y \otimes I$ is two.

The distance of a quantum error-correcting code is the minimum weight of a Pauli operator P_a such that

$$\langle \bar{i} | P_a | \bar{j} \rangle \neq C_a \delta_{ij}. \tag{2.27}$$

The definition of distance implies that for any Pauli operators P_a and P_b with weights $\left\lfloor \frac{d-1}{2} \right\rfloor$, the condition in Eq. (2.21) is automatically satisfied. Therefore, a quantum error-correcting code with distance d can correct any $\left\lfloor \frac{d-1}{2} \right\rfloor$-qubit quantum errors.

We have discussed the quantum errors which occur at unknown qubits. Now, we consider correcting quantum errors at t specified qubits. We call these quantum errors at specified qubits as located errors. In this case, the set of errors to be corrected, Ξ, is the set of Pauli operators, which act only nontrivially on these t qubits. Hence, $\forall P_a, P_b \in \Xi$, the weight of $P_a^\dagger P_b$ is no more than t. For a quantum code with distance $d > t$, the criteria in Eq. (2.21) is satisfied. Thus, a quantum error-correcting code with distance d can correct any $(d-1)$-qubit located error.

Another property of the quantum code with distance d is that it can detect whether any t-qubit ($t < d$) quantum error happened or not. To guarantee that a measurement can detect whether a t-qubit error P_a occurs or not, P_a should either keep the state unchanged or map the code to a state

orthogonal to the code space. That is,

$$P_a |\bar{i}\rangle = C_a |\bar{i}\rangle + |\psi_{ai}^{\perp}\rangle , \tag{2.28}$$

where $|\psi_{ai}^{\perp}\rangle$ is a state orthogonal to the code space. We find Eq (2.28) is equivalent to

$$\langle \bar{i}| P_a |\bar{j}\rangle = C_a \delta_{ij}. \tag{2.29}$$

In a quantum code with distance d, any P_a with weight less than d satisfies Eq. (2.29). Thus, a quantum error-correcting code with distance d can detect whether any $(d-1)$-qubit quantum error occurs or not.

2.2.3 Calderbank-Shor-Steane code

CSS codes is a special kind of quantum error-correcting codes utilizing the conceptions in classical linear codes. CSS codes are important because their special properties make their encoding easier than other codes. Before going into the detail of CSS codes, let us first explain binary linear codes.

A binary linear code encodes k bits into n bits. In the n-dimensional binary linear space, a k-dimensional binary subspace forms the code space. Each codeword encoding k bits is an element in the code space. Suppose $\boldsymbol{v}$ is an arbitrary k-binary vector representing the k-bit information to be encoded, the encoding process is a binary linear transformation

$$L(\boldsymbol{v}) = \boldsymbol{v}\boldsymbol{G}, \tag{2.30}$$

where $\boldsymbol{G}$ is a $k \times n$ binary matrix. The resultant $L(\boldsymbol{v})$, as an n-binary vector, is a codeword encoding $\boldsymbol{v}$.

We call $\boldsymbol{G}$ the generator matrix of this linear code. It consists of k linearly independent vectors,

i.e.,

$$\boldsymbol{G} = \begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \\ \vdots \\ \boldsymbol{u}_k \end{pmatrix}. \tag{2.31}$$

$\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_k\}$ span the k-dimensional code space.

On the other hand, any codeword $\boldsymbol{u}$ of the linear code satisfies a linear constraint

$$\boldsymbol{H}\boldsymbol{u}^\top = \boldsymbol{0}, \tag{2.32}$$

where $\boldsymbol{u}$ is an n-binary vector, $\boldsymbol{H}$ is an $(n-k) \times n$ matrix, and $\boldsymbol{0}$ is an $(n-k)$-binary vector. We call $\boldsymbol{H}$ the parity check matrix of this linear code.

The code space is the null space of the parity check matrix $\boldsymbol{H}$. From the rank-nullity theorem, we know that the row rank of matrix $\boldsymbol{H}$ is equal to $n-k$, i.e., $n-k$ rows in $\boldsymbol{H}$ are linearly independent from each other. Furthermore, from the linear constraint in Eq. (2.32), it's easy to conclude that

$$\boldsymbol{H}\boldsymbol{G}^\top = \boldsymbol{0}, \tag{2.33}$$

where $\boldsymbol{G}^\top$ is the transpose matrix of $\boldsymbol{G}$, and $\boldsymbol{0}$ is a $(n-k) \times k$ zero matrix.

An important concept in classical coding theory is the dual code. Let us denote the code with generator matrix $\boldsymbol{G}$ and parity check matrix $\boldsymbol{H}$ as $\mathcal{C}$. We know that the two matrices $\boldsymbol{H}$ and $\boldsymbol{G}$ satisfy the relation in Eq. (2.33). Take the transpose of Eq. (2.33), we get

$$\boldsymbol{G}\boldsymbol{H}^\top = \boldsymbol{0}, \tag{2.34}$$

where $\boldsymbol{0}$ is a $k \times (n-k)$ zero matrix.

Hence, if we consider $\boldsymbol{H}$ as the generator matrix of a linear code and vice versa $\boldsymbol{G}$ as the parity check matrix, then we obtain a new linear code, denoted by $\mathcal{C}^\perp$, which is called the dual code of $\mathcal{C}$.

As the code spaces of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are spanned by row vectors in $\boldsymbol{G}$ and $\boldsymbol{H}$ respectively, and $\boldsymbol{G}$ and $\boldsymbol{H}$ satisfy Eq. (2.33), the codes in $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are orthogonal with each other.

Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are two classical linear codes with $k_1 \times n$ generator matrix $\boldsymbol{G}_1$ and $k_2 \times n$ generator matrix $\boldsymbol{G}_2$. The corresponding parity check matrices are $(n-k_1)\times n$ dimensional $\boldsymbol{H}_1$ and $(n-k_2)\times n$ dimensional $\boldsymbol{H}_2$, respectively. If all the rows of $\boldsymbol{G}_2$ are in $\boldsymbol{G}_1$ or linear combinations of rows in $\boldsymbol{G}_1$, or equivalently, all the rows of $\boldsymbol{H}_1$ are in $\boldsymbol{H}_2$ or linear combinations of rows in $\boldsymbol{H}_2$, then the linear code $\mathcal{C}_2$ is a subcode of $\mathcal{C}_1$, i.e., $\mathcal{C}_2 \subseteq \mathcal{C}_1$.

As $\mathcal{C}_2 \subseteq \mathcal{C}_1$, one can obtain equivalence classes of $\mathcal{C}_2$ in $\mathcal{C}_1$. Given two codewords $u, v \in \mathcal{C}_1$, they are equivalent, i.e., $u \equiv v$, if and only if there exists a codeword $w \in \mathcal{C}_2$ such that $u = w + v$. Hence, these different equivalence classes are called the cosets of $\mathcal{C}_2$ in $\mathcal{C}_1$, the number of which equals to $2^{k_1-k_2}$.

One can construct a CSS quantum error-correcting code from these two linear classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$. Each basis element of the CSS code is associated to a coset of $\mathcal{C}_2$ in $\mathcal{C}_1$, where each basis element is an equally weighted superposition of all the codewords in the coset. That is

$$|\bar{u}\rangle := \frac{1}{\sqrt{2^{k_2}}} \sum_{w \in \mathcal{C}_2} |u + w\rangle \,. \tag{2.35}$$

In the case $w \equiv w'$, $|\bar{w}\rangle$ and $|\bar{w}'\rangle$ are the same logical qubit, i.e., $|\bar{w}\rangle = |\bar{w}'\rangle$. The dimension of the CSS code space equals to the number of cosets, $2^{k_1-k_2}$. Thus, the CSS code encodes $k_1 - k_2$ qubits into n qubits.

The first proposed CSS code is the seven-qubit Steane code [108]. It is derived from the Hamming code and its dual code. The Hamming code encodes four bits into seven bits, having the generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{2.36}$$

The generator matrix of its dual code is the parity check matrix of the Hamming code

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{2.37}$$

One can easily find that the dual code of the Hamming code is an even-weight subcode of the Hamming code. The odd-weight subcode of the Hamming code forms another coset in the Hamming code. Thus, the Steane code, developed from the Hamming code and its dual code, is

$$|\bar{0}\rangle := \frac{1}{\sqrt{8}} \sum_{v \in \text{Even}} |v\rangle, \tag{2.38}$$

$$|\bar{1}\rangle := \frac{1}{\sqrt{8}} \sum_{v \in \text{Odd}} |v\rangle, \tag{2.39}$$

where Even denotes the set of even-weight hamming codes and Odd denotes the set of odd-weight hamming codes.

This subsection introduces the CSS code and an important example, the Steane code. In the next subsection, I will introduce the general formalism of stabilizer quantum error-correcting codes and CSS code can be formulated as stabilizer code.

2.2.4 Stabilizer formalism of QEC

This subsection first introduces the Pauli group. Then I explain stabilizer codes, which are specified by Abelian subgroups of the Pauli group. The CSS code studied in the last subsection can be further formalized as a particular type of stabilizer codes. Finally, I discuss the encoding of stabilizer codes.

An n-qubit Pauli group is

$$\mathcal{G}_n := \pm\{I, X, Y, Z\}^{\otimes n}, \tag{2.40}$$

where

$$X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{and } Y \coloneqq ZX. \tag{2.41}$$

Here for the purpose of my investigation, it is enough to restrict to the real Pauli group and ignore imaginary coefficients. The Pauli group module sign is isomorphic to a cartesian product of binary vector spaces according to

$$\mathcal{I}_P : \mathcal{G}_n/\mathbb{Z}_2 \to \mathbb{Z}_2^n \times \mathbb{Z}_2^n : \bigotimes_{i=1}^{n} Z^{u_i} X^{v_i} \mapsto \begin{bmatrix} \boldsymbol{u} & \boldsymbol{v} \end{bmatrix}, \tag{2.42}$$

where

$$\boldsymbol{u} \coloneqq [u_1 \dots u_n], \ \boldsymbol{v} \coloneqq [v_1 \dots v_n]. \tag{2.43}$$

For example, in the two-qubit Pauli group, ZX is represented by binary vector $\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$, and YX is represented by $\begin{bmatrix} 1 & 0 & 1 & 1 \end{bmatrix}$. Two Pauli operators represented as binary vectors, $\begin{bmatrix} \boldsymbol{u} & \boldsymbol{v} \end{bmatrix}$ and $\begin{bmatrix} \boldsymbol{u}' & \boldsymbol{v}' \end{bmatrix}$, mutually commute if and only if

$$\boldsymbol{u} \cdot \boldsymbol{v}' + \boldsymbol{v} \cdot \boldsymbol{u}' = 0, \tag{2.44}$$

where $\cdot$ is the indefinite inner product

$$\boldsymbol{u} \cdot \boldsymbol{v} \coloneqq \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_2. \tag{2.45}$$

Otherwise, these two Pauli operators anti-commute with each other.

A stabilizer code [46] is the simultaneous eigenspace of all the elements of an Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_n$ with eigenvalue one. A generator set of $\mathcal{S}$ is a set of independent elements in $\mathcal{S}$ such that every element of $\mathcal{S}$ can be expressed as a product of the elements in this generator set. An $[[n,k,d]]$ stabilizer code has $n-k$ independent stabilizer generators, each of which can be represented by a $2n$-dimensional binary vector. The $[[n,k,d]]$ stabilizer code is characterized by an $(n-k) \times 2n$

stabilizer generator matrix, where each row represents a stabilizer generator.

The CSS code, discussed in Subsec. 2.2.3, is a stabilizer code whose stabilizer generators are either tensor products of X operators and identities, or tensor products of Z operators and identities [46]. Hence, the CSS stabilizer code is characterized by an $(n-k)\times 2n$ stabilizer generator matrix

$$\begin{bmatrix} \boldsymbol{H}_Z & \mathbf{0} \\ \mathbf{0} & \boldsymbol{H}_X \end{bmatrix}, \tag{2.46}$$

where $\boldsymbol{H}_Z$ and $\boldsymbol{H}_X$ are two matrices, and the $\mathbf{0}$s are appropriately sized zero matrices. If the CSS stabilizer is developed from the classical linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$, then $\boldsymbol{H}_Z$ in Eq. (2.46) is the parity check matrix of $\mathcal{C}_1$ and $\boldsymbol{H}_X$ in Eq. (2.46) is the generator matrix of $\mathcal{C}_2$.

Now I explain the encoding of a stabilizer code with stabilizer $\mathcal{S}$. The Pauli operators that preserve the stabilizer code space but act nontrivially on the encoded state are the logical Pauli operators on the encoded state [46]. The logical Pauli operators commute with all stabilizers in $\mathcal{S}$ but lie outside $\mathcal{S}$.

For an $[[n,1,d]]$ stabilizer code with stabilizer $\mathcal{S}$, we denote $\bar{Z}$ and $\bar{X}$ as the logical Z and logical X operators on an n-qubit encoded state. Suppose $|\psi_0\rangle$ is an eigenstate

$$\bar{Z}\,|\psi_0\rangle = |\psi_0\rangle\,, \tag{2.47}$$

and

$$\{M_i\}_{i=1}^{n-1}$$

are $n-1$ independent stabilizer generators of $\mathcal{S}$. The encoded logical states are [46]

$$|\bar{0}\rangle := \frac{1}{\sqrt{2^{n-1}}}\prod_{i=1}^{n-1}(I+M_i)\,|\psi_0\rangle\,, \tag{2.48}$$

and

$$|\bar{1}\rangle := \frac{\bar{X}}{\sqrt{2^{n-1}}}\prod_{i=1}^{n-1}(I+M_i)\,|\psi_0\rangle = \frac{1}{\sqrt{2^{n-1}}}\prod_{i=1}^{n-1}(I+M_i)\bar{X}\,|\psi_0\rangle\,. \tag{2.49}$$

Equations (2.48) and (2.49) indicate how to encode one qubit by a stabilizer code.

Suppose $|\psi_0\rangle = |\mathbf{0}\rangle$ is an eigenstate of $\bar{Z}$ with eigenvalue one. To encode $|\psi\rangle$ by a CSS code, using Eqs. (2.48) and (2.49), and the fact that Z-type stabilizers act trivially on $|\psi_0\rangle$, one only needs to apply X-type stabilizer operations. Furthermore, $I + M_i$ can be implemented by the combination of a Hadamard gate and CNOT gates, if M_i is a X-type stabilizer. Hence, by following this method, one can obtain the encoding circuit of the Steane code.

2.2.5 Graphs and linear algebra

In this subsection, we begin by defining graphs and the binary linear space. After explaining these two concepts, we describe an isomorphism from sets of edges of an n-vertex graph to binary vectors with length $\binom{n}{2}$ [35]. Our approach is inspired by homology theory to construct quantum error-correcting codes [54, 19]. Finally, we present examples of triangle graphs and star graphs.

A graph [35]

$$\mathscr{G} := (V, E) \tag{2.50}$$

comprises a set of vertices V and a set of edges

$$E \subseteq V \times V. \tag{2.51}$$

One example of a graph is the n-vertex complete graph, K_n.

To explain the binary linear space, we introduce $GF(2)$, which is the smallest finite field containing two elements $\{0,1\}$, together with addition and multiplication operations [73]. The linear space [102] over field $GF(2)$, denoted by $\mathbb{Z}_2^m$, is a set $\{0,1\}^m$, together with vector addition,

$$+ : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m, \tag{2.52}$$

and scalar multiplication,[2]

$$\cdot : GF(2) \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m. \tag{2.53}$$

Next we explain the relation between an edge set E of a graph $\mathscr{G}$ and a binary vector with length $\binom{|V|}{2}$, where $|V|$ is the cardinality of V.

Given $K_n = (V_K, E_K)$, the power set of E_K, which is the set of all the subsets of E_K and denoted 2^{E_K}, forms a binary linear space $\mathscr{E}$ [35]. For $\mathscr{U}$, $\mathscr{U}' \in 2^{E_K}$, the addition of $\mathscr{U}$ and $\mathscr{U}'$ amounts to the symmetric difference of $\mathscr{U}$ and $\mathscr{U}'$,

$$\mathscr{U} + \mathscr{U}' := \left(\mathscr{U} \cup \mathscr{U}'\right) \setminus \left(\mathscr{U} \cap \mathscr{U}'\right). \tag{2.54}$$

The empty set is the zero element and

$$\forall\, \mathscr{U} \in 2^{E_K},\ -\mathscr{U} := \mathscr{U}. \tag{2.55}$$

For v_i and v_j, an edge e_{ij} is a unit vector in $\mathscr{E}$, and $e_{ji} = e_{ij}$ because we are dealing with undirected graphs. The set of edges

$$\left\{e_{ij}\right\}_{1 \le i < j \le n} \tag{2.56}$$

forms an orthonormal basis of $\mathscr{E}$. As $\binom{n}{2}$ edges exist in K_n,

$$\dim \mathscr{E} = \binom{n}{2}. \tag{2.57}$$

Now we show that $\mathscr{E}$ is isomorphic to $\mathbb{Z}_2^{\binom{n}{2}}$ [35]. Given any $\mathscr{U} \in \mathscr{E}$, an isomorphism is

$$\mathcal{I}_{\mathscr{G}} : \mathscr{E} \to \mathbb{Z}_2^{\binom{n}{2}} : \mathscr{U} \mapsto \boldsymbol{u} = \left[u_1 \ldots u_{\binom{n}{2}}\right], \tag{2.58}$$

[2]Note we use $\cdot$ for the scalar multiplication only in Eq. (2.53) and Table 2.1. After this subsection, we use $\cdot$ only for inner product.

where

$$\{u_i\}_{i=1}^{\binom{n}{2}}$$

are the coefficients of $\mathscr{U}$ with respect to the basis in Eq. (2.56). The isomorphic mappings of the vector addition and the scalar multiplication are shown in Table 2.1.

Here we introduce two types of $\binom{n}{2}$-dimensional binary vectors and two linear subspaces spanned by these two types of vectors as examples of the isomorphism (2.58). These examples are used later for the construction of the CSS stabilizer code in Sec. 4.3. The two types of vectors in $\mathbb{Z}_2^{\binom{n}{2}}$ are

$$\boldsymbol{T}_{ijk} \coloneqq \boldsymbol{e}_{ij} + \boldsymbol{e}_{jk} + \boldsymbol{e}_{ki},\ \boldsymbol{A}_j \coloneqq \sum_{1 \le l \le n, l \neq j} \boldsymbol{e}_{lj}, \tag{2.59}$$

where $\boldsymbol{e}_{ij}$ is the unit vector $\mathcal{I}_{\mathscr{G}}(e_{ij})$. From the isomorphism (2.58), these two types of vectors can be represented by two different types of graphs. $\boldsymbol{T}_{ijk}$ is represented by a triangle graph connecting vertices

$$\{v_i, v_j, v_k\}, \tag{2.60}$$

and $\boldsymbol{A}_j$ is represented by a star graph with vertex v_j connected to every other vertex.

We construct the linear space

$$\mathcal{C}_1 \coloneqq \operatorname{span}\{\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_{n-1}\} \tag{2.61}$$

spanned by $n-1$ linearly independent $\{\boldsymbol{A}_j\}$, and the orthogonal linear space

$$\mathcal{C}_1^{\perp} \coloneqq \operatorname{span}\{\boldsymbol{T}_{123}, \boldsymbol{T}_{124}, \ldots, \boldsymbol{T}_{12n}, \boldsymbol{T}_{134}, \ldots, \boldsymbol{T}_{1n-1n}\} \tag{2.62}$$

	$\mathscr{E}$	$\mathbb{Z}_2^{\binom{n}{2}}$
$+$	$(\mathscr{U} \cup \mathscr{U}') \setminus (\mathscr{U} \cap \mathscr{U}')$	$\boldsymbol{u} + \boldsymbol{u}'$
$\cdot$	$0\mathscr{U} = \emptyset$, $1\mathscr{U} = \mathscr{U}$	$0\boldsymbol{u} = \boldsymbol{0}$, $1\boldsymbol{u} = \boldsymbol{u}$

Table 2.1: The mapping of the vector addition and the scalar multiplication on $\mathscr{E}$ to those operations on $\mathbb{Z}_2^{\binom{n}{2}}$

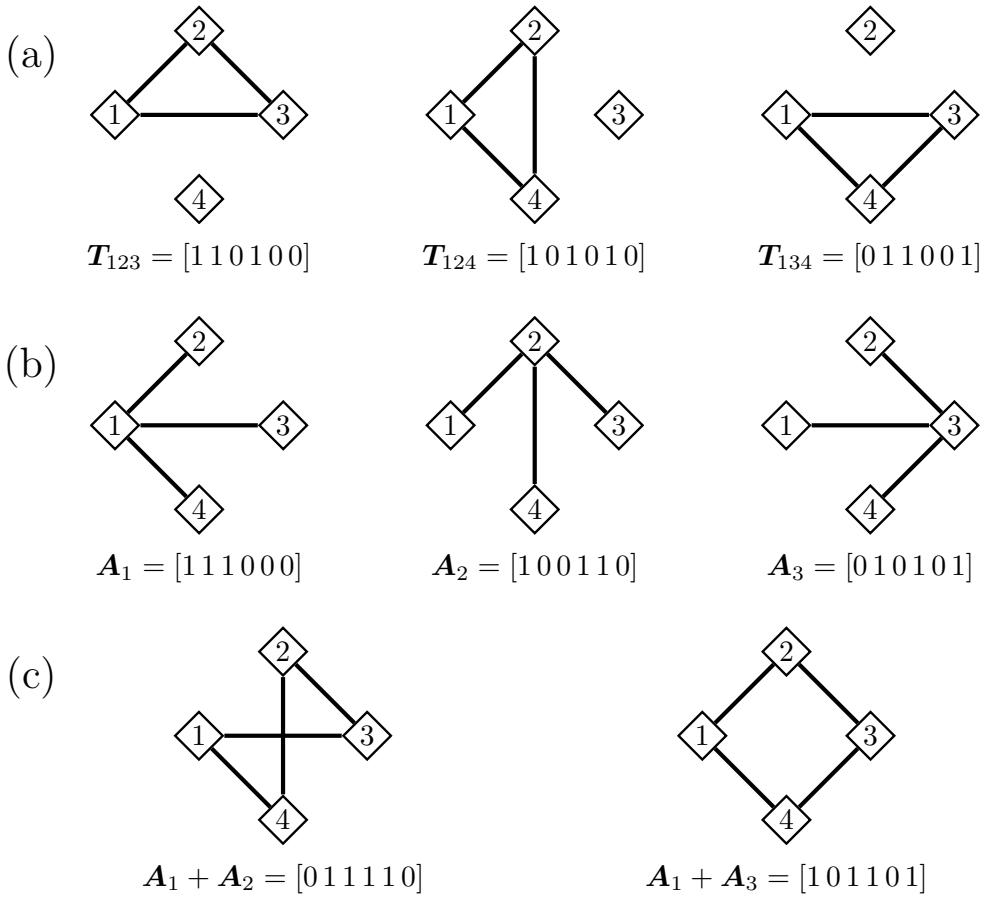


Figure 2.1: For $n = 4$, (a) the triangle graphs representing $\boldsymbol{T}_{1jk}$ $(2 \leq j < k \leq 4)$, (b) the star graphs representing $\boldsymbol{A}_l$ $(1 \leq l \leq 3)$ and (c) the graphs representing $\boldsymbol{A}_1 + \boldsymbol{A}_m$ $(2 \leq m \leq 3)$.

spanned by $\binom{n-1}{2}$ linearly independent $\{\boldsymbol{T}_{ijk}\}$. The elements in $\mathcal{C}_1^{\perp}$ are represented by Eulerian cycles (graph cycles that use each edge exactly once) [35]. Meanwhile, $\mathcal{C}_1$ comprises vectors orthogonal to all vectors in $\mathcal{C}_1^{\perp}$ [35], i.e.,

$$\mathcal{C}_1 = \left(\mathcal{C}_1^{\perp}\right)^{\perp}. \tag{2.63}$$

We introduce an $(n-2)$-dimensional linear subspace of $\mathcal{C}_1$

$$\mathcal{C}_2 \coloneqq \operatorname{span}\{\boldsymbol{A}_1 + \boldsymbol{A}_2, \boldsymbol{A}_1 + \boldsymbol{A}_3 \ldots, \boldsymbol{A}_1 + \boldsymbol{A}_{n-1}\} \subset \mathcal{C}_1. \tag{2.64}$$

$\mathcal{C}_2$ together with $\mathcal{C}_1$ specifies the CSS code for summoning in Subsec. 4.3. Figure 2.1(a), (b) and (c) depict the graphs representing bases of linear spaces $\mathcal{C}_1^{\perp}$, $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively for $n = 4$.

This subsection has shown that the power set of the edge set of an n-vertex complete graph forms a binary linear space, isomorphic to $\mathbb{Z}_2^{\binom{n}{2}}$. Hence, we have constructed a graph representation of any $\binom{n}{2}$-binary vector. The examples given in this subsection are useful to construct the CSS code for quantum summoning.

2.2.6 CWS code

An $((n,k))$ CWS code [30] encodes a k-dimensional Hilbert space to n qubits. This CWS code is specified by a word stabilizer, which is a 2^n-element Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_n$, and a set of k word operators, which are n-qubit Pauli operators

$$\{P_l\}_{l=1}^{k}.$$

The word stabilizer $\mathcal{S}$ specifies a unique $|\psi_{\mathcal{S}}\rangle$ such that $\forall M \in \mathcal{S}$,

$$M|\psi_{\mathcal{S}}\rangle = |\psi_{\mathcal{S}}\rangle. \tag{2.65}$$

The CWS code is spanned by the basis

$$\{|w_l\rangle \coloneqq P_l\,|\psi_{\mathcal{S}}\rangle\}_{l=1}^{k}. \tag{2.66}$$

Under local Clifford operations, any CWS code is equivalent to its standard form [30], whose word stabilizer is a graph-state stabilizer [100], and whose word operators contain only Z operators and identities. Thus, the stabilized state $|\psi_{\mathcal{S}}\rangle$ of a CWS code in its standard form is a graph state. Given a graph $\mathscr{G} = (V, E)$, the associated graph state is [100]

$$|\mathscr{G}\rangle = \prod_{e_{ij}\in E} \mathrm{CZ}_{e_{ij}} \mathrm{H}^{\otimes|V|}\,|0\rangle^{|V|}, \tag{2.67}$$

where $\mathrm{CZ}_{e_{ij}}$ is the controlled-Z gate with control qubit i and target qubit j, and H is the Hadamard gate.

CWS code is a non-stabilizer code and has been utilized to summon qubits [52]. I further explain how a CWS code is used for quantum summoning in Subsec. 4.5.

2.2.7 Quantum secret sharing

Secret sharing [106, 16] is an important cryptography protocol which has applications in electronic voting, electronic shopping and so on. Its quantum version [56, 27], i.e., QSS, can be divided, according to the types of the secret and the communication channels, into three different types [83]: classical-classical, classical-quantum and quantum-quantum. In this thesis, quantum secret sharing (QSS) refers only to the QQ QSS, where the secret is quantum information and the communication channels are all quantum channels.

In a secret sharing protocol, there is a dealer and multiple players. The dealer encodes a secret into multiple shares and distribute these shares to all the players. The combination of players, who lie in the access structure, are authorized to decode the secret. Whereas the combination of players in the forbidden structure are denied, to obtain any information about the secret. Any

subset of players is either an authorized set or a forbidden set. No subset of players can obtain partial information about the secret.

Although QSS is defined differently from QEC, it has a close relation with QEC. Every QSS code can be considered as a quantum error-correcting code, which can correct erasure errors. But not every quantum error-correcting code is a QSS code. In general quantum error-correcting codes, there exists a subset of physical qubits, which contains partial information of the encoded quantum state.

An important kind of QSS protocol is a (k,n)-threshold QSS protocol, where $k,n \in \mathbb{N}$ and $k \leq n$. The dealer encodes a secret into n shares. Only sets of at least k players are authorized to decode the quantum secret. Any set of less than k players cannot get any information about the quantum secret.

From the no-cloning theorem, it's obvious that $n \leq 2k-1$. Any (k,n)-threshold QSS code can be easily obtained from a $(k,2k-1)$-threshold QSS code. Any $(k,2k-1)$-threshold QSS code is a $[[2k-1,1,k]]$ quantum error-correcting code. In qubit case, k is at least three, i.e., the smallest code of this type of quantum codes is the $[[5,1,3]]$ code.

This section has reviewed the criteria of quantum errors to be corrected by QEC code and the distance of a quantum code. I have explained how to obtain a CSS code from two classical linear codes and the formalism of stabilizer codes. I have explained the connection between graph theory and linear algebra for the sake of the CSS code for quantum summoning. This section also has reviewed CWS codes, which are non-stabilizer codes and QSS as a particular QEC code.

2.3 Relativistic quantum information

This section reviews relativistic quantum information theory. I first review Minkowski spacetime in Subsec. 2.3.1 and Rindler coordinates in Subsec. 2.3.2. In Subsecs. 2.3.3 and 2.3.4, I review quantization of scalar field, Fock space and Bogoliubov transformation. In Subsec. 2.3.5, I explain the evolution of a scalar field inside a moving cavity in non-inertial frames, which is further studied

in Sec. 5.1.

2.3.1 Minkowski spacetime

This section reviews Minkowski spacetime and the basic concepts in special relativity, which provide important tools for later investigation. Spacetime is a differential manifold $\mathcal{M}$, at each point of which is locally isomorphic to an Euclidean space $\mathbb{R}^4$. We can define a coordinate function which maps each point $p \in \mathcal{M}$ to $\mathbb{R}^4$. For instance, in $(3+1)$-dimensional flat spacetime, i.e., Minkowski spacetime, the coordinate function is (t,x,y,z), where t is the time, and (x,y,z) are the spatial coordinates. The coordinates for two inertial observers are connected by a Lorentz transformation. Throughout this thesis, we use $c = \hbar = 1$.

Each point in spacetime is equipped with a metric tensor. In $(3+1)$-dimensional Minkowski spacetime, the metric tensor at every point is

$$g = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.68}$$

The metric tensor is Lorentz invariant, so also called Lorentz metric tensor. The metric tensor g_{ab} connects a covariant vector χ_a, which transforms in the same way as the transformation of coordinates, with the contravariant vector χ^a, which transforms in the opposite way as the transformation of coordinates,

$$\chi_a = g_{ab}\chi^b. \tag{2.69}$$

The inverse of the metric tensor g_{ab} is g^{ab}, i.e.,

$$g_{ab}g^{bc} = \delta_a^c. \tag{2.70}$$

Given a vector $v = v^a$ in spacetime, the norm of v is

$$(v,v) = v^a v_a = g_{ab} v^a v^b. \tag{2.71}$$

This norm is not positive semi-definite. If $(v,v) > 0$, then v is a space-like vector; if $(v,v) < 0$, then v is a time-like vector; and if $(v,v) = 0$, then v is a light-like vector. The metric tensor gives the infinitesimal distance between two neighboring points χ and $\chi + d\chi$, named line element,

$$\mathrm{d}s^2 = g_{ab}(\chi)\mathrm{d}\chi^a \mathrm{d}\chi^b. \tag{2.72}$$

This subsection presents basic concepts on Minkowski spacetime. In the next subsection, I explain Rindler coordinate that is the proper coordinate for a uniformly accelerating observer.

2.3.2 Rindler coordinates

This subsection discusses the proper coordinate for a uniformly accelerating observer, called Rindler coordinate. Besides coordinate system, I review proper time and proper length in Rindler coordinate. This subsection also discusses the four spacetime regions in a Rindler coordinate system.

The proper coordinates of an observer accelerating with a constant acceleration is called Rindler coordinate. The correspondence between the $(1+1)$-dimensional Minkowski coordinates (t,x) and the $(1+1)$-dimensional Rindler coordinate (χ,η) in region I is

$$x = \mathrm{e}^{\chi}\cosh\eta, \quad t = \mathrm{e}^{\chi}\sinh\eta, \tag{2.73}$$

where $\chi > 0$, and $\eta \in \mathbb{R}$. The metric tensor at each point (χ,η) is

$$g = \begin{pmatrix} -\mathrm{e}^{2\chi} & 0 \\ 0 & \mathrm{e}^{2\chi} \end{pmatrix} \tag{2.74}$$

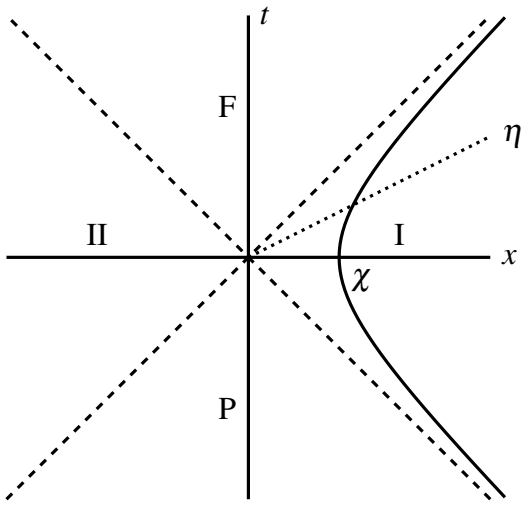


Figure 2.2: The figure shows a Rindler coordinate. x is position and t is time in Minkowski space-time. The hyperbolic curve with χ =constant is the trajectory of a uniformly accelerating observer. The line with η =constant is the simultaneity plane for the uniformly accelerating observer. The entire space is split into four regions: I, II, F, and P. The observer moves only inside region I.

Hence, the line element is

$$\mathrm{d}s^2 = \mathrm{e}^{2\chi}\left(-\mathrm{d}\eta^2 + \mathrm{d}\chi^2\right). \tag{2.75}$$

We can see that the light speed in Rindler coordinates is still one.

Then let us see the accelerated motion of an observer moving along a time-like curve with constant χ. Along a curve with constant χ, the proper time is

$$\tau = \int \sqrt{-\mathrm{d}s^2} = \int \mathrm{d}\eta \mathrm{e}^{\chi} = \eta \mathrm{e}^{\chi}. \tag{2.76}$$

The proper acceleration of an observer, moving along a curve with constant χ, is a constant,

$$a = \mathrm{e}^{-\chi}. \tag{2.77}$$

For an observer accelerating with a constant acceleration, the simultaneity plane is the curve

with constant η. The proper length along the curve with constant η is

$$l = \int \sqrt{\mathrm{d}s^2} = \int \mathrm{d}\chi \mathrm{e}^{\chi} = \mathrm{e}^{\chi}. \tag{2.78}$$

Thus, if two point-like objects move with different but constant accelerations, the proper length between these two objects, in the perspective of any constant accelerating observer, is a constant.

The Rindler coordinate splits the whole spacetime into four regions: I, II, F and P. The coordinate systems in region II can be obtained by flipping the signs in Eq. (2.73). A uniformly accelerating observer, called Rob, follows a trajectory with constant χ. Rob's trajectory asymptotically approaches the light-like line $x = t$, with speed asymptotically goes to the speed of light, and $x = t$ forms an event horizon for Rob. Rob can neither receive information from nor send information to region II. Regions I and II are causally disconnected from each other.

2.3.3 Quantization of scalar field

This subsection reviews Klein-Gordon equation and quantization of a real scalar massless field. A real scalar field, i.e., the Klein-Gordon field satisfying the Klein-Gordon equation,

$$\left(\Box - m^2\right)\phi = 0, \tag{2.79}$$

where $\Box = \partial_\mu \partial^\mu$ and $m = 0$ if it is a massless field. The massless Klein-Gordon equation is just a wave equation

$$\left(\partial_t^2 - \partial_x^2\right)\phi = 0. \tag{2.80}$$

By noting the momentum

$$\boldsymbol{p} = (\partial_t, \partial_x) = (\omega, k), \tag{2.81}$$

where ω is frequency and k is wave number. Eq. (2.80) implies that

$$\omega = \pm|k|. \tag{2.82}$$

In another word, Klein-Gordon equation admits both positive-frequency and negative-frequency solutions. For an inertial observer, the positive frequency solutions are

$$\partial_t \phi_k = -\mathrm{i}\omega_k \phi_k, \tag{2.83}$$

where $\omega = |k|$, while negative frequency solutions are

$$\partial_t \phi_k^* = \mathrm{i}\omega_k \phi_k^*. \tag{2.84}$$

An orthonormal set of solutions can be chosen with respect to the Lorentz-invariant pseudo inner product

$$(\phi_1, \phi_2) = -\mathrm{i}\int_\Sigma \mathrm{d}x \left(\phi_1 \partial_t \phi_2^* - \phi_2^* \partial_t \phi_1\right), \tag{2.85}$$

where Σ is a space-like separated hypersurface. By using the fact that current

$$j_\mu = \phi \partial_\mu \phi^* - \phi^* \partial_\mu \phi \tag{2.86}$$

satisfies the conservation law

$$\partial_\mu j^\mu = 0, \tag{2.87}$$

and Gauss's theorem, we can get that the pseudo inner product in Eq. (2.85) is independent of the hypersurface we choose. However, j_0 can be negative, implying that it cannot be interpreted as a probability density. The pseudo inner product in (2.85) is not positive semidefinite, but only positive semidefinite for positive frequency solutions. We have

$$(\phi_k, \phi_{k'}) = -(\phi_k^*, \phi_{k'}^*) = \delta_{kk'}, \quad (\phi_k, \phi_{k'}^*) = 0. \tag{2.88}$$

The field Φ is a linear combination of positive frequency solutions ϕ_k and negative frequency

solutions ϕ_k^*

$$\Phi = \sum_k \left(\alpha_k \phi_k + \alpha_k^* \phi_k^*\right), \tag{2.89}$$

where α and α^* are complex coefficients. To quantize the massless scalar field, the coefficients α and α^* are replaced by annihilation operator $\hat{a}$ and creation operator $\hat{a}^\dagger$; hence, Φ becomes a field operator

$$\hat{\Phi} = \sum_k \left(\hat{a}_k \phi_k + \hat{a}_k^\dagger \phi_k^*\right). \tag{2.90}$$

where the annihilation and creation operators satisfy the commutation relations

$$\begin{aligned} [\hat{a}_k, \hat{a}_{k'}] &= \left[\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger\right] = 0 \\ \left[\hat{a}_k, \hat{a}_{k'}^\dagger\right] &= \delta_{k,k'} \mathbb{1}. \end{aligned} \tag{2.91}$$

In curved spacetime, the operator $\Box$ is [15]

$$\Box\phi = \frac{1}{\sqrt{-\det\left(g^{ab}\right)}} \partial_\mu \left(\sqrt{-\det\left(g^{ab}\right)} g^{\mu\nu} \partial_\nu \phi\right). \tag{2.92}$$

Using Eq. (2.74), we know that in Rindler coordinates, the Klein-Gordon equation becomes

$$\left(\partial_\eta^2 - \partial_\chi^2\right)\phi = 0. \tag{2.93}$$

For an observer accelerating with a constant acceleration, the positive and negative frequency modes are

$$\partial_\eta \phi_k = -\mathrm{i}\omega\phi_k, \tag{2.94}$$

$$\partial_\eta \phi_k^* = \mathrm{i}\omega\phi_k^*, \tag{2.95}$$

respectively. Thus, the splitting of positive frequency and negative frequency solutions to the Klein-Gordon equation is not unique, but depends on the movement trajectory of the observer.

This subsection reviews Klein-Gordon equation, which admit both positive-frequency and negative-frequency solutions. For different observers, the splitting of positive- and negative-frequency solutions can be different. Next subsection explains the Fock space established by particles of the scalar field and the transformation between two different sets of solutions to field equation.

2.3.4 Fock space and Bogoliubov transformation

This subsection explains the concept of Fock space and Bogoliubov transformations between inequivalent Fock spaces. Fock space and Bogoliubov transformations are not only regarding to quantized scalar field, but also employed for quantized electromagnetic field later in Sec. 2.4.

An annihilation operator $\hat{a}_k$ annihilates a photon in state ϕ_k, whereas a creation operator $\hat{a}_k^\dagger$ creates a photon in state ϕ_k. To construct the whole Hilbert space, we start from the vacuum state $|0\rangle_{\mathscr{F}}$ that is

$$\forall k, \quad \hat{a}_k |0\rangle_{\mathscr{F}} = 0. \tag{2.96}$$

By applying a linear combination of creation operators, we get a single-boson state

$$|\psi\rangle = \sum_k \gamma_k \hat{a}_k^\dagger |0\rangle_{\mathscr{F}}, \tag{2.97}$$

where $\sum_k |\gamma_k|^2 = 1$. Similarly, we can get a two-boson state by applying creation operators on a single-boson state. In such a way, any n-boson state can be obtained. Hence, the bosonic Fock space is

$$\mathbb{C} \oplus \mathscr{H} \oplus S(\mathscr{H} \otimes \mathscr{H}) \oplus S(\mathscr{H} \otimes \mathscr{H} \otimes \mathscr{H}) \oplus \ldots, \tag{2.98}$$

where $\mathscr{H}$ is the Hilbert space spanned by all the single-boson states, and S is a symmetrization operator on a tensor product of $\mathscr{H}$s.

As claimed in Subsec. 2.3.3, the choice of classifying positive and negative frequency solutions is not unique. For an inertial observer, the positive and negative frequency modes are denoted by ϕ_k and ϕ_k^*. For a non-inertial observer (e.g., Rindler observer), the positive and negative frequency

modes are denoted by $\tilde{\phi}_k$ and $\tilde{\phi}_k^*$. These two different classifications of positive and negative frequency modes span the same field,

$$\hat{\Phi} = \sum_k \left(\hat{a}_k \phi_k + \hat{a}_k^\dagger \phi_k^* \right) = \sum_k \left(\hat{\tilde{a}}_k \tilde{\phi}_k + \hat{\tilde{a}}_k^\dagger \tilde{\phi}_k^* \right) \tag{2.99}$$

Hence, there is a transformation, called Bogoliubov transformation, connecting these two classifications, i.e.,

$$\tilde{\phi}_k = \sum_{k'} \alpha_{k,k'} \phi_{k'} + \beta_{k,k'} \phi_{k'}^*, \tag{2.100}$$

where $\alpha_{k,k'}, \beta_{k,k'} \in \mathbb{C}$. From Eq. (2.88), we get

$$\begin{aligned} \alpha_{k,k'} &= \left(\tilde{\phi}_k, \phi_{k'} \right), \text{ and} \\ \beta_{k,k'} &= -\left(\tilde{\phi}_k, \phi_{k'}^* \right). \end{aligned} \tag{2.101}$$

The corresponding transformation on annihilation and creation operators is

$$\hat{\tilde{a}}_k = \sum_{k'} \alpha_{kk'}^* \hat{a}_{k'} - \beta_{kk'}^* \hat{a}_{k'}^\dagger, \tag{2.102}$$

$$\hat{\tilde{a}}_k^\dagger = \sum_{k'} \alpha_{kk'} \hat{a}_{k'}^\dagger - \beta_{kk'} \hat{a}_{k'}. \tag{2.103}$$

As the new set of annihilation and creation operators should still satisfy the anti-commutation relations, the Bogoliubov transformation coefficients must satisfy

$$\sum_l \alpha_{kl}^* \alpha_{k'l} - \beta_{kl}^* \beta_{k'l} = \delta_{kk'}, \tag{2.104}$$

$$\sum_l \alpha_{kl} \beta_{k'l} - \beta_{kl} \alpha_{k'l} = 0. \tag{2.105}$$

A general Bogoliubov transformation preserves the pseudo inner product (2.85), but does not preserve the number of particles. A Bogoliubov transformation with at least one $\beta_{k,k'} \neq 0$ makes annihilation operators become linear transformations of both annihilation and creation operators.

As vacuum state is annihilated by any annihilation operator, a vacuum state, after such a Bogoliubov transformation, is no longer a vacuum state; hence, the Fock space after Bogoliubov transformation is no longer the original Fock space. Mathematically, Bogoliubov transformation is a linear transformation between two different representations of canonical commutation relations in Eq. (2.91). Specifically, Unruh effect [33, 114] tells us that the vacuum state in an inertial frame becomes a thermal state in Rindler coordinates.

I have explained that Bogoliubov transformation can yield inequivalent Fock spaces. Essentially, there can be two inequivalent vacuum states for two different observers. In the next subsection, I present a physical model utilizing Bogoliubov transformation to study the evolution of quantum information localized in a cavity moving non-inertially.

2.3.5 Scalar field inside a moving cavity in non-inertial frame

This section reviews the relativistic effects on the dynamics of a scalar field restricted inside a rigid cavity moving in space [21, 42, 43]. We investigate the trajectory shown in Fig. 2.3, where a cavity is initially in an inertial frame, starts accelerating uniformly, and goes into another initial frame after a certain time. The sudden change of the acceleration of the cavity alters the frequency concerning a comoving observer; hence, the number of particles does not remain constant during the sudden change of the acceleration. As this trajectory of cavity forms a basic building block (BBB) for any arbitrary trajectory in spacetime, the results in this section paves the way for us to investigate relativistic effects involving general motion trajectories.

Suppose the proper length of the cavity is L. When $t < 0$, the left mirror is at the position x_l and the right mirror is at the position $x_r = x_l + L$. When $t = 0$, the cavity starts accelerating. The proper acceleration of the left mirror is $a_l = \frac{1}{x_l}$ and the proper acceleration of the right mirror is $\frac{1}{x_r}$; hence, the proper distance between two mirrors, for an accelerating observer inside the cavity during acceleration, is still L.

Suppose the two mirrors of the cavity are perfectly reflecting; hence, the values of the scalar field at two boundaries are zero. By solving the Klein-Gordon equation with these boundary con-

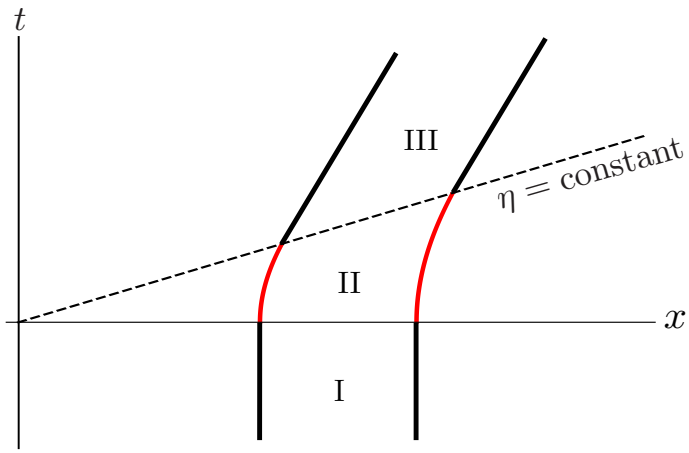


Figure 2.3: BBB for an arbitrary trajectory. The world lines of the left and right walls of the cavity are depicted. In region I, the cavity is inertial. In region II, the two walls of the cavity are accelerating with two different proper accelerations until the Rindler coordinate time $\eta = \frac{\tau}{a}$, where τ and a are proper time and acceleration respectively. In region III, the cavities have stopped accelerating and back in the inertial frame again. The hyperbolas (red curves) represent the trajectories of the cavity walls moving with constant proper acceleration, and the (black) straight lines correspond to the trajectories of the walls while they move inertially.

ditions in Minkowski spacetime, we get

$$\phi_n(t,x) = \frac{1}{\sqrt{n\pi}} \sin\left(\frac{\pi n}{L}(x-x_l)\right) \mathrm{e}^{-\mathrm{i}\frac{\pi n}{L}t}, \tag{2.106}$$

where $n \in \mathbb{N}^+$ and $x_l \leq x \leq x_l + L$. Analogously, we can get the solutions to Klein-Gordon equation in Rindler coordinates,

$$\tilde{\phi}_m(\eta,\chi) = \frac{1}{\sqrt{k\pi}} \sin\left(\frac{\pi m}{L'}(\chi-\chi_l)\right) \mathrm{e}^{-\mathrm{i}\frac{\pi m}{L'}\eta}, \tag{2.107}$$

where $\chi_l = \ln x_l$ is the position of the left mirror in Rindler coordinates,

$$L' = \ln x_r - \ln x_l = \ln \frac{x_l + L}{x_l} \tag{2.108}$$

is the Rindler coordinate length of the cavity and $\chi_l \leq \chi \leq \chi_l + L'$.

The Bogoliubov coefficients from region I to region II are conceptually determined by Eqs. (2.101).

However, those coefficients cannot be written in terms of elementary functions [43]. To circumvent this problem, ref. [43] introduces a dimensionless parameter

$$h = a_{\mathrm{c}} L \left(\text{or } \frac{a_{\mathrm{c}} L}{c^2} \right), \tag{2.109}$$

where

$$a_{\mathrm{c}} = \frac{2}{x_l + x_r} = \frac{2}{2x_l + L}, \tag{2.110}$$

is the acceleration of an accelerating observer in the center of the cavity.

We consider the case that $a_{\mathrm{c}} \ll \frac{c^2}{L}$. Then the Bogoliubov coefficients in Eqs. (2.101) are calculated perturbatively in h, i.e., the Taylor-Maclaurin expansions around $h = 0$,

$$ {}_0\alpha_{nm} = {}_0\alpha^{(0)}_{nm} + {}_0\alpha^{(1)}_{nm} h + {}_0\alpha^{(2)}_{nm} h^2 + O(h^3), \tag{2.111}$$

$$ {}_0\beta_{nm} = {}_0\beta^{(1)}_{nm} h + {}_0\beta^{(2)}_{nm} h^2 + O(h^3). \tag{2.112}$$

In the basis of $\{\phi_n, \phi_n^*\}_{n\in\mathbb{N}^+}$, the Bogoliubov transformation from region I to region II is written in terms of a Bogoliubov coefficient matrix

$$\mathcal{B} = \begin{bmatrix} {}_0\boldsymbol{\alpha} & -{}_0\boldsymbol{\beta} \\ -{}_0\boldsymbol{\beta}^* & {}_0\boldsymbol{\alpha}^* \end{bmatrix}, \tag{2.113}$$

where ${}_0\boldsymbol{\alpha} = \left({}_0\alpha_{nm}\right)_{n,m\in\mathbb{N}^+}$ and ${}_0\boldsymbol{\beta} = \left({}_0\beta_{nm}\right)_{n,m\in\mathbb{N}^+}$. Each entry in matrix $\mathcal{B}$ is a perturbative expansion in terms of h, as shown in Eqs. (2.111) and (2.112).

Within region II, there is only free evolution, i.e., phase rotations. To express phase rotation in terms of proper time in region II, we calculate proper frequency and see how proper frequency changes perturbatively in h. From Eq. (2.76), we know that the ratio between proper time and Rindler coordinate time is

$$\frac{\tau}{\eta} = e^{\chi}. \tag{2.114}$$

Using Eq. (2.77), the ratio between the proper frequency, $\tilde{\omega}$, for the observer in the middle of the cavity and the Rindler coordinate frequency, $\omega' = \frac{k\pi}{L'}$, equals the proper acceleration of the observer, i.e.,

$$\frac{\tilde{\omega}}{\omega'} = a_{\mathrm{c}}. \tag{2.115}$$

Using the definitions of h and ω', we get

$$\tilde{\omega} = \frac{k\pi h}{LL'}. \tag{2.116}$$

Below, we substitute L' as a function of L and h.

From Eq. (2.110), we know that

$$x_l = \frac{1}{a_c} - \frac{L}{2}. \tag{2.117}$$

Plugging this into Eq. (2.108), we obtain

$$\tilde{\omega} = \frac{k\pi h}{2L \operatorname{arctanh} \frac{h}{2}} = \omega \left(1 + O\left(h^2\right)\right), \tag{2.118}$$

where $\omega = \frac{k\pi}{L}$. Thus, the Bogoliubov transformation in region II is

$$\begin{bmatrix} \mathcal{R}(\tau) & \mathbf{0} \\ \mathbf{0} & \mathcal{R}(\tau)^* \end{bmatrix}, \tag{2.119}$$

where $\mathcal{R}(\tau) = \operatorname{diag}\left\{\mathrm{e}^{i\tilde{\omega}\tau} | k \in \mathbb{N}^+\right\}$.

As the Klein-Gordon equation is a Lorentz invariant equation, the solution in region III in terms of (t,x) is identical to Eq. (2.106) except that x_l is different. Thus, the Bogoliubov coefficients from region II to region III is obtained by just switching the two-mode functions in the Klein-Gordon

inner product of the Bogoliubov coefficients from region I to region II. Using the fact that

$$(\tilde{\phi}_m, \phi_n) = (\phi_n, \tilde{\phi}_m)^*, \tag{2.120}$$

$$(\tilde{\phi}_m, \phi_n^*) = -(\phi_n, \tilde{\phi}_m^*), \tag{2.121}$$

and Eq. (2.113), we know the Bogoliubov transformation matrix from region II to region III is

$$\begin{bmatrix} {}_0\boldsymbol{\alpha}^\dagger & {}_0\boldsymbol{\beta}^\top \\ {}_0\boldsymbol{\beta}^\dagger & {}_0\boldsymbol{\alpha}^\top \end{bmatrix}. \tag{2.122}$$

Eqs. (2.104) and (2.105) imply that the above Bogoliubov transformation matrix is the inverse matrix of $\mathcal{B}$ in (2.113), i.e.,

$$\mathcal{B}^{-1} = \begin{bmatrix} {}_0\boldsymbol{\alpha}^\dagger & {}_0\boldsymbol{\beta}^\top \\ {}_0\boldsymbol{\beta}^\dagger & {}_0\boldsymbol{\alpha}^\top \end{bmatrix}. \tag{2.123}$$

Thus, from region I to region III, the Bogoliubov transformation is

$$\begin{bmatrix} \boldsymbol{\alpha} & -\boldsymbol{\beta} \\ -\boldsymbol{\beta}^* & \boldsymbol{\alpha}^* \end{bmatrix}, \tag{2.124}$$

where

$$\boldsymbol{\alpha} = {}_0\boldsymbol{\alpha}^\dagger \mathcal{R}(\tau)\, {}_0\boldsymbol{\alpha} - {}_0\boldsymbol{\beta}^\top \mathcal{R}(\tau)^*\, {}_0\boldsymbol{\beta}^*, \tag{2.125}$$

and

$$\boldsymbol{\beta} = {}_0\boldsymbol{\alpha}^\dagger \mathcal{R}(\tau)\, {}_0\boldsymbol{\beta} - {}_0\boldsymbol{\beta}^\top \mathcal{R}(\tau)^*\, {}_0\boldsymbol{\alpha}^*. \tag{2.126}$$

Again, these Bogoliubov coefficients can be calculated perturbatively in h, i.e.,

$$\alpha_{nm} = \alpha_{nm}^{(0)} + \alpha_{nm}^{(1)} h + \alpha_{nm}^{(2)} h^2 + O(h^3), \tag{2.127}$$

$$\beta_{nm} = \beta_{nm}^{(1)} h + \beta_{nm}^{(2)} h^2 + O(h^3), \tag{2.128}$$

where $\alpha_{nm}^{(0)} = \delta_{nm} e^{-i\omega_n \tau}$. Using the perturbative expansions of the Bogoliubov coefficients (2.127), for the second-order terms of (2.104), we get

$$\mathrm{Re}\left(\alpha_{kk}^{(2)}\right) + f_{\alpha,k} - f_{\beta,k} = 0, \tag{2.129}$$

where

$$\begin{aligned} f_{\alpha,k} &:= \frac{1}{2}\sum_{n\neq k}\left|\alpha_{nk}^{(1)}\right|^2, \\ f_{\beta,k} &:= \frac{1}{2}\sum_{n\neq k}\left|\beta_{nk}^{(1)}\right|^2. \end{aligned} \tag{2.130}$$

These perturbative Bogoliubov coefficients were computed [21].

Although the calculation is based on scaler field, the relativistic effects on the evolution of quantum information inside a non-inertially moving cavity can be simulated by electromagnetic fields in cavities. Suppose we have a Fabry-P*é*rot cavity with two parallel reflecting mirrors. This cavity has one partially transmitting mirror and a perfectly reflecting mirror. When a waveguide with matching impedance is aligned closely to the transmitting mirror, the cavity can be coupled with the waveguide on one side. Transverse electromagnetic (TEM) modes in both the cavity and the waveguide can encode quantum information.

From Eq. (2.118), we know the frequency is slightly detuned during the acceleration of the cavity. Thus, a cavity, with a broad spectral width of the resonator mode, is necessary to sustain the resonator mode during acceleration [104]. In a cavity of length about one centimeter, the fundamental resonance frequency is between tens of GHz and one hundred GHz, which falls in the microwave region. To make $h = 0.01$, the acceleration a_c needs to in the order of $10^{17} m/s^2$, which is not feasible. To circumvent this problem, physicists use superconducting waveguides with tunable boundary conditions to simulate the quantum relativistic effect due to non-inertial motions [61, 119, 42].

In this section, I have reviewed Minkowski spacetime and Rindler coordinates. Then I have

discussed quantized scalar field along with Fock space and Bogoliubov transformations. At last, I explained the evolution of quantum information encoded in a scalar field inside a cavity, which moves non-inertially.

2.4 Gaussian quantum information

This section reviews CV quantum information [105, 20], especially Gaussian quantum information theory [116]. In Subsec. 2.4.1, I review the quantization of the electromagnetic field, leading to a harmonic oscillator. Subsection 2.4.2 reviews phase space representation of CV quantum states. Subsetion 2.4.3 reviews basic concepts in Gaussian quantum information, including Gaussian quantum states and Gaussian quantum unitary operations. Subsection 2.4.4 reviews Gaussian quantum channels. Finally in Subsec. 2.4.5, I review $(2,3)$ CV QSS protocol.

2.4.1 Quantization of electromagnetic field

This subsection reviews quantization of the electromagnetic field. I start with classical electromagnetic fields to obtain quantized harmonic oscillators. The content in this subsection is based on Ref. [78].

To begin, let us consider classical electromagnetic fields in free space. They are described by the following Maxwell equations

$$\nabla \times \boldsymbol{H} = \frac{\partial \boldsymbol{D}}{\partial t}, \tag{2.131}$$

$$\nabla \times \boldsymbol{E} = -\frac{\partial \boldsymbol{B}}{\partial t}, \tag{2.132}$$

$$\nabla \cdot \boldsymbol{B} = 0, \tag{2.133}$$

$$\nabla \cdot \boldsymbol{D} = 0, \tag{2.134}$$

with $\boldsymbol{B} = \mu_0 \boldsymbol{H}$ and $\boldsymbol{D} = \varepsilon_0 \boldsymbol{E}$. By using the fact that $\nabla \times \nabla \times \boldsymbol{E} = \nabla(\nabla \cdot \boldsymbol{E}) - \nabla^2 \boldsymbol{E}$, one can get

the wave equation

$$\nabla^2 \boldsymbol{E} - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\boldsymbol{E} = 0, \tag{2.135}$$

where $c = \frac{1}{\sqrt{\varepsilon_0 \mu_0}}$ is the speed of light.

Consider the electromagnetic wave confined in a box of volume $V = L_x \times L_y \times L_z$. The electric field can be expanded as a sum

$$\boldsymbol{E}(t, \boldsymbol{x}) = \sum_{\boldsymbol{k},\mathrm{p}=\pm 1} \boldsymbol{u}_\mathrm{p} A_{\boldsymbol{k},\mathrm{p}}(t) \mathrm{e}^{\mathrm{i}\boldsymbol{k}\boldsymbol{x}} + \boldsymbol{u}_\mathrm{p}^* A_{\boldsymbol{k},\mathrm{p}}(t)^* \mathrm{e}^{-\mathrm{i}\boldsymbol{k}\boldsymbol{x}}, \tag{2.136}$$

where $\boldsymbol{k} = \left(\frac{2n_x\pi}{L_x}, \frac{2n_y\pi}{L_y}, \frac{2n_z\pi}{L_z}\right)$ is the wavenumber, p denotes the polarization, $\boldsymbol{u}_{\pm 1} := \left(\frac{1}{\sqrt{2}}, \pm\frac{\mathrm{i}}{\sqrt{2}}, 0\right)$ is a unit vector representing a polarization direction, and $A_{\boldsymbol{k}}(t)$ is the time-dependent amplitude of the electric field. Each pair $(\boldsymbol{k}, \mathrm{p})$ specifies a plan-wave mode. One can obtain similar expansion for the magnetic field. From the energy density of electromagnetic field, i.e. $\frac{1}{2}\left(\varepsilon_0 |\boldsymbol{E}|^2 + \frac{1}{\mu_0}|\boldsymbol{B}|^2\right)$, we have

$$\mathcal{H} = 2\varepsilon_0 V \sum_{\boldsymbol{k},\mathrm{p}} |A_{\boldsymbol{k},\mathrm{p}}|^2. \tag{2.137}$$

If we define the generalized position and momentum as

$$X := \sqrt{\frac{2\varepsilon_0 V}{\hbar\omega}} \frac{A_{\boldsymbol{k},\mathrm{p}}(t) + A_{\boldsymbol{k},\mathrm{p}}(t)^*}{\sqrt{2}} \tag{2.138}$$

$$P := \sqrt{\frac{2\varepsilon_0 V}{\hbar\omega}} \frac{A_{\boldsymbol{k},\mathrm{p}}(t) - A_{\boldsymbol{k},\mathrm{p}}(t)^*}{\sqrt{2\mathrm{i}}}, \tag{2.139}$$

where $\omega = |\boldsymbol{k}|$ is the frequency, then for each mode $(\boldsymbol{k}, \mathrm{p})$, its Hamiltonian can be written as

$$\mathcal{H} = \frac{\hbar\omega}{2}(X^2 + P^2). \tag{2.140}$$

We can see that each mode of the electromagnetic field is a harmonic oscillator and they are independent from each other.

Now we are ready to quantize the electromagnetic field. Let us replace the classical generalized position X and momentum P by position operator $\hat{q}$ and momentum operator $\hat{p}$, which satisfy the

commutation relation ($\hbar = 1$)

$$[\hat{q}, \hat{p}] = \mathrm{i}\mathbb{1}. \tag{2.141}$$

Here we just focus on one mode and ignore all the other modes. Define the annihilation and creation operators

$$\hat{a} := \frac{\hat{q} + \mathrm{i}\hat{p}}{\sqrt{2}} \tag{2.142}$$

$$\hat{a}^\dagger := \frac{\hat{q} - \mathrm{i}\hat{p}}{\sqrt{2}}. \tag{2.143}$$

Hence, the Hamiltonian in Eq. (2.140) becomes the Hamiltonian of one quantum harmonic oscillator

$$\mathcal{H} = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{\mathbb{1}}{2} \right). \tag{2.144}$$

Finally, the quantized electric field in the cavity is

$$\hat{\boldsymbol{E}}(t, \boldsymbol{x}) = \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}} \sum_{\boldsymbol{k},\mathrm{p}} \boldsymbol{u}_\mathrm{p} \hat{a}_{\boldsymbol{k},\mathrm{p}}(t) \mathrm{e}^{\mathrm{i}\boldsymbol{k}\boldsymbol{x}} + \boldsymbol{u}_\mathrm{p}^* \hat{a}_{\boldsymbol{k},\mathrm{p}}^\dagger(t) \mathrm{e}^{-\mathrm{i}\boldsymbol{k}\boldsymbol{x}}. \tag{2.145}$$

Compared with Eq. (2.136), we find that by quantizing electric field, we just replace the classical amplitude by annihilation and creation operators satisfying the commutation relation in Eq. (2.91).

In this subsection, I have reviewed how to get quantized electric field from classical electric field by replacing generalized position and momentum by operators and introducing commutation relation between position and momentum operators.

2.4.2 Phase space

In this subsection, I review Weyl displacement operators and Wigner functions of trace-class operators. Then I also review P-presentation and Q-representation.

For a bosonic system with m modes, each mode is a quantized harmonic oscillator. Hence, the total state space is a tensor product of Hilbert spaces $\mathscr{H}^{\otimes m}$, where $\mathscr{H}$ is a single-mode Hilbert

space, spanned by Fock number states $\{|n\rangle_{\mathscr{F}}\}_{n=0}^{\infty}$, and m denotes the number of modes.

Each density operator on $\mathscr{F}$ is a trace-class operator. Given an observable O, its mean value is

$$\langle O\rangle_{\rho} \coloneqq \mathrm{tr}(O\rho) = \sum_{n=0}^{\infty} \langle n| O |n\rangle_{\mathscr{F}} . \tag{2.146}$$

To make $\mathrm{tr}(O\rho)$ well defined for any ρ on $\mathscr{F}$, either O is bounded or a sequence of bounded self-adjoint operator $O^{(n)}$ exists such that $\forall |\psi\rangle \in \mathscr{H}$ [49]

$$\left\| O^{(n)} |\psi\rangle - O |\psi\rangle \right\| \to 0, \text{ as } n \to \infty, \tag{2.147}$$

where $\|\cdot\|$ is the Euclidean norm on $\mathscr{F}$. For example, although the number operator $\hat{n}$ is not bounded, due to the finite energy restriction, a sequence of operators

$$\left\{ \sum_{n=0}^{m} n |n\rangle_{\mathscr{F}} \langle n| \right\}_{m=0}^{\infty} \tag{2.148}$$

approaches the limit in (2.147), so the mean photon number $\mathrm{tr}(\hat{n}\rho)$ is always well defined.

Weyl displacement operators

$$D(\boldsymbol{\alpha}) \coloneqq \exp\left(\sum_{i=1}^{m} \alpha_i \hat{a}_i - \alpha_i^* \hat{a}_i^{\dagger} \right), \tag{2.149}$$

where $\boldsymbol{\alpha} \coloneqq (\alpha_1, \ldots, \alpha_m) \in \mathbb{C}^m$, span an orthogonal basis for trace-class operators on $\mathscr{F}^{\otimes m}$ [105]. Any trace-class operator ρ can be written as an integral

$$\rho = \frac{1}{\pi^m} \int_{\mathbb{C}^m} \mathrm{d}^{2m}\boldsymbol{\alpha} \chi_{\rho}(\boldsymbol{\alpha}) D(-\boldsymbol{\alpha}), \tag{2.150}$$

where

$$\chi_{\rho}(\boldsymbol{\alpha}) \coloneqq \mathrm{tr}(\rho D(\boldsymbol{\alpha})), \tag{2.151}$$

is called the characteristic function of density operator ρ. The Fourier transformation of $\chi_{\rho}(\boldsymbol{\alpha})$ is

the Wigner function

$$\mathscr{W}_\rho(\boldsymbol{\alpha}) \coloneqq \int_{\mathbb{C}^m} \frac{\mathrm{d}^{2m}\boldsymbol{\beta}}{\pi^{2m}} \mathrm{e}^{\boldsymbol{\alpha}\boldsymbol{\beta}^\dagger - \boldsymbol{\beta}\boldsymbol{\alpha}^\dagger} \chi_\rho(\boldsymbol{\beta}), \tag{2.152}$$

which is a quasi-probability function over the phase space. The total integral of a Wigner function is one, i.e.,

$$\int_{\mathbb{C}^m} \mathrm{d}^{2m}\boldsymbol{\alpha} \mathscr{W}_\rho(\boldsymbol{\alpha}) = 1. \tag{2.153}$$

The projection of $\mathscr{W}_\rho(\boldsymbol{\alpha})$ onto one quadrature yields a marginal distribution, which can be sampled by homodyne detections. However, different from a classical probability distribution, $\mathscr{W}_\rho(\boldsymbol{\alpha})$ can have negative values.

Similarly, we can obtain the Glauber-Sudarshan P-representation $P_\rho(\boldsymbol{\alpha})$ and Husimi Q-representation $Q_\rho(\boldsymbol{\alpha})$ of ρ from the Fourier transformations of different characteristic functions

$$\chi_\rho^{(1)}(\boldsymbol{\alpha}) \coloneqq \mathrm{tr}(\rho D(\boldsymbol{\alpha})) \mathrm{e}^{\frac{|\boldsymbol{\alpha}|^2}{2^{m+1}}}, \tag{2.154}$$

and

$$\chi_\rho^{(-1)}(\boldsymbol{\alpha}) \coloneqq \mathrm{tr}(\rho D(\boldsymbol{\alpha})) \mathrm{e}^{-\frac{|\boldsymbol{\alpha}|^2}{2^{m+1}}}, \tag{2.155}$$

respectively. $P_\rho(\boldsymbol{\alpha})$ of ρ satisfies

$$\rho = \int_{\mathbb{C}^{2m}} \mathrm{d}^{2m}\boldsymbol{\alpha} P_\rho(\boldsymbol{\alpha}) \left|\boldsymbol{\alpha}\right\rangle \left\langle\boldsymbol{\alpha}\right|, \tag{2.156}$$

and is not a well-defined function if ρ is a non-classical state. Whereas, $Q_\rho(\boldsymbol{\alpha})$ of ρ satisfies

$$Q_\rho(\boldsymbol{\alpha}) = \frac{1}{\pi^m} \left\langle\boldsymbol{\alpha}\right| \rho \left|\boldsymbol{\alpha}\right\rangle, \tag{2.157}$$

and is always a well-defined function for any state ρ.

This subsection reviews three different phase-space distributions of CV quantum states by introducing Weyl displacement operators. In the next subsection, I focus on a particular class of CV states: Gaussian states.

2.4.3 Gaussian states and Gaussian unitary operations

In this subsection, I explain Gaussian states and Gaussian unitary operations. I explain essential Gaussian states like coherent states, thermal states, and squeezed vacuum states. I also review common single-mode and two-mode Gaussian unitary operations.

Gaussian states are those states whose Wigner function is a Gaussian distribution. Gaussian states can be characterized by their first two statistical moments of the quadrature operators. Denote the vector of quadrature operators by

$$\hat{\boldsymbol{x}} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \ldots, \hat{q}_m, \hat{p}_m), \tag{2.158}$$

where for each mode k, the position and momentum operators are

$$\hat{q}_k = \frac{1}{\sqrt{2}}(\hat{a}_k + \hat{a}_k^\dagger), \tag{2.159}$$

$$\hat{p}_k = \frac{-\mathrm{i}}{\sqrt{2}}(\hat{a}_k - \hat{a}_k^\dagger), \tag{2.160}$$

and the canonical commutation relations between two sets of quadrature operators are

$$\begin{aligned} &[\hat{q}_k, \hat{q}_{k'}] = [\hat{p}_k, \hat{p}_{k'}] = 0, \\ &[\hat{q}_k, \hat{p}_{k'}] = \mathrm{i}\delta_{kk'}. \end{aligned} \tag{2.161}$$

The first two satistical moments of $\hat{\boldsymbol{x}}$ are mean values

$$\bar{\boldsymbol{x}} \coloneqq \langle \hat{\boldsymbol{x}} \rangle = \mathrm{Tr}(\hat{\boldsymbol{x}}\rho), \tag{2.162}$$

and covariance matrix

$$\boldsymbol{V}_{ij} \coloneqq \frac{1}{2}\left\langle \left\{ \hat{x}_i - \langle \hat{x}_i \rangle, \hat{x}_j - \langle \hat{x}_j \rangle \right\} \right\rangle, \tag{2.163}$$

where $\{A, B\} \coloneqq AB + BA$ is the anti-commutator.

Discrete variable (qubit or qudit)	Continuous variable
Finite-dimensional Hilbert space	Countably-infinite-dimensional Hilbert space
Pauli group	Heisenberg-Weyl (HW) group
Clifford group	$\mathrm{HW}(m) \rtimes \mathrm{Sp}(2m,\mathbb{R})$

Table 2.2: Comparison between discrete-variable quantum information and CV quantum information.

Gaussian operations are those operations that preserve the Gaussian character of a quantum state. Gaussian-preserving unitary operations form the semidirect product group [13]

$$\mathrm{HW}(m) \rtimes \mathrm{Sp}(2m,\mathbb{R}) = \{U_{\boldsymbol{S},\boldsymbol{d}}; \boldsymbol{S} \in \mathrm{Sp}(2m,\mathbb{R}), \boldsymbol{d} \in \mathbb{R}^{2m}\} \tag{2.164}$$

for $\mathrm{HW}(m)$ the Heisenberg-Weyl group comprising displacement operations (2.149) on m-mode phase space and $\mathrm{Sp}(2m,\mathbb{R}) \coloneqq \{\boldsymbol{S} \in GL(2m,\mathbb{R}); \boldsymbol{S}\Omega\boldsymbol{S}^\top = \Omega\}$ the real symplectic group comprising squeezers and linear optical interferometers. Gaussian unitary operations are generated by Hamiltonians which are quadratic in annihilation and creation operators. Table 2.2 shows the analogy between Pauli group and Heisenberg-Weyl group, as well as Clifford group and the group of all Gaussian unitary operations.

Here, unitary operations are those transformations $U \in \mathscr{L}(\mathscr{F})$ such that $\forall |\psi\rangle, |\phi\rangle \in \mathscr{H}$,

$$\langle\psi|\phi\rangle = \langle U\psi|U\phi\rangle\,. \tag{2.165}$$

Both $\mathrm{HW}(m)$ and $\mathrm{Sp}(2m,\mathbb{R})$ are non-compact groups, and they have unitary representations on Hilbert space $\mathscr{H}$. The unitary operations

$$\mathrm{e}^{-\mathrm{i}\left(\phi\mathbb{1}+\alpha\hat{a}+\alpha^*\hat{a}^\dagger\right)} \tag{2.166}$$

for $\phi \in [0,2\pi)$ and $\alpha \in \mathbb{C}$ form a unitary representation of $\mathrm{HW}(1)$ on $\mathscr{H}$ [18]. Unitary operation $U_{\boldsymbol{S},\boldsymbol{d}}$, inducing symplectic transformation $\boldsymbol{S}$ and displacement $\boldsymbol{d}$ on phase space, is the unitary representation of $\mathrm{HW}(m) \rtimes \mathrm{Sp}(2m,\mathbb{R})$ on $\mathscr{H}$.

In Heisenberg picture, a Gaussian unitary operation leads to a linear transformation of the quadrature operators

$$\hat{\boldsymbol{x}} \to U^{\dagger}_{\boldsymbol{S},\boldsymbol{d}} \hat{\boldsymbol{x}} U_{\boldsymbol{S},\boldsymbol{d}} = \boldsymbol{S}\hat{\boldsymbol{x}} + \boldsymbol{d}. \tag{2.167}$$

Every Gaussian unitary operation is equivalent to an affine map $(\boldsymbol{S}, \boldsymbol{d})$ in phase space. In terms of the mean values and the covariance matrix of quadrature operators, a Gaussian unitary operation $(\boldsymbol{S}, \boldsymbol{d})$ transforms

$$\begin{aligned} \bar{\boldsymbol{x}} &\to \boldsymbol{S}\bar{\boldsymbol{x}} + \boldsymbol{d}, \\ \boldsymbol{V} &\to \boldsymbol{S}\boldsymbol{V}\boldsymbol{S}^{\top}. \end{aligned} \tag{2.168}$$

As the first two statistical moments characterize a Gaussian state, the transformations in Eqs. (2.168) completely characterize a Gaussian unitary transformation.

Here I provide some important examples of Gaussian unitary operations, which will be used later. We begin with vacuum state that is the state annihilated by annihilation operator

$$\hat{a} \left|0\right\rangle_{\mathscr{F}} = 0. \tag{2.169}$$

By applying a displacement operator $D(\alpha)$, we get a coherent state

$$\left|\alpha\right\rangle = D(\alpha) \left|0\right\rangle_{\mathscr{F}}. \tag{2.170}$$

Coherent state $\left|\alpha\right\rangle$ is the eigenstate of the annihilation operator $\hat{a}$, i.e.,

$$\hat{a} \left|\alpha\right\rangle = \alpha \left|\alpha\right\rangle. \tag{2.171}$$

The mean values of quadrature operators are $\bar{\boldsymbol{x}} = (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$. The covariance matrix $\boldsymbol{V}$ is the identity matrix.

A thermal state at temperature T is a Gaussian state with density operator on Fock basis

$$\rho_T(\bar{n}_T) = \sum_{n=0}^{\infty} \frac{\bar{n}_T^n}{(\bar{n}_T+1)^{n+1}} |n\rangle_{\mathscr{F}} \langle n|, \; \bar{n}_T \coloneqq \frac{1}{e^{\frac{\hbar\omega}{k_B T}} - 1}, \tag{2.172}$$

where $\bar{n}_T$ is the mean photon number, ω is the frequency for this mode, and k_B is Boltzmann's constant. The density operator of a thermal state can be represented as a function of annihilation and creation operators [29, 39],

$$\rho_T(\bar{n}_T) = \frac{1}{\bar{n}_T+1} \sum_{n=0}^{\infty} \frac{(-1)^n \hat{a}^{\dagger n} \hat{a}^n}{n!(\bar{n}_T+1)^n}. \tag{2.173}$$

The mean values are zero and the covariance matrix is

$$\boldsymbol{V} = (2\bar{n}+1)\mathbb{1}, \tag{2.174}$$

where $\mathbb{1}$ is an identity matrix.

Next, we discuss single-mode squeezed states, which can be generated by degenerate spontaneous parametric down-conversion (SPDC). When a strong pump laser with phone frequency 2ω is ejected onto a nonlinear crystal, there are certain nonzero probability that a photon is split into two photons with the same frequency ω. The Hamiltonian of the nonlinear optical process is

$$\mathcal{H} = i\hbar(s^* \hat{a}^{\dagger 2} - s\hat{a}^2), \tag{2.175}$$

where $s \in \mathbb{C}$.

Suppose s is real; hence, the unitary operation $U = \exp\left(\frac{i\mathcal{H}}{2\hbar}\right)$ leads to the Bogoliubov transformation

$$\hat{a} \to \cosh s\hat{a} - \sinh s\hat{a}^\dagger. \tag{2.176}$$

Then the quadrature operators are transformed by the symplectic matrix

$$\boldsymbol{S} = \begin{pmatrix} \mathrm{e}^{-s} & 0 \\ 0 & \mathrm{e}^{s} \end{pmatrix} \tag{2.177}$$

The covariance of a single-mode squeezed state is

$$\boldsymbol{V} = \begin{pmatrix} \mathrm{e}^{-2s} & 0 \\ 0 & \mathrm{e}^{2s} \end{pmatrix}, \tag{2.178}$$

indicating that the uncertainty of quadrature $\hat{q}$ is squeezed, while the uncertainty of quadrature $\hat{p}$ is amplified.

Besides single-mode quantum operations, two-mode quantum operations are also common for CV quantum information processing. Beam splitting is a two-mode quantum operation, which combines two optical fields and preserves the total photon number. The Hamiltonian of beam splitting is

$$\mathcal{H} = \mathrm{i}\hbar \left(\gamma^* \hat{a}_1^\dagger \hat{a}_2 - \gamma \hat{a}_1 \hat{a}_2^\dagger \right), \tag{2.179}$$

where $\gamma \in \mathbb{C}$. Suppose γ is real. Then the unitary operation $\exp\left(\frac{-\mathrm{i}\mathcal{H}}{\hbar}\right)$ leads to the Bogoliubov transformation

$$\hat{a}_1 \to \cos\gamma \hat{a}_1 - \sin\gamma \hat{a}_2 \tag{2.180}$$

$$\hat{a}_2 \to \cos\gamma \hat{a}_2 + \sin\gamma \hat{a}_1 \tag{2.181}$$

Hence, the symplectic transformation of beam splitting on quadrature operators is

$$BS = \begin{pmatrix} \cos\gamma \mathbb{1} & -\sin\gamma \mathbb{1} \\ \sin\gamma \mathbb{1} & \cos\gamma \mathbb{1} \end{pmatrix}. \tag{2.182}$$

Another kind of two-mode quantum operation is two-mode squeezing. Two-mode squeezed

state can be generated by non-degenerate SPDC. In non-degenerate SPDC, a strong pump laser is ejected onto a nonlinear crystal, and certain photons with frequency 2ω are split into two photons, one with frequency ω_1 and the other with frequency $\omega_2 = 2\omega - \omega_1$. The Hamiltonian of this process is

$$\mathcal{H} = \mathrm{i}\hbar \left(s^* \hat{a}_1 \hat{a}_2 - s \hat{a}_1^\dagger \hat{a}_2^\dagger \right), \tag{2.183}$$

where $s \in \mathbb{C}$.

Suppose s is real. Then the unitary operation $\exp\left(\frac{-\mathrm{i}\mathcal{H}}{\hbar}\right)$ leads to the Bogoliubov transformation

$$\hat{a}_1 \to \cosh s \hat{a}_1 + \sinh s \hat{a}_2^\dagger, \tag{2.184}$$

$$\hat{a}_2 \to \cosh s \hat{a}_2 + \sinh s \hat{a}_1^\dagger. \tag{2.185}$$

The symplectic transformation on quadrature operators is

$$TMS = \begin{pmatrix} \cosh s \mathbb{1} & \sinh s Z \\ \sinh s Z & \cosh s \mathbb{1} \end{pmatrix}, \tag{2.186}$$

where $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. From Eq. (2.168), we know that the covariance matrix of a two-mode squeezed vacuum state is

$$\boldsymbol{V} = \begin{pmatrix} v\mathbb{1} & \sqrt{v^2-1}Z \\ \sqrt{v^2-1}Z & v\mathbb{1} \end{pmatrix}, \tag{2.187}$$

where $v = \cosh^2 s + \sinh^2 s$.

From the covariance matrix (2.187), we find that that

$$\mathrm{Var}\left(\frac{\hat{q}_1 - \hat{q}_2}{\sqrt{2}} \right) = \mathrm{Var}\left(\frac{\hat{p}_1 + \hat{p}_2}{\sqrt{2}} \right) = \mathrm{e}^{-2s}, \tag{2.188}$$

where $\mathrm{Var}(A) = \langle A^2 \rangle - \langle A \rangle^2$. When $s > 0$, the variances of the linear combinations of quadrature operators in Eq. (2.188) are squeezed, meaning that the two modes are correlated with each other.

2.4.4 Gaussian channels

This subsection first reviews the general form of Gaussian channels. Then I present the canonical form of a single-mode Gaussian channel. Finally, I discuss two types of single-mode Gaussian channels: one is thermal lossy channel; the other is the amplifying channel. This subsection mainly follows the content in [116].

A Gaussian channel maps a Gaussian quantum state to another Gaussian quantum state. A general Gaussian channel yields the transformation

$$\bar{\boldsymbol{x}} \to \boldsymbol{M}\bar{\boldsymbol{x}} + \boldsymbol{d}, \tag{2.189}$$

$$\boldsymbol{V} \to \boldsymbol{M}\boldsymbol{V}\boldsymbol{M}^{\top} + \boldsymbol{N}, \tag{2.190}$$

where $\boldsymbol{M}$ and $\boldsymbol{N}^{\top} = \boldsymbol{N}$ are real matrices satisfying

$$\boldsymbol{N} + \mathrm{i}\boldsymbol{\Omega} - \mathrm{i}\boldsymbol{M}\boldsymbol{\Omega}\boldsymbol{M}^{\top} \geq \boldsymbol{0}. \tag{2.191}$$

When $\boldsymbol{N} = \boldsymbol{0}$ and $\boldsymbol{M}$ is a symplectic matrix, the Gaussian channel becomes a Gaussian unitary operation in Eq. (2.168).

Any single-mode Gaussian channel $\mathcal{E}$, characterized by $\boldsymbol{d}$, $\boldsymbol{M}$ and $\boldsymbol{N}$, is equivalent to a canonical single-mode Gaussian channel $\mathcal{E}_{\mathrm{c}}$ up to two Gaussian unitary operations. For the canonical form $\mathcal{E}_{\mathrm{c}}$, $\boldsymbol{d}_{\mathcal{E}_{\mathrm{c}}} = 0$ and both $\boldsymbol{M}_{\mathcal{E}_{\mathrm{c}}}$ and $\boldsymbol{N}_{\mathcal{E}_{\mathrm{c}}}$ are diagonal matrices, which are determined by three parameters, invariant under Gaussian unitary operations. The first is

$$\mathscr{R} := \min\left[\mathrm{rank}(\boldsymbol{M}), \mathrm{rank}(\boldsymbol{N})\right]. \tag{2.192}$$

The second is transmissivity of the channel

$$\zeta := \det \boldsymbol{M}. \tag{2.193}$$

The third is thermal number $\bar{n}$, the definition of which is omitted here.

Now let me explain two important classes of single-mode Gaussian channels. The first one is lossy channel or attenuation channel, for which, $\mathscr{R} = 2$ and $0 < \zeta < 1$. The transformation matrices for lossy channels are

$$\boldsymbol{M}_{\mathcal{E}_c} = \sqrt{\zeta}\mathbb{1}, \quad \boldsymbol{N}_{\mathcal{E}_c} = (1-\zeta)(2\bar{n}+1)\mathbb{1}. \tag{2.194}$$

Lossy channels can be implemented by a beam splitter with transmissivity ζ combining the input mode with $\rho_T(\bar{n})$. The second one is amplifying channel, for which, $\mathscr{R} = 2$ and $\zeta > 1$. The transformation matrices for amplifying channels are

$$\boldsymbol{M}_{\mathcal{E}_c} = \sqrt{\zeta}\mathbb{1}, \quad \boldsymbol{N}_{\mathcal{E}_c} = (\zeta-1)(2\bar{n}+1)\mathbb{1}. \tag{2.195}$$

Amplifying channels can be implemented by a two-mode squeezing operation combining the input mode with $\rho_T(\bar{n})$.

This subsection has reviewed the general form of multi-mode Gaussian channels and the canonical form of single-mode Gaussian channels. Next subsection presents a CV quantum communication protocol.

2.4.5 Continuous-variable tripartite QSS

In this subsection, let us review a tripartite QSS protocol where the secret is CV quantum information. This protocol was investigated theoretically [72] and experimentally implemented in optical system [71]. This protocol is a $(2,3)$-threshold QSS protocol. It encodes one quantum state into a tripartite quantum state as three quantum shares. These three quantum shares are distributed to three players. Any two players can use their two quantum shares to decode the secret quantum state.

Hereafter suppose the secret state is an arbitrary coherent state. As all the coherent states form an overcomplete basis of the infinite-dimensional Hilbert space, this QSS protocol can share any

CV quantum information in principle. Now I explain how this protocol encodes and decodes a coherent state in the Heisenberg picture.

Suppose the quadrature operators of the secret coherent state are $(\hat{q}_\alpha, \hat{p}_\alpha)$. Two ancillary states are both single-mode squeezed vacuum states, one of which is squeezed in quadrature $\hat{q}$ and the other is squeezed in quadrature $\hat{p}$. The quadrature operators of these two ancillary states can be written as $\left(\mathrm{e}^{-s}\hat{q}^{(0)}, \mathrm{e}^{s}\hat{p}^{(0)}\right)$ and $\left(\mathrm{e}^{s}\hat{q}'^{(0)}, \mathrm{e}^{-s}\hat{p}'^{(0)}\right)$, where $\left(\hat{q}^{(0)}, \hat{p}^{(0)}\right)$ and $\left(\hat{q}'^{(0)}, \hat{p}'^{(0)}\right)$ are the quadrature operators of two vacuum states and s is the squeezing parameter.

The two ancillary states are combined by a balanced beam splitter, and the output state is a two-mode squeezed state. One output is combined with the secret state by another balanced beam splitter. Hence, the two outputs of the second beam splitter together with the other output of the first beam splitter form the three quantum shares. The quadrature operators of these three quantum shares are expressed in terms of the input quadrature operators in the following.

$$(\hat{q}_1, \hat{p}_1) = \left(\frac{1}{\sqrt{2}}\hat{q}_\alpha + \frac{1}{2}\mathrm{e}^{-s}\hat{q}^{(0)} + \frac{1}{2}\mathrm{e}^{s}\hat{q}'^{(0)}, \frac{1}{\sqrt{2}}\hat{p}_\alpha + \frac{1}{2}\mathrm{e}^{s}\hat{p}^{(0)} + \frac{1}{2}\mathrm{e}^{-s}\hat{p}'^{(0)}\right), \tag{2.196}$$

$$(\hat{q}_2, \hat{p}_2) = \left(\frac{1}{\sqrt{2}}\hat{q}_\alpha - \frac{1}{2}\mathrm{e}^{-s}\hat{q}^{(0)} - \frac{1}{2}\mathrm{e}^{s}\hat{q}'^{(0)}, \frac{1}{\sqrt{2}}\hat{p}_\alpha - \frac{1}{2}\mathrm{e}^{s}\hat{p}^{(0)} - \frac{1}{2}\mathrm{e}^{-s}\hat{p}'^{(0)}\right), \tag{2.197}$$

$$(\hat{q}_3, \hat{p}_3) = \left(\frac{1}{\sqrt{2}}\mathrm{e}^{-s}\hat{q}^{(0)} - \frac{1}{\sqrt{2}}\mathrm{e}^{s}\hat{q}'^{(0)}, \frac{1}{\sqrt{2}}\mathrm{e}^{s}\hat{p}^{(0)} - \frac{1}{\sqrt{2}}\mathrm{e}^{-s}\hat{p}'^{(0)}\right). \tag{2.198}$$

Fig. 2.4 shows the encoding circuit of this $(2,3)$ quantum secret sharing scheme.

These three quantum shares are distributed to players 1, 2 and 3. If s is large enough, all the quantum shares contain high quantum noises such that any single player can obtain little information about the quantum secret state. If player 1 and player 2 collaborate, they just combine their two quantum shares by a balanced beamer. One output of the beam splitter is the quantum secret state.

If player 2 and player 3 collaborate, then they first combine their two quantum shares by a $2/3$ reflective beam splitter. Then they apply a homodyne detection on quadrature $\hat{q}$ of one output of the beam splitter, obtaining the measurement outcome q_{out}. Hence, they apply a displacement operation on quadrature $\hat{q}$ of the other output of the beam splitter with the shift amount being

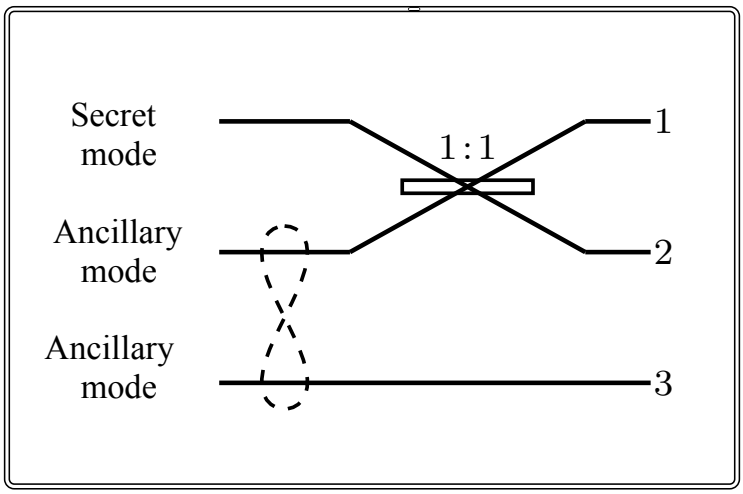


Figure 2.4: The encoding circuit for CV $(2,3)$-threshold quantum secret sharing. The "8" shaped symbol represents a two-mode squeezed-vacuum state. The upper two modes are combined on a balanced beam splitter. The three outputs are three quantum shares, denoted by mode 1, mode 2, and mode 3.

the product of q_{out} and amplification gain $G = 2\sqrt{2}$. The final state is a squeezed version of the quantum secret state. The quadrature operators of the final state are

$$(\hat{q}_{\text{final}}, \hat{p}_{\text{final}}) = \left(\sqrt{3}\hat{q}_\alpha - \sqrt{6}\mathrm{e}^{-s}\hat{q}^{(0)}, \frac{1}{\sqrt{3}}\hat{p}_\alpha - \frac{\sqrt{2}}{\sqrt{3}}\mathrm{e}^{-s}\hat{p}'^{(0)} \right). \tag{2.199}$$

When the squeezing parameter s goes to infinity, the fidelity of the decoded state approaches unity. A similar decoding scheme for the case that player 1 and player 3 collaborate is omitted here.

In this section, I have reviewed the quantized harmonic oscillator and phase spacetime representation of CV quantum states. I have discussed Gaussian quantum states, Gaussian unitary operations and Gaussian quantum channels. Finally, I have reviewed a CV QSS protocol, which is used later in Sec. 5.2.

This chapter reviews elements of quantum information theory, QEC, relativistic quantum information, and Gaussian quantum information. QEC is utilized for quantum summoning protocol in Chapter 4. The results on relativistic quantum information lays the foundation for relativistic quantum secret sharing in Chapter 5. Gaussian quantum information theory is useful in Chapters 5, 6

and 7.

Chapter 3

Quantum summoning

This chapter reviews quantum summoning, first proposed by Kent [65] and reformulated by Hayden and May [52]. After that, more general summoning protocols are introduced [2, 53, 66] and more efficient QEC codes are proposed for summoning [54, 121]. Quantum summoning is investigated for both the purpose of relativistic quantum cryptography [62, 63, 67] as well as for the interpretation of quantum information paradoxes in subtle spacetime structures [85]. I explain quantum summoning as an adversarial game formulated in [52] in Sec. 3.1. Section 3.2 presents the mathematical definitions of summoning including notations. Section 3.3 reviews several generalized quantum summoning tasks.

3.1 Quantum summoning

This section introduces a quantum task, called quantum summoning, in Minkowski spacetime. Quantum summoning is a relativistic quantum information processing task combining both quantum mechanics and special relativity. I explain the procedure of this task and also present two examples to illustrate how to summon a qubit by using quantum secret sharing or quantum error correction code.

Summoning is an information processing protocol involving two adversarial parties Alice and Bob [65, 52, 54]. Bob's role is to provide quantum information to Alice and to designate where the

quantum information is to be summoned and Alice's role is to summon quantum information at the designated spacetime location. Associated with each request point y is a reveal point z_y that is in the causal future of y. The intersection of the future light cone of y with the past light cone of z_y is called a causal diamond, expressed as $\diamondsuit$. We label causal diamonds and show a label i in the diamond as $\langle i \rangle$. Besides the request and reveal points, Alice and Bob also agree upon a starting point s, where Bob provides the quantum information to Alice.

Alice and Bob can arrange their agents at various points in spacetime prior to the start of summoning [54]. Bob designates one agent to be the referee who sends quantum information to point s and classical information to all the request points. Alice designates one agent to be the starting agent S, who is situated at point s, and she delegates agents to each request and reveal point. We label the agent at point x by A_x. Suppose Alice and her agents have ideal quantum devices and instantaneous quantum-information-processing power. Figure 3.1 shows an example of Alice's and Bob's agents arranged in spacetime.

When summoning starts, the referee prepares a quantum state

$$|\psi\rangle \in \mathscr{H}, \tag{3.1}$$

where $\mathscr{H}$ is a finite d-dimensional Hilbert space [52], and transmits $|\psi\rangle$ to the starting agent. Alice and all her agents do not have any knowledge of $|\psi\rangle$. The referee randomly chooses one request point, say y, and sends the request only to A_y. Then Alice's task is to present the quantum state $|\psi\rangle$ at the corresponding reveal point z_y, by her agents' collaboration.

Given a set of causal diamonds $\left\{\langle i \rangle\right\}_{i=1}^{N}$, summoning might be infeasible [65] due to the restrictions of both the no-cloning theorem [93, 120, 34, 91] and no superluminal communication [120]. Quantum summoning is possible when there exists a protocol for Alice such that, no matter which request point is chosen, Alice can reconstruct the state at the corresponding reveal point with perfect certainty.

Theorem 1 ([52])**.** *Summoning is possible if and only if the following two conditions are satisfied.*

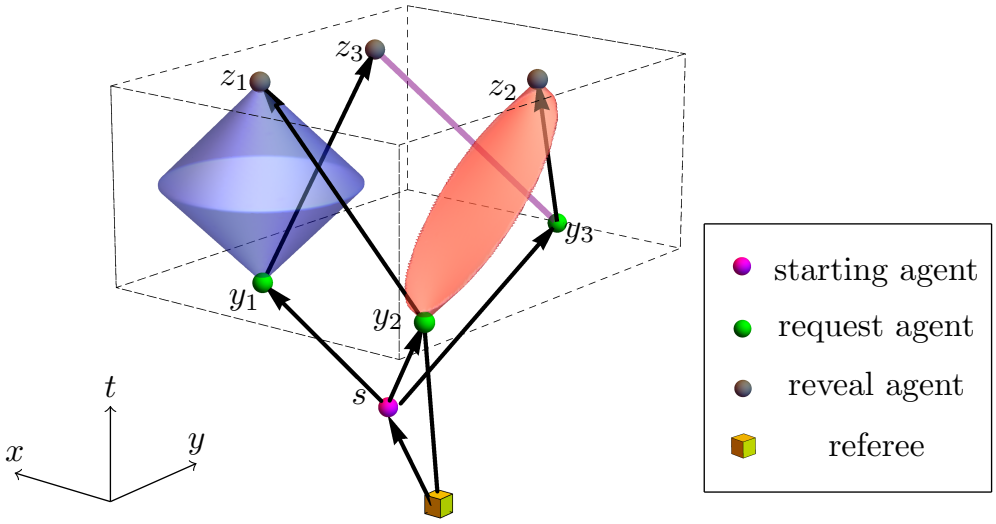


Figure 3.1: Three causal diamonds (red, blue and purple) in spacetime. The red oval shape is a causal diamond formed by two spacetime points close to light-like line and the purple line segment is a causal diamond formed by two light-like seperated spacetime points. A referee, a starting agent, three request agents, and three reveal agents are arranged in spacetime. An arrow represents a quantum communication channel from one agent to another agent, and a line segment between two agents represents a classical channel from one to the other. The referee sends a quantum state $|\psi\rangle$ to the starting agent, and randomly chooses y_2 to send a classical request to A_{y_2}. The starting agent encodes $|\psi\rangle$ to three qutrits and distribute them to three request agents respectively. A_{y_2} sends her qutrit to A_{z_2}. Receiving no request, the request agents at y_1 and y_3 send their qutrits to A_{z_3} and A_{z_2} respectively. Hence, A_{z_2} receives two qutrits and decodes the state $|\psi\rangle$.

1. *All reveal points are in the causal future of* s.

2. *Each pair of causal diamonds is causally related, which means that there exists a point in one causal diamond that is causally related with at least one point in the other causal diamond.*

We call a set of causal diamonds satisfying these two conditions a “valid configuration" for summoning.

We represent a configuration of causal diamonds by a graph $\mathscr{G}$ as follows [52, 54]. We assign each causal diamond to a vertex and use the label of the causal diamond to label the vertex. If two causal diamonds are causally related, an edge e is inserted between the two corresponding vertices in G. A valid configuration of N causal diamonds is represented by an N-vertex complete graph denoted K_N, for which each pair of vertices is connected by an edge [35].

In Fig. 3.1, we present an example of using quantum secret sharing [27, 47, 83] to summon quantum information [52]. After receiving a qubit $|\psi\rangle$, the starting agent encodes $|\psi\rangle$ into three qutrits[1] [27] and distributes the three qutrits to the three request agents. If A_{y_i} ($i = 1, 2,$ or 3) receives the request, then the request agent sends her qutrit to the reveal point

$$z_i := z_{y_i}. \tag{3.2}$$

Otherwise, she sends her qutrit to the reveal point $z_{(i-1) \bmod 3}$. In such a way, no matter which request agent receives the request, the associated reveal agent receives two qutrits to retrieve the original qubit $|\psi\rangle$.

Quantum summoning is an operational task to interpret how quantum information can be delocalized and later localized again in spacetime. Quantum summoning can be considered as a superposition of localization of quantum information in spacetime in a restricted way: quantum information is delocalized in several causal diamonds, possibly overlap with each other, such that the quantum information can be localized in any one of these causal diamonds, but localization in one causal diamond forbids the localization in any other causal diamond. However, this classi-

[1] A qutrit or a quantum trit is a quantum state in a three-level system

cal interpretation of the locality of quantum systems is not accurate, as quantum particle only has operation meaning when we consider a detector and any particle cannot have a definite position without any uncertainty. What we mean by localization of quantum information is that in a small region in spacetime, the probability to detect a particle within this region is close to unit [94]. Furthermore, All the agents in quantum summoning are in one inertial frame such that we do not need to consider how Lorentz transformation affects quantum information.

In this section, I have reviewed quantum summoning as an adversarial game. The conditions for quantum summoning imply the limitation of distribution of quantum information in spacetime. QEC code, specifically, QSS can be used to summon quantum information.

3.2 Mathematical definition of summoning

In this section, we mathematically define both classical and quantum summoning. We begin by formalizing the notions of past and future light cones and causal diamonds. We then establish notations for a configuration of causal diamonds and the sets of request and reveal points. Subsequently, we give a careful definition of both classical and quantum summoning, and when these tasks are trivial.

Each spacetime point is $x \in \mathcal{M}$, where $\mathcal{M}$ denotes Minkowski spacetime [111]. The future light cone for x is

$$\mathrm{fut}(x) := \{w \in \mathcal{M}; w \succ x\}, \tag{3.3}$$

where $w \succ x$ indicates that information can be sent from x to w. The past light cone for x is

$$\mathrm{pas}(x) := \{w \in \mathcal{M}; w \prec x\}, \tag{3.4}$$

where $w \prec x$ indicates that information can be received at x from w. A causal diamond for a pair

of points $(y_i, z_i) \in \mathcal{M} \times \mathcal{M}$ satisfying $y_i \prec z_i$ is

$$\diamondsuit_i := \{x \in \mathcal{M}; x \in \text{fut}(y_i) \cap \text{pas}(z_i)\}. \tag{3.5}$$

A configuration of causal diamonds is

$$\mathscr{C} := \left\{\diamondsuit_i; y_i \prec z_i\right\}, \tag{3.6}$$

and $N := |\mathscr{C}|$. Two causal diamonds $\diamondsuit_i$ and $\diamondsuit_j$ are causally related if and only if $\exists x \in \diamondsuit_i$, $\exists w \in \diamondsuit_j$ such that either $x \in \text{fut}(w)$, or $x \in \text{pas}(w)$. The set of request points is

$$\text{REQ} := \left\{y_i \in \mathcal{M}; \diamondsuit_i \in \mathscr{C}\right\}, \tag{3.7}$$

and the set of reveal points is

$$\text{REV} := \left\{z_i \in \mathcal{M}; \diamondsuit_i \in \mathscr{C}\right\}. \tag{3.8}$$

A starting point is $\text{s} \in \mathcal{M}$ such that $\forall z \in \text{REV}, z \in \text{fut}(\text{s})$, where there is a starting agent S.

We now formalize Kent's classical summoning protocol [65] by making each object mathematically well defined. Given starting agent S at $\text{s} \in \mathcal{M}$, request agents

$$\text{REQAG} := \left\{A_y; y \in \text{REQ}\right\} \tag{3.9}$$

and corresponding reveal agents

$$\text{REVAG} := \{A_z; z \in \text{REV}\}, \tag{3.10}$$

and S possessing n-bit string $m \in \{0,1\}^n$, summoning is the task of delivering m to any agent in REVAG given arbitrary external selection of some $y \in \text{REQ}$, which is only revealed at spacetime point y.

Remark 1. Classical summoning is trivial because S broadcasts m to all $z \in \mathrm{REV}$ [65].

The notion of quantum summoning [65, 52] builds on the concept of classical summoning, which we formalize as follows. Given a starting agent S, REQAG and REVAG, and S possessing quantum information

$$|\Psi\rangle \in \mathscr{H}_2^{\otimes n} \tag{3.11}$$

(with S possibly oblivious to $|\Psi\rangle$), summoning is the task of delivering $|\Psi\rangle$ to any agent in REVAG given arbitrary external selection of some $y \in \mathrm{REQ}$, which is only revealed at spacetime point y.

Remark 2. Summoning is trivial if S has a classical description of $|\Psi\rangle$ because S broadcasts this description such that all agents in REVAG receive and can reconstruct $|\Psi\rangle$.

Remark 3. Quantum summoning is trivial if there is a causal curve, which starts from s and runs sequentially through all $\diamondsuit_i \in \mathscr{C}$ in any order. The protocol is trivial in this case because quantum information can simply be sent along this causal curve. When quantum information arrives at $\diamondsuit_j$, A_{y_j} decides whether to send it to z_j or to send it to the next causal diamond depending on whether she receives the request or not. In the next section, I explain more generalized quantum summoning protocols.

3.3 Generalization of quantum summoning

This section explains several generalized versions of quantum summoning. These quantum tasks relax the restriction of single one request, generalize the functional dependence of reveal points on the classical inputs at request points, and study localization in any arbitrary spacetime regions rather than causal diamonds, respectively.

The first generalized quantum summoning task is a multi-request single-reveal summoning task [2]. The difference of this generalized summoning task is that Bob's agent, referee, does not have to choose only one request point. Instead, he randomly chooses a nonempty set

$$\{y_i; i \in S\} \tag{3.12}$$

of request points, where $S \subseteq [N]$ and $S \neq \emptyset$. Then, Alice, with her agents, is required to reconstruct the state $|\psi\rangle$ at any reveal point

$$z \in \{z_i; i \in S\}. \tag{3.13}$$

Corollary 1.1 ([2]). *Multi-request single-reveal summoning task is possible if and only if the following two conditions are satisfied:*

1. *All reveal points are in the causal future of* s.
2. *For any nonempty subset $S \in [N]$, there exists $i \in S$ such that z_i is in the causal future of y_j for every $j \in S$.*

The conditions in Corollary 1.1 is more restrictive than the conditions in Theorem 1.

Another generalized summoning task generalizes the functional dependence of reveal point on the classical inputs at request points [66]. The difference between this generalized summoning task and the original summoning task is that in the original summoning tasks, the classical input at every request point y_i is one bit: one indicates a request at z_i and zero indicates no request at z_i. In this generalized summoning task, the input at each request point y_i can be any integer $m_i \in [n_i]$, and $f(m_1, \ldots, m_N)$ determines which reveal point Alice should reconstruct the unknown state $|\psi\rangle$, where f is a surjective mapping

$$f : [n_1] \times [n_2] \times \cdots \times [n_N] \to [N], \tag{3.14}$$

where $\times$ denotes a Cartesian product. This task is possible when there exists a protocol for Alice such that no matter what inputs are at the request points, Alice, with her agents, can reconstruct the unknown state at the corresponding reveal point.

Corollary 1.2 ([66]). *Summoning task with unconstrained inputs and a single reveal point is possible if and only if the following conditions are satisfied:*

1. *All reveal points are in the causal future of* s.

2. *For each pair of reveal points* (z_i, z_j)*, the set* $S_{ij} := \{y_k; y_k \prec z_i, y_k \prec z_j, k \in [N]\} \neq \emptyset$.

3. *For each pair of reveal points* (z_i, z_j)*, any possible inputs at the set of request points* S_{ij} *can logically exclude at least one possibility of* z_i *and* z_j *as the designated reveal point.*

Quantum summoning for a set of causal diamonds can also be generalized to a localization task, where quantum information is distributed over a collection of arbitrary spacetime regions. In the localization task, a third party, Charlie, prepares a state $|\psi\rangle$, which is unknown to both Alice and Bob, and hands $|\psi\rangle$ over to Alice at point s. Bob's task is to randomly choose a spacetime region, say Σ, from a set of arbitrary spacetime regions, and prepare $|\psi\rangle$ by utilizing exactly the information present inside Σ. Although Bob can access only the information present inside the region Σ, he does not have to reconstruct $|\psi\rangle$ inside Σ. Instead, Bob can reconstruct the state $|\psi\rangle$ either inside Σ or later. Alice's task is to distribute state $|\psi\rangle$ over all the spacetime regions, with help from her agents, such that no matter which region Bob chooses, he can always successfully prepare state $|\psi\rangle$. To accomplish this task, Alice can designate her agents to be distributed anywhere in spacetime.

A localization task is possible when no matter which region Bob chooses, there exists a protocol for Bob to reconstruct the state $|\psi\rangle$ with perfect certainty.

Corollary 1.3 ([53])**.** *Localization task is possible if and only if*

1. *For each spacetime region, there is at least one point in the causal future of* s.

2. *Each pair of spacetime regions is causally related, which means that there exists a point in one region that is causally related to at least one point in the other region.*

When those spacetime regions are causal diamonds, these two conditions become the same as the conditions in Theorem 1.

All these different versions of quantum tasks follow the common basic idea: certain unknown quantum information, prepared somewhere in spacetime, is delocalized over a set of spacetime regions and then localized later at another spacetime point. All these tasks and their conditions

to be possible provide us with the operational interpretations of the limitations of distribution of quantum information in spacetime. Studying which quantum tasks is possible in spacetime and which is impossible may be a way to find potential applications in relativistic quantum cryptography [64, 77]. On the other hand, understanding the flow of quantum information in Minkowski spacetime paves the way for physicists to solve quantum information puzzles in subtle spacetime structures [55, 51, 85].

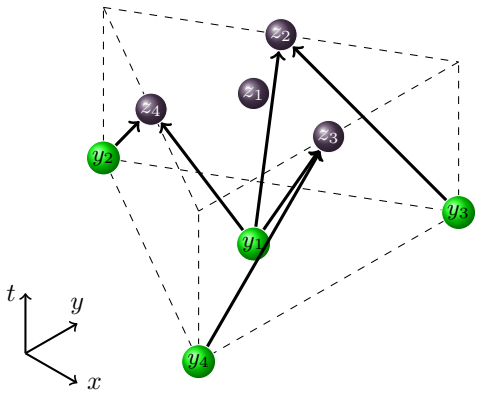
This chapter has reviewed quantum summoning and the generalized tasks. The next chapter presents protocols to accomplish these tasks based on a QEC code.

Chapter 4

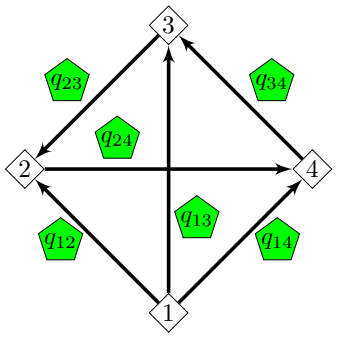
Efficient code for quantum summoning

This chapter presents an efficient QEC code to summon quantum information. For single-qubit summoning, we present a protocol based on a Calderbank-Shor-Steane code that decreases the space complexity for encoding by a factor of two compared to the previous best result and reduces the gate complexity from scaling as the cube to the square of the number of causal diamonds. Our protocol includes decoding whose gate complexity scales linearly with the number of causal diamonds. Our thorough framework for quantum summoning enables full specification of the protocol, including spatial and temporal implementation and costs, which enables quantum summoning to be a well-posed protocol for relativistic quantum communication purposes.

We specify the actions that the starting agent and each of the request and reveal agents perform to fulfill any summoning request in Sec. 4.1. The revised protocols for generalized quantum summoning tasks are provided in Sec. 4.2. For any valid configuration of causal diamonds, we propose a CSS code for the protocol of quantum summoning in Sec. 4.3. The encoding and decoding circuits of the CSS code are provided in Sec. 4.4. In Sec. 4.5, we show that the CSS code consumes fewer quantum resources than the CWS code [52].



(a)



(b)

Agent	Assigned qubits
A_{y_1}	q_{12}, q_{13}, q_{14}
A_{y_2}	q_{24}
A_{y_3}	q_{23}
A_{y_4}	q_{34}

(c)

Figure 4.1: (a) A configuration of four causal diamonds in $2+1$ dimensions. Three request points (y_2, y_3, y_4) are placed at the base vertices of an equilateral triangular prism and a fourth (y_4) is placed at the centroid of base vertices. The reveal points are placed at the midpoints of the top vertices (z_1, z_2, z_3) and the centroid of the top vertices. The volume of the diamond is not shown for visual clarity. The black arrows represent causal connections between points. (b) A complete graph representing the causal connections between the diamonds depicted in (a). For the CSS code the qubit q_{ij} is assigned to edge e_{ij}. (c) A table showing which requests agents is each physical qubit sent to.

4.1 Protocol for summoning

Here we propose a protocol using the CSS code (1.1) for summoning one qubit in any valid spacetime configuration. This CSS code assigns one qubit to each edge of the complete graph $K_{\tilde{N}}$; hence, the number of qubits used by the protocol is

$$Q = \binom{\tilde{N}}{2}, \tag{4.1}$$

for N and $\tilde{N}$ related according to Eq. (1.1).

For a spacetime configuration with an even number N of causal diamonds, $\tilde{N} := N$ and S employs the CSS code (1.1) to encode a qubit,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{4.2}$$

into Q (4.1) qubits and assigns each qubit to an edge of the complete graph $K_{\tilde{N}}$. The qubit assigned

to the edge e_{ij} is called q_{ij}, where e_{ij} denotes the edge connecting $\langle i \rangle$ to $\langle j \rangle$ for $i, j \in [N]$ and $i \neq j$,.

S sends q_{ij} to A_{y_i} if

$$y_i \prec z_j, \tag{4.3}$$

and to A_{y_j} if

$$y_j \prec z_i. \tag{4.4}$$

If A_{y_i} receives the summoning request, she sends all the qubits in her possession to A_{z_i}. Otherwise, she sends each qubit q_{ij} in her possession to A_{z_j}. As each vertex is adjacent to $N-1$ edges, any reveal agent, who receives the summoning request, receives $N-1$ qubits. Later, we prove that $\forall\, r \in [N] \coloneqq (1\,2\cdots N)$, the qubits

$$\{q_{rk}; k \in [N] \setminus \{r\}\} \tag{4.5}$$

can be used to decode $|\psi\rangle$ perfectly. Fig. (4.1) shows how the qubits are assigned to the request agents for a configuration of four causal diamonds.

In a configuration of an odd number of causal diamonds,

$$\tilde{N} \coloneqq N+1. \tag{4.6}$$

S introduces one more vertex

$\langle N{+}1 \rangle$

to obtain graph K_{N+1}. This new vertex can be seen as fictitious causal diamond causally related to every causal diamond, but the summoning request is never sent to this causal diamond. Then S employs the CSS code (1.1), which encodes $|\psi\rangle$ into $\binom{N+1}{2}$ qubits. As before, S sends each qubit q_{ij}, where $i, j \in [N]$, to A_{y_i} if

$$y_i \prec z_j, \tag{4.7}$$

and to A_{y_j} if

$$y_j \prec z_i. \tag{4.8}$$

S sends each additional qubit q_{jN+1} to reveal agent A_{z_j}. As in the even case, if A_{y_i} receives the summoning request, A_{y_i} sends all the qubits in her possession to A_{z_i}. Otherwise, she sends each qubit q_{ij} in her possession to A_{z_j}. Any reveal agent who receives the summoning request, ultimately receives N qubits to decode $|\psi\rangle$. For any $r \in [N+1]$, the qubits

$$\{q_{rk}; k \in [N+1] \setminus \{r\}\} \tag{4.9}$$

can be used to decode $|\psi\rangle$ perfectly.

This subsection has explained our protocol for quantum summoning. The next section explains how the quantum summoning protocol can be revised to accomplish generalized summoning tasks.

4.2 Protocols for generalized summoning

This protocol can also be used to accomplish a multi-request single-reveal summoning task. Corollary 1.1 implies that in a valid configuration for multi-request single-reveal summoning task, the causal diamonds are causally ordered. Denote A_{y_r} the earliest request agent, who receives a request. By following the above protocol, the reveal agent A_{z_r} receives the $N-1$ qubits if N is even and the N qubits if N is odd; hence, A_{z_r} can decode the state $|\psi\rangle$.

This protocol can also be amended, by adding preshared entangled Bell states and teleportation operations, to accomplish a quantum summoning task with unconstrained classical inputs [66]. To interpret how teleportation works in this revised protocol, we first consider the simplest nontrivial case, where for each pair (i, j), there are only two request points in S_{ij} and then use iteration to show that this revised protocol works in any valid configuration. Suppose $S_{ij} = \{y_p, y_q\}$ for $p, q \in [N]$, and A_{y_p} and A_{y_q} preshares n_p entangled Bell pairs with labels in $[n_p]$. When summoning begins, S sends the quantum share ρ_{ij} to A_{y_p}. When A_{y_p} receives a classical input m_p, A_{y_p} applies

Bell measurement on the combination of ρ_{ij} and the entangled state with label m_p and broadcast the measurement outcomes and the value of m_p. When A_{y_q} receives a classical input m_q, A_{y_q} sends the entangled state with label m, for every $m \in [n_p]$, to z_i if the pair of inputs (m, m_q) precludes z_j, and vise versa. This operation works as condition 3 in Corollary 1.2 indicates that any pair (m, m_q) must preclude at least one of z_i and z_j as the designated reveal point. A_{y_q} also broadcasts her value of m_q.

In such a way, if z_i or z_j is the designated reveal point, the corresponding reveal agent must receive the quantum state and classical information enough to reconstruct ρ_{ij}. Applying the above protocol for every pair of i and j guarantees that the designated reveal agent z_r can always receive enough information to prepare all the qubits in Eq. (4.5) and hence reconstruct $|\psi\rangle$. If there are more than two request points in S_{ij}, by iterating the above protocol for all the agents at request points in S_{ij}, the designated reveal agent must receive enough information to reconstruct ρ_{ij}. Thus, the revised protocol can accomplish quantum summoning task with unconstrained classical inputs for any valid configuration.

Again, this protocol can be revised to accomplish a localization task. In a localization task, Alice encodes state $|\psi\rangle$ into Q qubits. For each pair of spacetime regions Σ_i and Σ_j, where we suppose Σ_i causally precedes Σ_j, Alice sends ρ_{ij} to Σ_i. If Bob is not present in Σ_i, then Alice's agent in Σ_i sends ρ_{ij} to Σ_j. In this way, Bob in region Σ_r can always obtain all the $N-1$ qubits in Eq. (4.5), and thus reconstruct $|\psi\rangle$.

In both Subsecs. 4.1 and 4.2, we have discussed protocols based on a CSS code encoding one qubit into $\binom{\tilde{N}}{2}$ qubits. Subsection 4.3 provides the detail of the CSS code (1.1) used in our protocols.

4.3 The CSS code

In this subsection, we propose a stabilizer code with each qubit assigned to an edge of $K_{\tilde{N}}$. We show that it is an $\left[\left[\binom{\tilde{N}}{2}, 1, \frac{\tilde{N}}{2}\right]\right]$ CSS code, which can be used to summon a qubit by protocols in

Secs. 4.1 and 4.2.

Theorem 2. *The stabilizer code, specified by a*

$$\left[\binom{\tilde{N}}{2}-1\right]\times 2\binom{\tilde{N}}{2}$$

stabilizer generator matrix

$$\boldsymbol{H}_{\tilde{N}}=\left[\begin{array}{c|c} \boldsymbol{T}_{123} & \boldsymbol{0} \\ \boldsymbol{T}_{124} & \boldsymbol{0} \\ \vdots & \vdots \\ \boldsymbol{T}_{12\tilde{N}} & \boldsymbol{0} \\ \boldsymbol{T}_{134} & \boldsymbol{0} \\ \vdots & \vdots \\ \boldsymbol{T}_{1\tilde{N}-1\tilde{N}} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{A}_1+\boldsymbol{A}_2 \\ \boldsymbol{0} & \boldsymbol{A}_1+\boldsymbol{A}_3 \\ \vdots & \vdots \\ \boldsymbol{0} & \boldsymbol{A}_1+\boldsymbol{A}_{\tilde{N}-1} \end{array}\right], \tag{4.10}$$

where $\boldsymbol{0}$ *is an* $\binom{\tilde{N}}{2}$*-dimensional zero vector, is an* $\left[\left[\binom{\tilde{N}}{2},1,\frac{\tilde{N}}{2}\right]\right]$ *CSS code, which can correct erasure errors at qubits* q_{ij} *for* $i,j\in[N]\setminus\{r\}$ *for any* $r\in\left[\tilde{N}\right]$.

The stabilizer generator matrix (4.10) is analogous to the stabilizer generator matrix of the homological CV quantum error-correcting code [54]. By changing -1 to 1 in the stabilizer generator matrix of the CV code, one obtains the generator matrix (4.10) from the generator matrix of the CV code. In CV codes, ± 1 in the generator matrix represents the phase-space displacement operators $\mathrm{e}^{\pm \mathrm{i}\hat{q}}$ and $\mathrm{e}^{\pm \mathrm{i}\hat{p}}$, respectively. On the other hand, in the qubit code, 1 and 0 in the generator matrix represent Pauli operators Z and X, respectively.

To prove this theorem, we prove the following three lemmas.

Lemma 3. *$\boldsymbol{H}_{\tilde{N}}$ (4.10) is a stabilizer generator matrix of a CSS code, which encodes one qubit into $\binom{\tilde{N}}{2}$ qubits.*

Proof. From Eqs. (2.61) and (2.62),

$$\boldsymbol{T}_{1jk} \cdot (\boldsymbol{A}_1 + \boldsymbol{A}_l) = 0, \tag{4.11}$$

for any j, k, l such that $2 \leq j < k \leq \tilde{N}$ and $2 \leq l \leq \tilde{N} - 1$. Using Eq. (2.44), we know that all the stabilizer generators in $\boldsymbol{H}_{\tilde{N}}$ (4.10) commute with each other, thereby generating an Abelian subgroup $\mathcal{S}$ of $\mathcal{G}_{\binom{\tilde{N}}{2}}$. There are $\binom{\tilde{N}}{2} - 1$ independent stabilizer generators, so this stabilizer code encodes one qubit into $\binom{\tilde{N}}{2}$ qubits. The first $\binom{\tilde{N}-1}{2}$ stabilizer generators contain only Z operators and identities and the other $\tilde{N} - 2$ stabilizer generators contain only X operators and identities. Thus, the stabilizer code is a CSS code. □

In $\boldsymbol{H}_{\tilde{N}}$, the vectors representing the Z-type stabilizers and the X-type stabilizers span $\mathcal{C}_1^{\perp}$ (2.62) and $\mathcal{C}_2$ (2.64) for $n = \tilde{N}$ respectively. Thus, the CSS code in Theorem 2 is specified by the linear codes $\mathcal{C}_1$ (2.61) and $\mathcal{C}_2$ (2.64) for $n = \tilde{N}$.

Now we show that by assigning each of the $\binom{\tilde{N}}{2}$ physical qubits to an edge in $K_{\tilde{N}}$, this CSS code can correct the erasure errors at those qubits, which are not connected to vertex $\diamondsuit{r}$, for any $r \in [\tilde{N}]$. Hence, by following the protocol of quantum summoning in Sec. 4.1, no matter which A_{y_r} receives the request, the associated reveal agent A_{z_r} can decode the original state $|\psi\rangle$ from her $\tilde{N} - 1$ qubits in Eq. (4.5) or Eq. (4.9).

Lemma 4. *For any $r \in [\tilde{N}]$, the CSS code in Theorem 2 can correct erasure errors at qubits q_{ij} for $i, j \in [\tilde{N}] \setminus \{r\}$.*

Proof. Denote Ξ_r as the set of Pauli operators at qubits q_{ij} for $i, j \in [\tilde{N}] \setminus \{r\}$. For any Pauli operator $P \in \Xi_r$, its vector representation (2.42) is denoted

$$P = \begin{bmatrix} \boldsymbol{P}_Z & \boldsymbol{P}_X \end{bmatrix}. \tag{4.12}$$

As P acts nontrivially only at qubits q_{ij} for $i,j \in \left[\tilde{N}\right] \setminus \{r\}$,

$$\forall k \in \left[\tilde{N}\right] \setminus \{r\},\ \boldsymbol{P}_Z \cdot \boldsymbol{e}_{rk} = \boldsymbol{P}_X \cdot \boldsymbol{e}_{rk} = 0. \tag{4.13}$$

To show that the stabilizer code in Theorem 2 can correct any error in Ξ_r for every r, it is sufficient to prove that [46]

$$\forall P \in \Xi_r,\ P \in C(\mathcal{S}) \Rightarrow P \in \mathcal{S}, \tag{4.14}$$

where $\mathcal{S}$ is the stabilizer group generated by the stabilizer generators in $\boldsymbol{H}_{\tilde{N}}$ (4.10) and $C(\mathcal{S})$ is the centralizer of $\mathcal{S}$ in $\mathcal{G}_{\binom{\tilde{N}}{2}}$, i.e. the group of the Pauli operators commuting with all the elements of $\mathcal{S}$. Using Eq. (2.44), we know that $P \in C(\mathcal{S})$ if and only if

$$\forall \boldsymbol{v} \in \mathcal{C}_1^{\perp},\ \boldsymbol{P}_X \cdot \boldsymbol{v} = 0, \tag{4.15}$$

and

$$\forall \boldsymbol{u} \in \mathcal{C}_2,\ \boldsymbol{P}_Z \cdot \boldsymbol{u} = 0. \tag{4.16}$$

From $\boldsymbol{T}_{rij} \in \mathcal{C}_1^{\perp}$ and Eq. (4.15),

$$\boldsymbol{P}_X \cdot \boldsymbol{T}_{rij} = 0. \tag{4.17}$$

It implies that

$$\boldsymbol{P}_X \cdot (\boldsymbol{e}_{ri} + \boldsymbol{e}_{rj} + \boldsymbol{e}_{ij}) = 0. \tag{4.18}$$

Using Eq. (4.13), we know that

$$\boldsymbol{P}_X \cdot \boldsymbol{e}_{ij} = 0. \tag{4.19}$$

Equation (4.19), together with Eq. (4.13), implies that $\boldsymbol{P}_X = \boldsymbol{0}$.

Next we prove that Eq. (4.16) implies that $\boldsymbol{P}_Z \in \mathcal{C}_1^{\perp}$. Suppose

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_1 = 1. \tag{4.20}$$

Then Eq. (4.16) implies that for $2 \leq l \leq \tilde{N} - 1$,

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_l = 1. \tag{4.21}$$

As $\tilde{N}$ is even,

$$\sum_{m=1}^{\tilde{N}-1} \boldsymbol{P}_Z \cdot \boldsymbol{A}_m = 1. \tag{4.22}$$

As

$$\sum_{m=1}^{\tilde{N}} \boldsymbol{P}_Z \cdot \boldsymbol{A}_m = \boldsymbol{P}_Z \cdot \sum_{m=1}^{\tilde{N}} \boldsymbol{A}_m = 0, \tag{4.23}$$

we have

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_{\tilde{N}} = 1. \tag{4.24}$$

Hence,

$$\forall k \in \left[\tilde{N}\right], \boldsymbol{P}_Z \cdot \boldsymbol{A}_k = 1. \tag{4.25}$$

Equation (4.25) contradicts Eq. (4.13) because Eq. (4.13) implies that

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_r = 0. \tag{4.26}$$

Thus, (4.20) is false and

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_1 = 0. \tag{4.27}$$

Then Eq. (4.16) indicates that for $2 \leq l \leq \tilde{N} - 1$,

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_l = 0, \tag{4.28}$$

hence,

$$\sum_{m=1}^{\tilde{N}-1} \boldsymbol{P}_Z \cdot \boldsymbol{A}_m = 0. \tag{4.29}$$

From Eq. (4.23), we know that

$$\boldsymbol{P}_Z \cdot \boldsymbol{A}_{\tilde{N}} = 0. \tag{4.30}$$

Thus,

$$\forall k \in \left[\tilde{N}\right], \boldsymbol{P}_Z \cdot \boldsymbol{A}_k = 0, \tag{4.31}$$

which indicates that $\boldsymbol{P}_Z \in \mathcal{C}_1^{\perp}$. Since $\boldsymbol{P}_X = \mathbf{0}$, we know that P is a Z-type stabilizer in $\mathcal{S}$.

□

The proof is a modified version of that for the CV code [54] with the infinite-dimensional field $\mathbb{R}$ replaced by the finite-dimensional field $\mathbb{Z}_2$. One side effect of this modification is that $\tilde{N}$ has to be even. Lemma 4 is no longer true if $\tilde{N}$ is odd. To see this, we consider an example of a three-qubit code with stabilizer generators $\{ZZZ, IXX\}$. If $r = 3$, this code should correct any Pauli error at q_{12}. This is false, because the Pauli error at q_{12}, ZII, commutes with both stabilizer generators but does not lie in the stabilizer group.

Now we find the distance of the CSS code, which is an important parameter characterizing the capability of the code to detect and correct errors.

Lemma 5. *The distance of the CSS code in Theorem 2 is $\tilde{N}/2$.*

Proof. The distance of the stabilizer code in Theorem 2 equals to the minimum weight of the Pauli operators in $C(\mathcal{S}) \setminus \mathcal{S}$ [46]. To prove the minimum weight of the Pauli operators in $C(\mathcal{S}) \setminus \mathcal{S}$ is $\tilde{N}/2$, we first show that there exists a Pauli operator

$$P := \bigotimes_{i=1}^{\tilde{N}/2} Z_{q_{2i-1,2i}} \tag{4.32}$$

with weight $\tilde{N}/2$ such that $P \in C(\mathcal{S}) \setminus \mathcal{S}$. Then we show that no Pauli operator with weight less than $\tilde{N}/2$ lies in $C(\mathcal{S}) \setminus \mathcal{S}$.

From Eq (4.32), we know that

$$\boldsymbol{P}_Z = \sum_{i=1}^{\tilde{N}/2} \boldsymbol{e}_{2i-1,2i},\ \boldsymbol{P}_X = \boldsymbol{0}. \tag{4.33}$$

From Eq. (4.33), we find that

$$\forall\, l \in \left[\tilde{N}\right],\ \boldsymbol{P}_Z \cdot \boldsymbol{A}_l = 1; \tag{4.34}$$

hence,

$$\forall\, \boldsymbol{v} \in \mathcal{C}_2,\ \boldsymbol{P}_Z \cdot \boldsymbol{v} = 0. \tag{4.35}$$

From the fact that $\boldsymbol{P}_X = \boldsymbol{0}$, we know that P (4.32) commutes with all the stabilizers in $\mathcal{S}$, i.e., $P \in C(\mathcal{S})$. As $\boldsymbol{P}_Z$ cannot be represented by an Euclidean cycle,

$$\boldsymbol{P}_Z \notin \mathcal{C}_1^{\perp}. \tag{4.36}$$

Thus, $E \notin \mathcal{S}$, and hence

$$P \in C(\mathcal{S}) \setminus \mathcal{S}. \tag{4.37}$$

For any Pauli operator P' with weight less than $\tilde{N}/2$, there exists an $r \in \left[\tilde{N}\right]$ such that

$$\forall k \in \left[\tilde{N}\right] \setminus \{r\},\ \boldsymbol{P}'_Z \cdot \boldsymbol{e}_{rk} = \boldsymbol{P}'_X \cdot \boldsymbol{e}_{rk} = 0. \tag{4.38}$$

From the proof of Lemma 4, we know that

$$P' \in C(\mathcal{S}) \Rightarrow P' \in \mathcal{S}. \tag{4.39}$$

It implies that

$$P' \notin C(\mathcal{S}) \setminus \mathcal{S}. \tag{4.40}$$

Thus, no Pauli operator with weight less than $\tilde{N}/2$ lies in $C(\mathcal{S}) \setminus \mathcal{S}$.

□

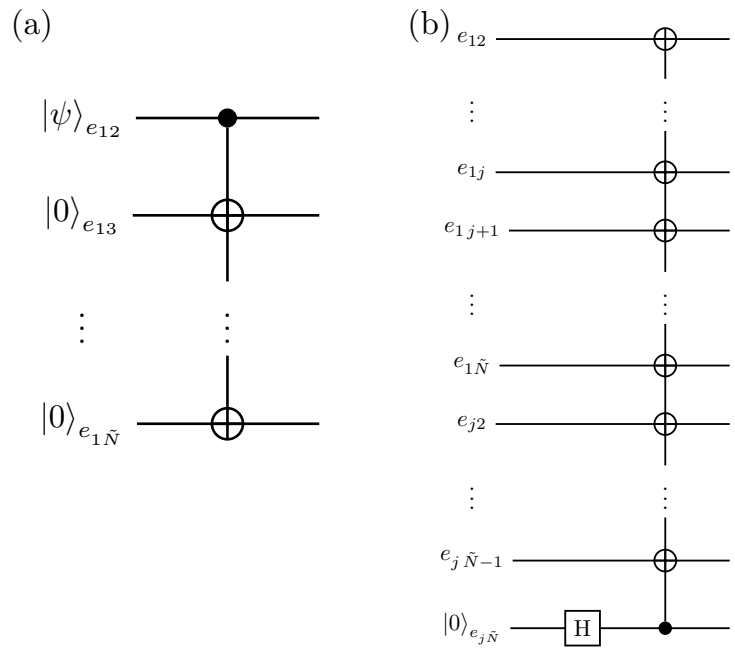


Figure 4.2: (a) Multiple CNOT gates with $|\psi\rangle_{e_{12}}$ as the control qubit and $\{|0\rangle_{e_{1i}}\}_{i=2}^{\tilde{N}}$ as the target qubits; (b) A Hadamard gate is applied at $|0\rangle_{e_{j\tilde{N}}}$ followed by multiple CNOT gates with $|0\rangle_{e_{j\tilde{N}}}$ as the control qubit and the qubits assigned to $\{e_{1l}\}_{l=[\tilde{N}],l\neq j} \cup \{e_{jk}\}_{k=2}^{\tilde{N}-1}$ as target qubits.

Lemma 5 implies that the CSS code can correct any $\left(\tilde{N}/2-1\right)$-qubit erasure errors. Although the distance of this CSS code scales as $O\left(\tilde{N}\right)$, Lemma 4 implies that the CSS code can correct particular erasure errors at $O\left(\tilde{N}^2\right)$ qubits.

This subsection has specified the CSS code (1.1) by its stabilizer generator matrix (4.10). We have shown the erasure errors that the CSS code, can correct and the distance of the CSS code. In the next subsection, we explain how to encode and decode this CSS code.

4.4 Encoding and decoding

In the last subsection, we have shown that the encoding of our CSS code employs $O(N^2)$ qubits while the decoding uses only $O(N)$ qubits. In this subsection, we present systematic methods to construct encoding and decoding circuits for our CSS code. The encoding method used here follows the standard method of encoding stabilizer codes [21], discussed in Subsec. 2.2.4. Our

decoding method differs from the stabilizer code decoding method because it only corrects erasure errors, which occur in summoning. We also calculate the gate complexity of both the encoding and the decoding circuits. It is shown that the gate complexity in the encoding is $O(N^2)$ and in the decoding is $O(N)$.

To build the encoding circuit of this CSS code, we introduce logical operations on the encoded state. By using the vector representation (2.42), the logical operations are

$$\bar{X} := \begin{bmatrix} \mathbf{0} & \boldsymbol{A}_1 \end{bmatrix} \tag{4.41}$$

and

$$\bar{Z} := \begin{bmatrix} \boldsymbol{A}_1 & \mathbf{0} \end{bmatrix}. \tag{4.42}$$

From $\boldsymbol{A}_1 \cdot \boldsymbol{A}_1 = 1$ and Eq. (2.44), $\bar{X}$ and $\bar{Z}$ anti-commute with each other.

We choose

$$|\psi_0\rangle = |\mathbf{0}\rangle := |0\rangle^{\binom{\tilde{N}}{2}}, \tag{4.43}$$

which is an eigenstate of $\bar{Z}$ with eigenvalue one. To encode $|\psi\rangle$ (4.2), using Eqs. (2.48) and (2.49), and the fact that Z-type stabilizers act trivially on $|\psi_0\rangle$, we obtain the encoded state

$$\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \prod_{j=2}^{\tilde{N}-1} \left(I + \bigotimes_{i=1}^{\binom{\tilde{N}}{2}} X^{(\boldsymbol{A}_1+\boldsymbol{A}_j)_i} \right) (\alpha|\mathbf{0}\rangle + \beta|\boldsymbol{A}_1\rangle), \tag{4.44}$$

where

$$|\boldsymbol{A}_1\rangle = \prod_{i=1}^{\binom{\tilde{N}}{2}} X^{(\boldsymbol{A}_1)_i} |\mathbf{0}\rangle, \tag{4.45}$$

and $(\boldsymbol{A}_1 + \boldsymbol{A}_j)_i$ and $(\boldsymbol{A}_1)_i$ are the i-th entries of vectors $\boldsymbol{A}_1 + \boldsymbol{A}_j$ and $\boldsymbol{A}_1$ respectively.

S applies CNOT gates as in Fig. 4.2(a) to the product state

$$|\psi\rangle \otimes |0\rangle^{\binom{\tilde{N}}{2}-1}, \tag{4.46}$$

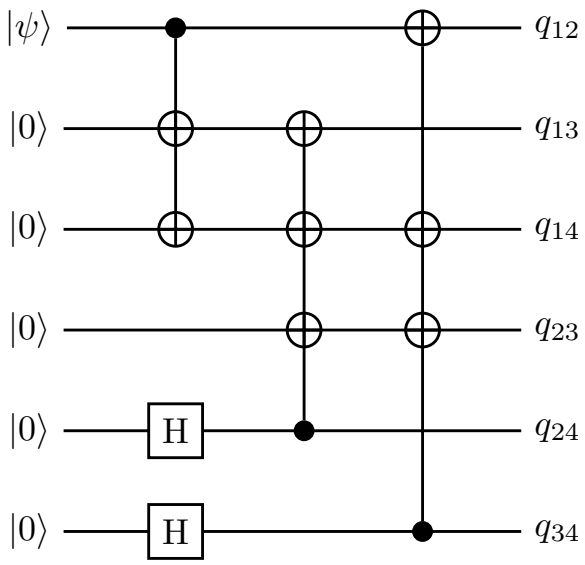


Figure 4.3: The encoding circuit of the CSS code comprising Hadamard gates and CNOT gates when $\tilde{N} = 4$. The inputs of this circuit are $|\psi\rangle \otimes |00000\rangle$ and the outputs of this circuit are the qubits assigned to each edge of the complete graph K_4 shown in Fig. 4.1(b).

to obtain

$$\alpha |\mathbf{0}\rangle + \beta |\boldsymbol{A}_1\rangle . \tag{4.47}$$

Then S implements each operation

$$I + \bigotimes_{i=1}^{m} X^{(\boldsymbol{A}_1 + \boldsymbol{A}_j)_i}, \tag{4.48}$$

where $1 \leq j \leq \tilde{N} - 2$, by using CNOT gates and a Hadamard gate as in Fig. 4.2(b). Finally, S obtains the encoded state (4.44). Figure 4.3 presents an example of the encoding circuit for $\tilde{N} = 4$.

The number of CNOT gates in Fig. 4.2(a) is $O(N)$. In Fig. 4.2(b), the number of CNOT gates is $O(N)$ and the number of Hadamard gate is one. As the circuit in Fig. 4.2(a) is only applied once and the circuit in Fig. 4.2(b) must be applied $O(N)$ times. The encoding of the CSS code consumes $O\left(N^2\right)$ CNOT gates and $O(N)$ Hadamard gates; hence, the number of qubits for the encoding of the CSS code is $O\left(N^2\right)$.

The decoding scheme is explained in the following. Suppose the designated reveal point is z_r. Reveal agent A_{z_r} cannot decode by measuring the syndromes as she has only $\tilde{N} - 1$ qubits. To

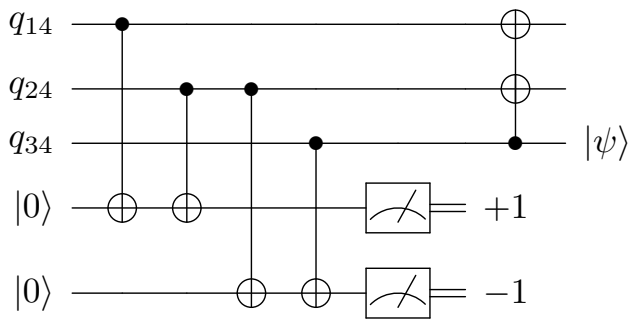


Figure 4.4: One example of the decoding circuit comprising CNOT gates and measurements of Z operators for $\tilde{N} = 4$. The inputs of the circuit are three physical qubits q_{14}, q_{24} and q_{34} and two ancillary qubits $|00\rangle$. The measurement outcomes on the two ancillary qubits are $+1$ and -1, based on which two CNOT gates are applied with the third qubit as the control qubit and the first two qubits as the target qubits. The third output qubit is the original qubit $|\psi\rangle$.

decode the original state $|\psi\rangle$ from the $\tilde{N}-1$ qubits with reduced density matrix ρ_r, which is obtained later in Eq. (4.61), reveal agent A_{z_r} measures the set of mutually commutative Hermitian operators

$$\left\{Z_{q_{rk}} Z_{q_{rk+1}}; k \in \left[\tilde{N}-1\right] \setminus \{r\}\right\}, \tag{4.49}$$

where $Z_{q_{rk}}$ represents the Z operator on the qubit q_{rk}. After applying the projective measurements, the reduced state is projected onto one codeword, becoming a pure state.

According to the measurement outcomes, by applying $\tilde{N}-2$ CNOT gates with one control qubit and distinct target qubits, A_{z_r} obtains the original state $|\psi\rangle$ at the control qubit. Fig. 4.4 presents an example of the decoding circuit when the request is received at $\langle 4 \rangle$. In decoding, the number of quantum gates is $O(N)$ and the number of single-qubit measurements is also $O(N)$.

Now let me calculate the reduced density matrix ρ_r and explain why this decoding works. From Eqs. (2.48) and (2.49),

$$|\bar{0}\rangle = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{x}\rangle, \tag{4.50}$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{2^{\tilde{N}-2}}} \sum_{\boldsymbol{x} \in \mathcal{C}_2} |\boldsymbol{A}_1 + \boldsymbol{x}\rangle, \tag{4.51}$$

form a basis of the CSS code in Theorem 2. The encoded state (4.44) is an equally weighted superposition of the codewords given in Eqs. (4.50) and (4.51). Hence, the density matrix of the $\binom{\tilde{N}}{2}$ physical qubits encoding $|\psi\rangle$ (4.2) is

$$\begin{aligned}\rho =& \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} (\alpha |\boldsymbol{x}\rangle + \beta |\boldsymbol{A}_1 + \boldsymbol{x}\rangle) \\ & \times \sum_{\boldsymbol{y}\in\mathcal{C}_2} (\alpha^* \langle \boldsymbol{y}| + \beta^* \langle \boldsymbol{A}_1 + \boldsymbol{y}|) . \end{aligned} \tag{4.52}$$

However, A_{z_r}only receives $\tilde{N}-1$ qubits, and the other qubits are lost. After tracing out the lost qubits, the reduced state ρ_r (4.61) becomes a mixture of the codewords.

To express the reduced density matrix, we give the following notations. The subset of edges connected to $\diamondsuit r$ in $K_{\tilde{N}}$ is denoted by E_r and the complement of E_r in E, i.e. the subset of edges not connected to $\diamondsuit r$, is denoted by E_r^c. In the same way as 2^{E_K} forms a linear space

$$\mathscr{E} \cong \mathbb{Z}_2^{\binom{\tilde{N}}{2}},$$

the power set 2^{E_r} forms a linear subspace

$$\mathscr{E}_r \cong \mathbb{Z}_2^{\tilde{N}-1} \tag{4.53}$$

and the power set $2^{E_r^c}$ forms the orthogonal complement of $\mathscr{E}_r$ in $\mathscr{E}$, denoted by

$$\mathscr{E}_r^{\perp} \cong \mathbb{Z}_2^{\binom{\tilde{N}-1}{2}}. \tag{4.54}$$

For a vector $\boldsymbol{v} \in \mathscr{E}$, we use $\boldsymbol{v}_r$ to denote the projection of $\boldsymbol{v}$ onto $\mathscr{E}_r$, and $\boldsymbol{v}_r^{\perp}$ to denote the projection of $\boldsymbol{v}$ onto $\mathscr{E}_r^{\perp}$.

Now we calculate the reduced density matrix ρ_r of the $\tilde{N}-1$ qubits $\left\{q_{rk}; k \in \left[\tilde{N}\right] \setminus \{r\}\right\}$. As

$$\forall r \in \left[\tilde{N}\right], \sum_{\boldsymbol{x}\in\mathcal{C}_2} |\boldsymbol{A}_r + \boldsymbol{x}\rangle = \sum_{\boldsymbol{x}\in\mathcal{C}_2} |\boldsymbol{A}_1 + \boldsymbol{x}\rangle, \tag{4.55}$$

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \mathrm{tr}_{E_r^c} \left[\sum_{\boldsymbol{x}\in\mathcal{C}_2} \left(\alpha \left|\boldsymbol{x}\right\rangle + \beta \left|\boldsymbol{A}_r + \boldsymbol{x}\right\rangle \right) \sum_{\boldsymbol{y}\in\mathcal{C}_2} \left(\alpha^* \left\langle\boldsymbol{y}\right| + \beta^* \left\langle\boldsymbol{A}_r + \boldsymbol{y}\right| \right) \right], \tag{4.56}$$

where $\mathrm{tr}_{E_r^c}$ denotes the partial trace over the qubits $\left\{q_{ij}; i,j \in \left[\tilde{N}\right] \setminus \{r\}\right\}$. From the definition of partial trace [88],

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{v}\in\mathscr{C}_r^\perp} \left\langle \boldsymbol{v} \right| \sum_{\boldsymbol{x}\in\mathcal{C}_2} \left(\alpha \left|\boldsymbol{x}\right\rangle + \beta \left|\boldsymbol{A}_r + \boldsymbol{x}\right\rangle \right) \sum_{\boldsymbol{y}\in\mathcal{C}_2} \left(\alpha^* \left\langle\boldsymbol{y}\right| + \beta^* \left\langle\boldsymbol{A}_r + \boldsymbol{y}\right| \right) \left| \boldsymbol{v} \right\rangle. \tag{4.57}$$

For each $\boldsymbol{v} \in \mathscr{C}_r^\perp$, there is at most one $\boldsymbol{x} \in \mathcal{C}_2$ such that

$$\boldsymbol{x}_r^\perp = \boldsymbol{v}; \tag{4.58}$$

hence, we get

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} \left\langle \boldsymbol{x}_r^\perp \right| \left(\alpha \left|\boldsymbol{x}\right\rangle + \beta \left|\boldsymbol{A}_r + \boldsymbol{x}\right\rangle \right) \left(\alpha^* \left\langle\boldsymbol{x}\right| + \beta^* \left\langle\boldsymbol{A}_r + \boldsymbol{x}\right| \right) \left| \boldsymbol{x}_r^\perp \right\rangle. \tag{4.59}$$

As

$$\left\langle \boldsymbol{x}_r^\perp \right| \left.\boldsymbol{x}\right\rangle = \left|\boldsymbol{x}_r\right\rangle \text{ and } \left\langle \boldsymbol{x}_r^\perp \right| \left.\boldsymbol{A}_r + \boldsymbol{x}\right\rangle = \left|\mathbf{1} + \boldsymbol{x}_r\right\rangle, \tag{4.60}$$

where $\mathbf{1}$ is an $(\tilde{N}-1)$-dimensional vector with all the entries equal to 1,

$$\rho_r = \frac{1}{2^{\tilde{N}-2}} \sum_{\boldsymbol{x}\in\mathcal{C}_2} \left(\alpha \left|\boldsymbol{x}_r\right\rangle + \beta \left|\mathbf{1} + \boldsymbol{x}_r\right\rangle \right) \left(\alpha^* \left\langle\boldsymbol{x}_r\right| + \beta^* \left\langle\mathbf{1} + \boldsymbol{x}_r\right| \right). \tag{4.61}$$

$\forall \boldsymbol{x} \in \mathcal{C}_2$, $\left|\boldsymbol{x}_r\right\rangle$ and $\left|\mathbf{1} + \boldsymbol{x}_r\right\rangle$ are the eigenstates of each parity-check operator in (4.49) with same eigenvalue, so any linear combination

$$\alpha \left|\boldsymbol{x}_r\right\rangle + \beta \left|\mathbf{1} + \boldsymbol{x}_r\right\rangle$$

is a common eigenstate of the Hermitian operators (4.49), with the eigenvalues forming a vector

consisting of ± 1. For

$$\forall \boldsymbol{x}, \boldsymbol{z} \in \mathcal{C}_2 \text{ and } \boldsymbol{x} \neq \boldsymbol{z}, \tag{4.62}$$

the two eigenstates

$$\alpha \left| \boldsymbol{x}_r \right\rangle + \beta \left| \mathbf{1} + \boldsymbol{x}_r \right\rangle \tag{4.63}$$

and

$$\alpha \left| \boldsymbol{z}_r \right\rangle + \beta \left| \mathbf{1} + \boldsymbol{z}_r \right\rangle \tag{4.64}$$

have different eigenvalue vectors. This is because if (4.63) and (4.64) have the same eigenvalues, then either $\boldsymbol{x}_r = \boldsymbol{z}_r$ or $\boldsymbol{x}_r = \boldsymbol{z}_r + \mathbf{1}$, both of which contradict condition (4.62). Thus, ρ_r in Eq. (4.61) is an equally weighted mixture of the common eigenstates of the Hermitian operators (4.49) with different eigenvalue vectors.

After the projective measurements on all the Hermitian operators (4.49), the reduced state is projected onto

$$\alpha \left| \boldsymbol{y}_r \right\rangle + \beta \left| \mathbf{1} + \boldsymbol{y}_r \right\rangle, \tag{4.65}$$

where $\boldsymbol{y} \in \mathcal{C}_2$ and $\boldsymbol{y}_r$ is the projection of $\boldsymbol{y}$ onto $\mathscr{E}_r$. The corresponding measurement outcomes are $\left\{ (-1)^{\boldsymbol{y}_r^{(i)} + \boldsymbol{y}_r^{(i+1)}}; i \in \left[\tilde{N} - 2 \right] \right\}$, where $\boldsymbol{y}_r^{(i)}$ is the i-th component in $\boldsymbol{y}_r$. (4.65) is the state after the measurements of the Hermitian operators in (4.49).

4.5 Comparison with the CWS code

Now we compare the quantum resources required by our CSS code with Hayden and May's CWS code [52]. For any N causal diamonds, Hayden and May propose a $\left(\left(2\binom{N}{2}, 2 \right) \right)$ CWS code to summon a qubit. This $\left(\left(2\binom{N}{2}, 2 \right) \right)$ CWS code is specified by a graph-state stabilizer represented by a graph $\mathscr{G}_{\text{CWS}}$ and two word operators

$$\left\{ I, Z^{\otimes N(N-1)} \right\}. \tag{4.66}$$

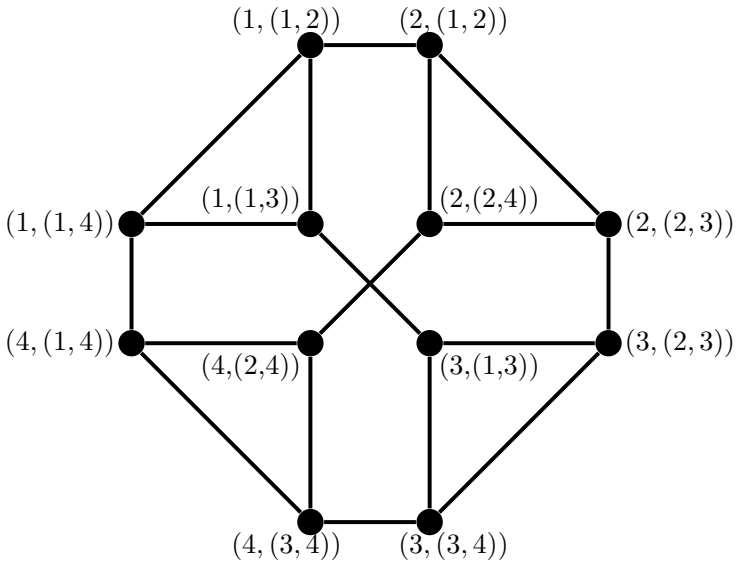


Figure 4.5: $\mathscr{G}_{\text{CWS}}$ for $N = 4$. Each vertex of $\mathscr{G}_{\text{CWS}}$ is labeled by $(j,(j,k))$ for $1 \leq j,k \leq 4$ and $k \neq j$. Each $(j,(j,k))$ is adjacent to $(k,(j,k))$ and $(j,(j,l))$, where $1 \leq l \leq 4$ and $l \neq j$ or k.

Given an N-vertex complete graph $K_N = \{V_K, E_K\}$, $\mathscr{G}_{\text{CWS}}$ is the line graph [35] of $\mathscr{G}' := \{V', E'\}$, where

$$V' = V_K \cup E_K, \tag{4.67}$$

and

$$E' = \{(v,(v,w)); v \in V_K, (v,w) \in E_K\}. \tag{4.68}$$

Figure 4.5 presents $\mathscr{G}_{\text{CWS}}$ for $N = 4$. This CWS code can be used to summon one qubit in four causal diamonds [52] by employing twelve qubits.

To investigate the complexity of the encoding of the CWS code, we need to know the complexity of preparing graph state $|\mathscr{G}_{\text{CWS}}\rangle$. From Eq. (2.67), we know that the number of controlled-Z gates and Hadamard gates in preparing a graph state equals to the number of edges and vertices in the graph, respectively. The numbers of edges and vertices in $\mathscr{G}_{\text{CWS}}$ are

$$|E(\mathscr{G}_{\text{CWS}})| = \frac{N(N-1)^2}{2}, \tag{4.69}$$

$$|V(\mathscr{G}_{\text{CWS}})| = N(N-1). \tag{4.70}$$

Thus, preparing $|\mathscr{G}_{\mathrm{CWS}}\rangle$ requires $O\left(N^3\right)$ controlled-Z gates and $O\left(N^2\right)$ Hadamard gates. Applying the codeword operators (4.66) requires additional $O\left(N^2\right)$ controlled-Z gates.

In conclusion, the encoding of the CWS code consumes $O\left(N^3\right)$ controlled-Z gates and $O\left(N^2\right)$ Hadamard gates. Compared with the CWS code, our CSS code reduces the number of quantum gates for encoding from $O\left(N^3\right)$ to $O\left(N^2\right)$.

Our protocol employs a CSS code to summon quantum information in any valid configuration. The CSS code can correct the erasure errors that occur in the quantum summoning task and also the generalized summoning tasks. The encoding and the decoding methods for this CSS code have been presented. Finally, we have compared the complexity of the encoding of the CSS code with the encoding of the CWS code and found that our CSS code is more efficient.

4.6 Discussion

We have presented a protocol to summon quantum information efficiently in any valid configuration of causal diamonds. Central to our protocol is a CSS code that encodes one logical qubit into $O(N^2)$ physical qubits, where each physical qubit is assigned to an edge of a complete graph whose vertices correspond to causal diamonds. This code is a qubit version of the homological CV quantum error correcting code [54]. The CSS code is designed using the fact that the power set of edges of a complete graph can be cast as a vector space. The stabilizer generators of the CSS code correspond to triangle graphs and sums of star graphs.

The properties of these graphs are used to show that the logical qubit can be decoded from the subset of physical qubits that are assigned to edges adjacent to any vertex. To employ this code for summoning, the physical qubits are sent to the request points in such a way that the past of every reveal point contains enough physical qubits to decode the original qubit. Our protocol design, similar to one used previously [54], ensures that whenever a request agent receives the request the associated reveal agent receives all physical qubits required to decode the original qubit.

We also present procedures to design the encoding and decoding circuits for the CSS code. We

show that our protocol is less resource-intensive than the protocol based on the CWS code [52] which uses circuits that are $O(N^2)$ wide and $O(N^3)$ deep. The circuits for the CSS code have width that is also $O(N^2)$ but half that of the CWS code and require only $O(N^2)$ gates.

4.7 Conclusion

Our protocol for summoning is designed to work for any valid configuration of causal diamonds, where the underlying CSS code depends only on the number of causal diamonds. It is likely that codes can be designed that reduce resource usage by exploiting the structure of causal connections between the causal diamonds, examples being when a single causal curve connects multiple causal diamonds [54] or when the graph representing causal connections is acyclic [2].

While any given configuration of causal diamonds may be realized in man-made quantum networks, a useful avenue of research would be to classify the configurations that can occur naturally in flat or curved spacetimes. Our codes as well as other codes for quantum summoning assume that entangled states may be transferred without decoherence in spacetime. Quantum summoning in curved spacetime or Rindler coordinates might require the usage of codes that protect against decoherence caused due to gravity or acceleration [8, 42, 6].

Chapter 5

Relativistic quantum secret sharing

In quantum secret sharing protocols, the usual presumption is that the distribution of quantum shares and players' collaboration are both performed inertially. In this chapter, we develop a quantum secret sharing protocol that relaxes these assumptions wherein we consider the effects due to the accelerating motion of the shares. Specifically, we solve the $(2,3)$-threshold CV quantum secret sharing in non-inertial frames. To this aim, in Sec. 5.1, we formulate the effect of relativistic motion on the quantum field inside a cavity as a bosonic quantum Gaussian channel. In Sec. 5.2, we investigate how the fidelity of quantum secret sharing is affected by the non-uniform motion of the quantum shares. Furthermore, we fully characterize the canonical form of the Gaussian channel which can be utilized in quantum information processing protocols to include relativistic effects.

5.1 Methods

In this section, we employ the framework of Gaussian quantum information [116, 1] to write the evolution of the quantum field inside the cavity in a BBB, as depicted in Fig. 2.3, as a Gaussian quantum channel. We use this channel, in Section 5.2, to study the effect of non-inertial motion of the shares on the fidelity of the quantum secret sharing. Moreover, we characterize the canonical form of the channel and show that it is a thermal lossy channel.

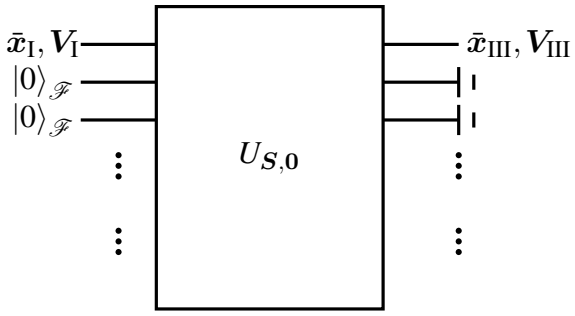


Figure 5.1: The BBB is depicted for the case wherein the first mode of the cavity is used to encode and decode quantum information. We assume all the other modes are initially prepared in vacuum and after the BBB, which is represented by the Gaussian unitary operation $U_{\boldsymbol{S},\mathbf{0}}$, the rest of the modes are ignored.

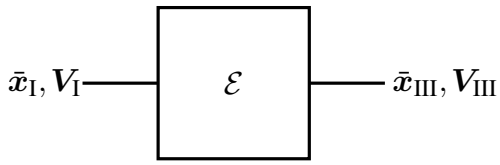


Figure 5.2: The operations performed in Fig. 5.1 are all Gaussian operations, which enables us to express the BBB as a Gaussian channel $\mathcal{E}$ acting on the first and second moments.

In Fig. 5.2, we have depicted the scenario wherein all the modes of the cavity are prepared in the vacuum state except mode k, which is prepared in a Gaussian state with first and second moments $\bar{\boldsymbol{x}}_{\mathrm{I}}$ and $\boldsymbol{V}_{\mathrm{I}}$ respectively. First, the initial state of the cavity evolves through the Gaussian unitary operation with symplectic transformation $\boldsymbol{S}$ and subsequently all the modes except mode k are traced out. As both the Gaussian unitary operation and the tracing operation preserve the Gaussianity of a quantum state, the BBB can be written as a Gaussian channel. Hence, using Eqs. (2.102), (2.103), (2.159) and (2.160), the matrices $\boldsymbol{M}$ and $\boldsymbol{N}$ for mode k read as

$$\boldsymbol{M}_{kk} = \begin{bmatrix} \mathrm{Re}\,(\alpha_{kk} - \beta_{kk}) & \mathrm{Im}\,(\alpha_{kk} + \beta_{kk}) \\ -\mathrm{Im}\,(\alpha_{kk} - \beta_{kk}) & \mathrm{Re}\,(\alpha_{kk} + \beta_{kk}) \end{bmatrix}, \tag{5.1}$$

$$\boldsymbol{N}_k = \sum_{n \neq k} \boldsymbol{M}_{nk} \boldsymbol{M}_{nk}^{\top}. \tag{5.2}$$

We are interested in the final quantum state up to third order in h, which means that we only

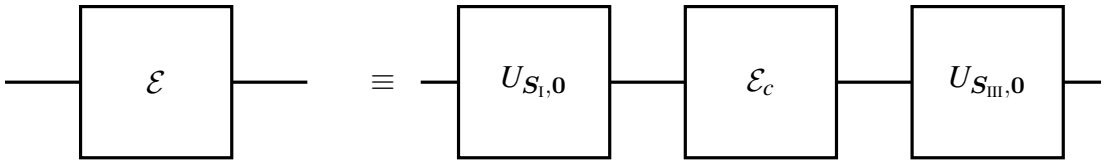


Figure 5.3: The canonical form of the BBB Gaussian channel, $\mathcal{E}$, which is decomposed into its canonical form, $\mathcal{E}_c$, up to two Gaussian unitary operations in regions I and III with symplectic transformations, i.e., $\boldsymbol{S}_{\rm I}$ and $\boldsymbol{S}_{\rm III}$.

need the matrices in Eqs. (5.1) and (5.2) up to (but not including) third order in h; i.e.,

$$
\begin{aligned}
\boldsymbol{M}_{kk} &= \boldsymbol{M}_{kk}^{(0)} + \boldsymbol{M}_{kk}^{(2)} h^2 + O(h^3), \\
\boldsymbol{N}_k &= \boldsymbol{N}_k^{(2)} h^2 + O(h^3), \\
\boldsymbol{N}_k^{(2)} &= \sum_{n\neq k} \boldsymbol{M}_{nk}^{(1)} \boldsymbol{M}_{nk}^{(1)\top}, \\
\boldsymbol{M}_{kk}^{(0)} &= \begin{bmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{bmatrix}, \phi = \tilde{\omega}_k \tau \\
\boldsymbol{M}_{nk}^{(0)} &= \boldsymbol{M}_{kk}^{(1)} = 0 \ (n \neq k), \\
\boldsymbol{M}_{nk}^{(i)} &= \begin{bmatrix} \mathrm{Re}\left(\alpha_{nk}^{(i)} - \beta_{nk}^{(i)}\right) & \mathrm{Im}\left(\alpha_{nk}^{(i)} + \beta_{nk}^{(i)}\right) \\ -\mathrm{Im}\left(\alpha_{nk}^{(i)} - \beta_{nk}^{(i)}\right) & \mathrm{Re}\left(\alpha_{nk}^{(i)} + \beta_{nk}^{(i)}\right) \end{bmatrix},
\end{aligned}
\tag{5.3}
$$

where in the last matrix $i = 1, 2$. We emphasize that as we are estimating the effect of the Gaussian channel up to third order in h, the term $\boldsymbol{M}_{kk}^{(2)} \boldsymbol{V}_{\rm I} \boldsymbol{M}_{kk}^{(2)\top}$ is to be ignored.

As was discuss in Subsec. 2.4.4, any Gaussian quantum channel can be decomposed into its canonical. This means that we can decompose the Gaussian channel for the BBB as shown in Fig. 5.3. Here, $\boldsymbol{S}_{\rm I}$ and $\boldsymbol{S}_{\rm III}$ are two symplectic transformations in the region I and III, which correspond to the two Gaussian unitary operators. We use $\boldsymbol{M}_c$ and $\boldsymbol{N}_c$ for the canonical form of the channel, $\mathcal{E}_c$, as opposed to the channel $\mathcal{E}$ for which we have used $\boldsymbol{M}$ and $\boldsymbol{N}$.

In transforming a Gaussian quantum channel $\mathcal{E}$ to its canonical form $\mathcal{E}_c$, some properties of the

channel remain invariant up to Gaussian unitary operations $U_{\boldsymbol{S}_{\mathrm{I},\mathbf{0}}}$ and $U_{\boldsymbol{S}_{\mathrm{III},\mathbf{0}}}$. The first invariant, in our case, is $\mathscr{R} = 2$. Using the fact that $\det\left(\boldsymbol{M}_{kk}^{(0)} + \boldsymbol{M}_{kk}^{(2)} h^2\right) = 1 + \operatorname{tr} \boldsymbol{M}_{kk}^{(2)} h^2$ and Eq. (2.129), the second invariant is the transmissivity,

$$\zeta = \det \boldsymbol{M}_{kk} = 1 - \zeta_k^{(2)} h^2 + O(h^3), \tag{5.4}$$

where

$$\zeta_k^{(2)} := 2\left(f_{\alpha,k} - f_{\beta,k}\right).$$

As $\zeta^{(2)}$ increases, the transmissivity decreases.

The final invariant is thermal number $\bar{n}$ associated to the canonical form of the quantum channel $\mathcal{E}$. We calculate the leading order term of $\bar{n}$, which is

$$\bar{n} := \frac{\sqrt{\det \boldsymbol{N}}}{2|1-\zeta|} - \frac{1}{2} = \frac{\sqrt{\left(f_{\alpha,k} + f_{\beta,k}\right)^2 - 4\left|g_{\alpha\beta,k}\right|^2}}{2\left(f_{\alpha,k} - f_{\beta,k}\right)} - \frac{1}{2}, \tag{5.5}$$

where $g_{\alpha\beta,k} := \sum_{n\neq k} \alpha_{nk}^{(1)} \beta_{nk}^{(1)}$.

The main advantage of working with the canonical form of the BBB channel is that we can completely characterize it. For the Gaussian-unitary invariants, we find $\zeta \in (0,1)$ and $\mathscr{R} = 2$, from which we can conclude that the canonical form of the BBB channel is a lossy Gaussian channel. The channel is lossy due to the fact that its transmissivity is smaller than one; i.e., $\zeta < 1$. Furthermore, from this analyses, we conclude that the quantum channel $\mathcal{E}_c$ can be simulated by interacting mode k of the cavity and a thermal state with mean photon number $\bar{n}$ (5.5) via a beam splitter of transmittance ζ.

In this section, we employed the framework of Gaussian channels to find matrices $\boldsymbol{M}$ and $\boldsymbol{N}$ in (2.189) for a BBB ($\boldsymbol{d} = \mathbf{0}$). From this point on, we use them to include the effect of relativity on the quantum field inside a cavity while the cavity moves non-inertially. Moreover, we computed

the channel invariants, transmissivity and the average number of thermal particles, which enabled us to identify the BBB as a thermal lossy channel.

5.2 The relativistic protocol

In this section, we present the relativistic variant of (2,3)-threshold CV quantum secret sharing. We first include the effect of acceleration on the distribution of quantum shares and then we consider different possible collaboration scenarios between the players. In each case, we show that the fidelity of quantum secret sharing is reduced, except for a thermal state, when compared to the non-relativistic scenarios.

5.2.1 Distribution of quantum shares

In our case, modes 1, 2, and 3 are three quantum Gaussian shares and each mode corresponds to a mode in a cavity. The Gaussian state of each quantum share occupies one single mode inside each cavity, and the other modes inside each cavity are all in vacuum states. The three quantum shares are distributed to the three players.

After encoding using the scheme shown in Fig. 2.4, the dealer transports the three cavities to the three players. Fig. 5.4 shows the distribution of the quantum shares. The three players are located at different spacetime points. One player (Player 3) is at the same spatial position as the dealer and the other two players (Players 1 and 2) have the same distance to the dealer[1]. The dealer and three players are relatively static, so they share an inertial frame. As depicted in Fig. 5.4, Cavities 1 and 3 inevitably need to be accelerated and then decelerated to reach the spacetime regions of Players 1 and 3 respectively. Using the quantum channel derived in Sec. 5.1, we consider the effect of such a non-uniform motion of the cavities on the quantum share, which is encoded in a single mode of each cavity. In this scenario, Cavity 3 remains static during the whole distribution.

[1]To simplify the calculations, we have chosen the symmetric configuration of the players and the dealer, Fig. 5.4, which suffices to study the relativistic effects in the distribution stage.

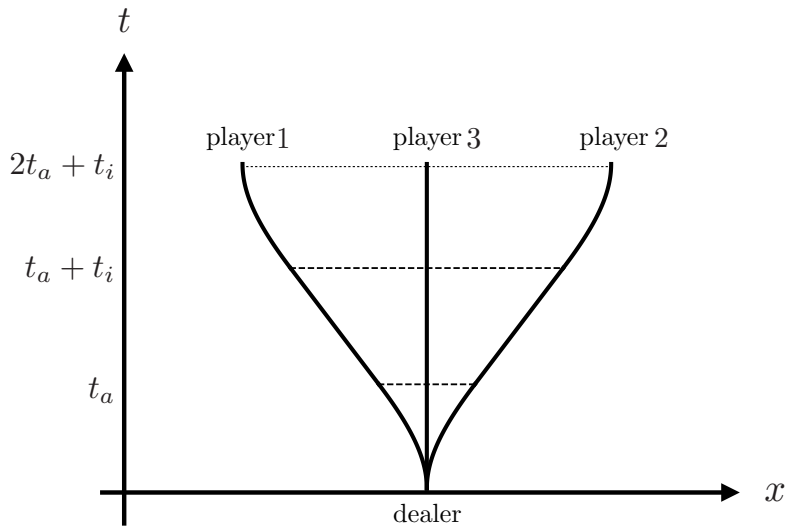


Figure 5.4: The worldlines of the quantum cavities during transportation. From $t = 0$ to $t = t_a$, the two cavities, represented by the furthest left and the furthest right worldlines, accelerate with the proper acceleration a in two opposite directions. From $t = t_a$ to $t = t_a + t_i$, they move with constant velocities. From $t = t_a + t_i$ to $t = 2t_a + t_i$, the two cavities decelerate with the proper acceleration a and become stationary. The cavity represented by the middle world line remains static.

Here the cavities can be either optical cavities or microwave resonators, depending on the resonance frequency, with low internal losses. To distribute the three quantum shares into three distinct cavities, the dealer couples a waveguide, guiding a TEM wave encoding one quantum share, with one mirror of a cavity. After the dealer turns off the coupling, he sends these cavities to the three players. To readout the information in a cavity, players, couple a waveguide with one partially transmitting mirror of each cavity and transmit the output to the measurement setup shown in Fig. 5.5 (a) or Fig. 5.10 (a).

5.2.2 Players' collaboration

After the quantum shares are distributed between the three players, two of them need to collaborate to decode the quantum secret. Three different scenarios are possible; Players 1 and 3, 2 and 3, or 1 and 2 can constitute the subset of collaborating players. The effect of acceleration on the fidelity of quantum secret sharing in the latter two cases is the same (due to the present symmetry), and we only consider the scenario wherein Players 2 and 3 collaborate.

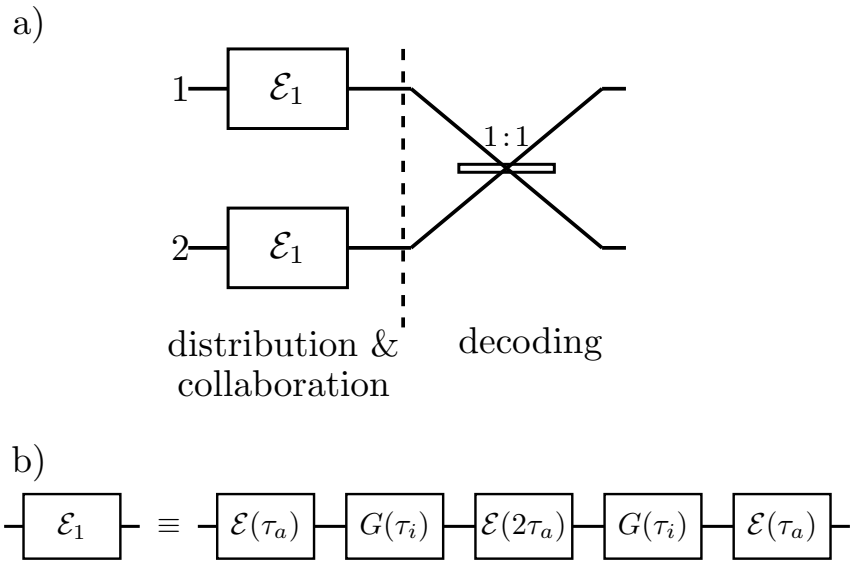


Figure 5.5: (a) The thermal lossy channel $\mathcal{E}_1$ is the Gaussian channel that represents the total evolution of the first and the second quantum shares during the distribution and the collaboration stage. Then the quantum secret is decoded using a balanced beam splitter. (b) $\mathcal{E}_1$ is a single-mode Gaussian channel composed of five Gaussian channels in series. $\mathcal{E}(\tau_a)$ is the Gaussian channel for a BBB during the proper time τ_a and $G(\tau_i)$ represents the Gaussian channel of the free evolution in an inertial frame with proper time τ_i.

Collaboration between Players 1 and 2

First, we consider the case wherein Players 1 and 2 are collaborating. To decode the quantum secret, their cavities are transported to the same spacetime point as shown in Fig. 5.6. After the two cavities are in the same position, the quantum secret is decoded by beam splitting the two modes that were employed to encode the quantum secret. From $t = 2t_a + t_i$ to $t = 4t_a + 2t_i$, each mode of the two-mode Gaussian state goes through the same single-mode Gaussian channel $\mathcal{E}_1$ as shown in Fig. 5.5.

The Gaussian quantum channel $\mathcal{E}_1$ is composed of five Gaussian channels in series (See Fig. 5.5(b)). The channel $\mathcal{E}(\tau_a)$ corresponds to uniformly accelerated motion of the cavity to the left (or to the right) during the proper time τ_a, while the channel $\mathcal{E}(2\tau_a)$ represents the cavity moving with con-

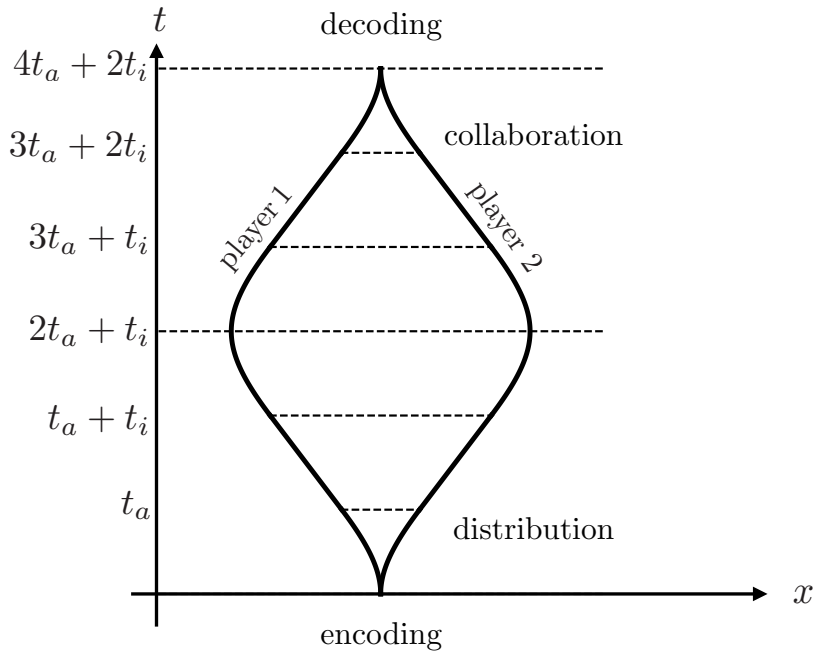


Figure 5.6: The two curves represent two worldlines in spacetime. Each worldline is the trajectory of one cavity carrying a quantum share. From $t = 2t_a + t_i$ to $t = 3t_a + t_i$, the two cavities accelerate with proper acceleration a towards each other. From $t = 3t_a + t_i$ to $t = 3t_a + 2t_i$, the two cavities are moving with constant velocity. From $t = 3t_a + 2t_i$ to $t = 4t_a + 2t_i$, the two cavities decelerate with proper acceleration a to arrive at the same spacetime point.

stant proper acceleration to the right (or to the left) during the proper time $2\tau_a$. Also, the quantum channel $G(\tau_i)$ corresponds to the inertial movement of the cavity with constant velocity for the proper time τ_i. Using (5.3), the first and second moments of the k-th mode of the cavity, up to third order in h, are transformed as

$$\bar{\boldsymbol{x}} \xmapsto{\mathcal{E}(\tau_a)} \left(M_{\phi_a}^{(0)} + M_{kk}^{(2)} h^2\right) \bar{\boldsymbol{x}}, \tag{5.6}$$

$$\begin{aligned} \boldsymbol{V} \xmapsto{\mathcal{E}(\tau_a)} & M_{\phi_a}^{(0)} \boldsymbol{V} M_{\phi_a}^{(0)\top} \\ & + \left(M_{\phi_a}^{(0)} \boldsymbol{V} M_{kk}^{(2)\top} + M_{kk}^{(2)} \boldsymbol{V} M_{\phi_a}^{(0)\top}\right) h^2 + N_k^{(2)} h^2, \end{aligned} \tag{5.7}$$

where $M_{\phi_a}^{(0)}$, $M_{kk}^{(2)}$, and $N_k^{(2)}$ are given in (5.3).

The Gaussian channel $G(\tau_i)$ represents the free evolution of the Gaussian state during the inertial movement of the cavity in proper time τ_i,

$$\bar{\boldsymbol{x}} \xmapsto{G(\tau_i)} M_{\phi_i}^{(0)} \bar{\boldsymbol{x}}, \tag{5.8}$$

$$\boldsymbol{V} \xmapsto{G(\tau_i)} M_{\phi_i}^{(0)} \boldsymbol{V} M_{\phi_i}^{(0)\top}, \tag{5.9}$$

where

$$M_{\phi_i}^{(0)} = \begin{bmatrix} \cos\phi_i & -\sin\phi_i \\ \sin\phi_i & \cos\phi_i \end{bmatrix},$$

and $\phi_i = \frac{k\pi\tau_i}{L}$ is the phase accumulated during the free evolution from $t = t_a$ to $t = t_a + t_i$, and from $t = 3t_a + t_i$ to $t = 3t_a + 2t_i$. To simplify the later calculations, we suppose the phase shift during the inertial movement is $\phi_i = \pi - 2\phi_a$.

Therefore, we can express the collaboration between Players 1 and 3, shown in Fig. 5.6, as the

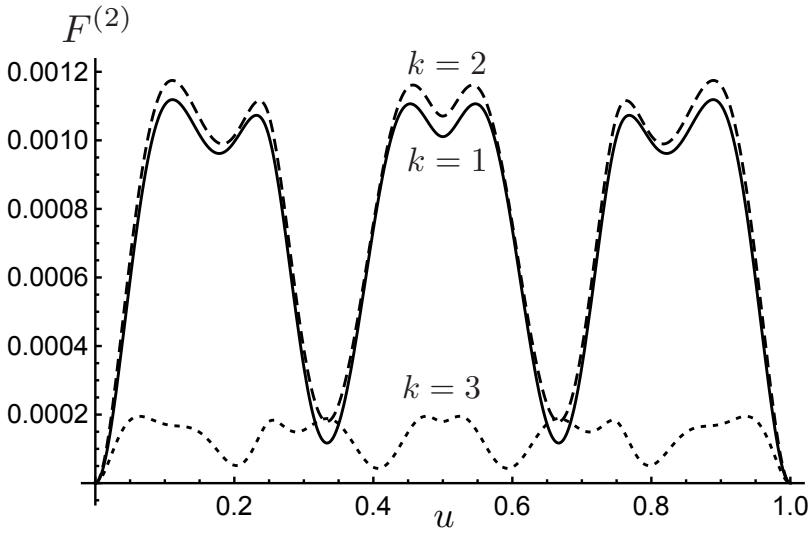


Figure 5.7: $F^{(2)}$ as a function of u for modes $k = 1$ (solid), 2 (dashed), and 3 (dotted) when the secret Gaussian state is a coherent state.

Gaussian channel $\mathcal{E}_1$,

$$\mathcal{E}_1 := \mathcal{E}(\tau_a) \circ G(\tau_i) \circ \mathcal{E}(2\tau_a) \circ G(\tau_i) \circ \mathcal{E}(\tau_a). \tag{5.10}$$

If the secret Gaussian state is a coherent state and the free evolution is ignored; i.e., $M^{(0)} = \mathbb{I}$, the Gaussian transformation of the channel $\mathcal{E}_1$ for the mode k is

$$\bar{\boldsymbol{x}} \overset{\mathcal{E}_1}{\longmapsto} \bar{\boldsymbol{x}} + (2M^{(2)}_{kk,\tau_a} + M^{(2)}_{kk,2\tau_a})h^2\bar{\boldsymbol{x}}, \tag{5.11}$$

$$\begin{aligned}\mathbb{I} \overset{\mathcal{E}_1}{\longmapsto} \mathbb{I} + \Big(&2M^{(2)}_{kk,\tau_a} + 2M^{(2)\top}_{kk,\tau_a} + M^{(2)}_{kk,2\tau_a} + M^{(2)\top}_{kk,2\tau_a} \\ &+ 2N^{(2)}_{k,\tau_a} + N^{(2)}_{k,2\tau_a}\Big)h^2,\end{aligned} \tag{5.12}$$

where $M^{(2)}_{kk,\tau_a}$ and $N^{(2)}_{k,\tau_a}$ are in terms of proper time τ_a.

After the two cavities arrive at the same spacetime region, the two Gaussian quantum shares are combined using a balanced beam splitter, as shown in Fig. 5.5. The decoded Gaussian quantum secret is not a pure state anymore due to the effect of acceleration during distribution and collaboration. For a coherent state as the encoded secret Gaussian state, we calculate the fidelity of the

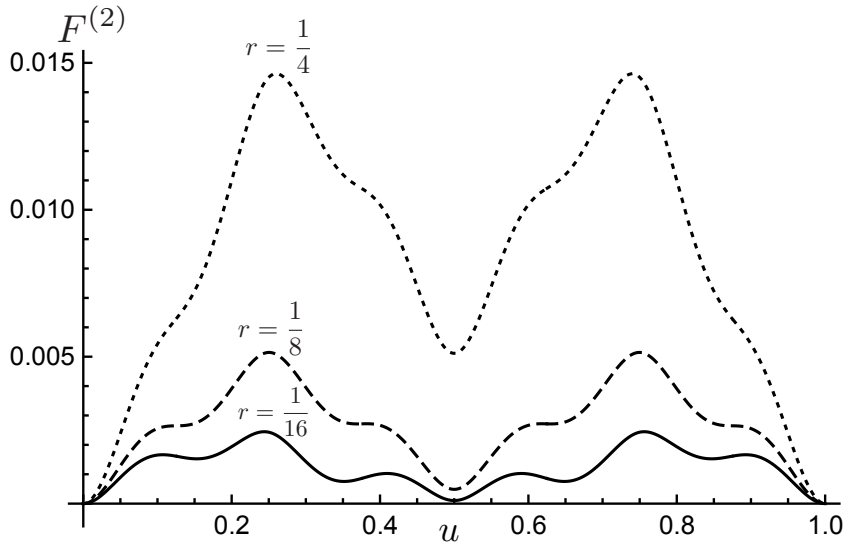


Figure 5.8: $F^{(2)}$ as a function of u for the ground mode $(k = 1)$, when the secret Gaussian state is a squeezed-vacuum state for squeezing parameters $r = \frac{1}{16}$ (solid), $\frac{1}{8}$ (dashed), and $\frac{1}{4}$ (dotted).

quantum secret sharing [71, 72]

$$F = 1 - 2\left(2f_{\beta,k,2u} + f_{\beta,k,u}\right)h^2 + O(h^3). \tag{5.13}$$

Interestingly, from (5.13), we conclude that the fidelity for a coherent state is independent of the initial mean photon number of the quantum secret. In other words, the fidelity of a coherent state is the same as the fidelity of the vacuum state.

In Fig. 5.8, we have plotted the second-order coefficient of the fidelity, $F^{(2)}$, for a squeezed-vacuum quantum secret; i.e., $F = 1 - F^{(2)}h^2$. Here we choose to plot all the quantities in terms of

$$u := \frac{\tilde{\omega}\tau}{2\pi k} = \frac{h\tau}{4L\,\mathrm{arctanh}\,\frac{h}{2}}. \tag{5.14}$$

as the Bogoliubov coefficients for a BBB are periodic in u with the period of 1. The figure shows that the fidelity decreases as the squeezing parameter r increases, i.e., as the mean photon number in the secret increases. This is in contrast to the case where the secret state is a coherent state.

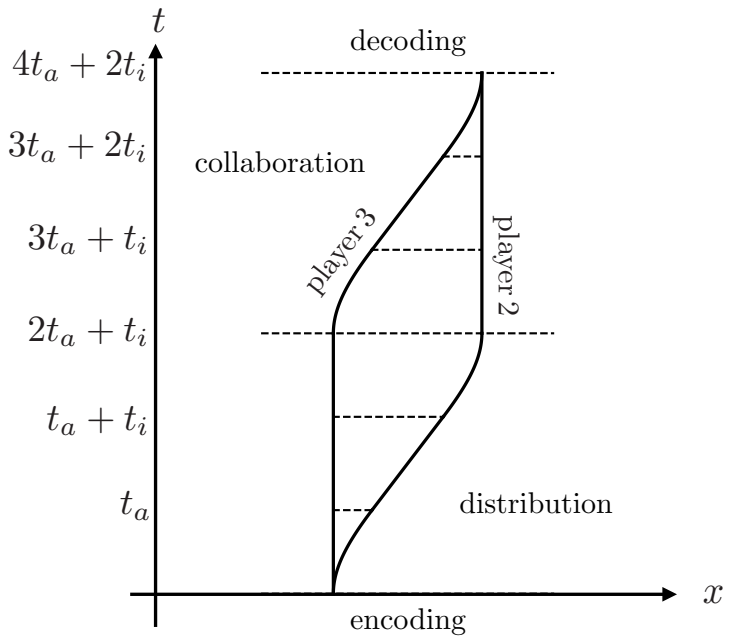


Figure 5.9: The two curves represent two worldlines in spacetime. The left worldline is the trajectory of the cavity carrying the third quantum share and the right worldline is the trajectory of the cavity carrying the second quantum share. From $t = 2t_a + t_i$ to $t = 4t_a + 2t_i$, the third cavity remains static. From $t = 2t_a + t_i$ to $t = 3t_a + t_i$, the second cavity accelerates with proper acceleration a. From $t = 3t_a + t_i$ to $t = 3t_a + 2t_i$, it moves with constant velocity and from $t = 3t_a + 2t_i$ to $t = 4t_a + 2t_i$, decelerates with proper acceleration a.

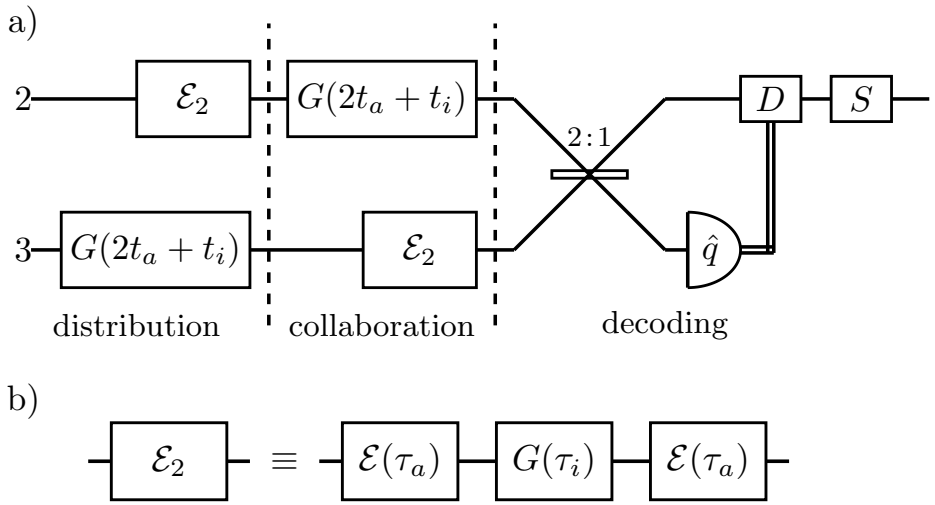


Figure 5.10: (a) The decoding circuit for the case wherein players 2 and 3 collaborate. $\mathcal{E}_2$ is a Gaussian thermal lossy channel. $G(2t_a + t_i)$ is the free evolution in the inertial frame. First, the two modes are combined on a beam splitter with reflectivity $2/3$. Then the quadrature $\hat{q}$ of the second output mode is measured and a displacement operation controlled by the measurement outcome and a squeezing operation are applied on the first output mode. (b) $\mathcal{E}_2$ is a single-mode Gaussian channel composed of three Gaussian channels in series.

Collaboration between Players 2 and 3

The second collaboration scenario we consider is the case wherein Players 2 and 3 collaborate to reconstruct the secret quantum state[2]. Similar to the previous case, the quantum shares of Players 2 and 3 are first transported to the same spacetime region. Fig. 5.9 shows the trajectories of the two corresponding cavities in this scenario. Note that the trajectory of the second cavity during the collaboration stage is the same as the trajectory of the third cavity during the distribution stage of the protocol. As Fig. 5.10 shows, the second quantum share goes through the channel $\mathcal{E}_2$ during distribution, while it goes through the channel $G(2t_a + t_i)$ during collaboration. The third quantum share first goes through the channel $G(2t_a + t_i)$ when the shares are being distributed and then is affected by the channel $\mathcal{E}_2$, which represents the effect of acceleration on this quantum share during collaboration.

[2]We emphasize that the collaboration between Players 1 and 2 results in the same results for the fidelity of the quantum secret sharing, which is simply due to the symmetry in the configuration of the players.

As shown in Fig. 5.10, the quantum Gaussian channel $\mathcal{E}_2$ is a combination of three quantum Gaussian channels, one of which is merely a phase rotation, i.e., $G(\tau_i)$. Assuming the input state of the Gaussian channel $\mathcal{E}_2$ is a coherent state and the free evolution is ignored, then the transformation of the first and second moments due to the channel $\mathcal{E}_2$ can be written as

$$\bar{\boldsymbol{x}} \overset{\mathcal{E}_2}{\longmapsto} \left(\mathbb{I} + 2M_{kk}^{(2)} h^2\right) \bar{\boldsymbol{x}}, \tag{5.15}$$

$$\mathbb{I} \overset{\mathcal{E}_2}{\longmapsto} \mathbb{I} + 2\left(M_{kk}^{(2)} + M_{kk}^{(2)\top} + N_k^{(2)}\right) h^2. \tag{5.16}$$

After the second and the third quantum shares reach the same spacetime region, the decoding of the quantum secret begins. For decoding, we employ the procedure introduced in [71, 72]. The optical decoding circuit is shown in Fig. 5.10, which is applied to reconstruct the secret quantum Gaussian state. We calculate the fidelity of quantum secret sharing in this case up to third order; i.e.,

$$F = F^{(0)} - F^{(2)} h^2 + O(h^3), \tag{5.17}$$

where $F^{(0)}$ and $F^{(2)}$ are

$$\begin{aligned} F^{(0)} &= \frac{1}{1+\mathrm{e}^{-s}}, \\ F^{(2)} &= \frac{4\mathrm{e}^{s}}{(1+\mathrm{e}^{s})^2}\left[f_{\beta,k} - f_{\alpha,k} + \mathrm{e}^{s}(f_{\alpha,k} + 2f_{\beta,k})\right]. \end{aligned} \tag{5.18}$$

In Fig. 5.11, we plotted the second-order coefficient of the fidelity $F^{(2)}$ as a function of u for $k = 1, 2, 3$. We observe from this figure that as the mode number k increases, the fidelity decreases, which suggests that the optimal mode for encoding the quantum secret is $k = 1$.

In the limit $s \to \infty$, the fidelity up to third order is

$$F = 1 - 4\left(f_{\alpha,k} + 2f_{\beta,k}\right) h^2 + O(h^3). \tag{5.19}$$

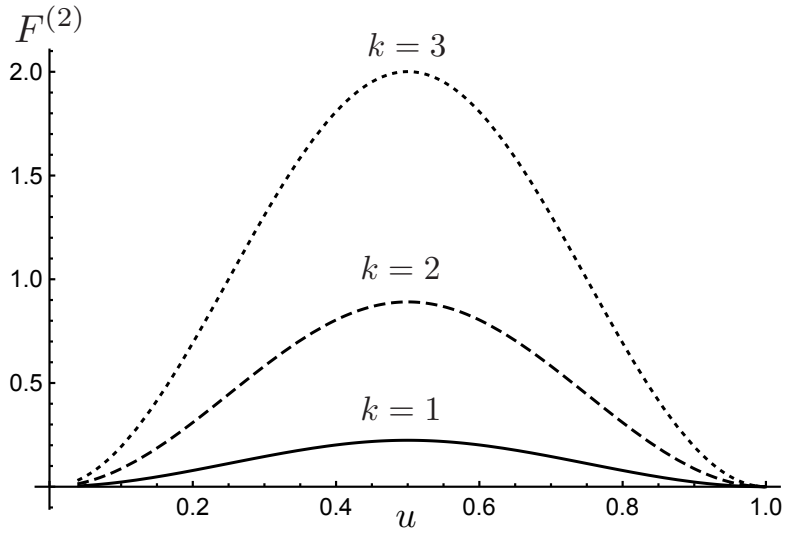


Figure 5.11: $F^{(2)}$ as a function of u for modes $k = 1$ (solid), 2 (dashed), and 3 (dotted) when the two-mode squeezing parameter $s = 1$.

Hence, in the limit of infinite squeezing and in the absence of acceleration ($h = 0$), fidelity is one. However, for non-zero acceleration, fidelity is always smaller than one, even if a maximally entangled state is employed to encode the quantum secret.

5.3 Conclusions and discussions

Here we study the effect of relativistic motion on $(2,3)$-threshold quantum Gaussian secret sharing. In our scheme, the dealer employs a single mode of a cavity to encode each quantum share. We begin by fully characterizing the BBB as a quantum Gaussian channel. We find that the canonical form of this channel is a thermal lossy channel. This form of the channel is useful for studying relativistic effects in quantum-information-processing tasks.

We consider different possible collaboration scenarios between different subsets of players and analyze how each scenario can be written as a composition of quantum Gaussian channels. We find that the decoherence due to the relativistic motion of the quantum shares during distribution and also collaboration, reduces the fidelity of quantum secret sharing.

Interestingly, we observe in the scenario wherein Players 1 and 2 are collaborating, depicted in Fig. 5.6, the fidelity is independent of the initial mean photon number in the encoded secret. Hence, in this case, the fidelity for a coherent state is the same as that of a vacuum state. Moreover, in the second scenario, Fig. 5.9, we find that when the quantum secret is a coherent state (or a vacuum state), the best encoding strategy is to encode the quantum secret in the ground mode of the cavity. We observe that the fidelity of the protocol is smaller than one, even in the limit of infinite squeezing, i.e., when maximal entanglement is used as a resource (See Eq. (5.19)).

As a future line of research, we are interested in extending our results to the more general case of (k,n)-threshold quantum secret sharing. Furthermore, we hope that the methods developed here can be employed to relax the conditions on spacetime replication of quantum states [54, 52], i.e., to consider the effect of non-uniform motion on this task.

Chapter 6

Characterization of quantum systems

To verify whether a quantum channel is a reliable channel for certain purposes, like quantum communication, physicists need to learn information about this quantum channel. One straight way is to do tomography, which is highly resource consuming. Furthermore, we do not always need to get all the information of a quantum channel when we only care how good it is concerning a target channel. Thus, more efficient approaches are proposed based on fidelity estimation and benchmarking to characterize the information of a quantum channel. Compared to tomography, which fully characterize a quantum state or a quantum channel, we call these approaches partial characterization of quantum systems. This chapter reviews several approaches to partially characterize quantum states or quantum channels.

Section 6.1 reviews direct fidelity estimation of both quantum states and quantum channels, and also discusses its adaption into CV quantum states. Section 6.2 reviews verification of quantum states and presents a verification scheme for Gaussian states. In Sec. 6.3, I review a scheme to benchmark the average performance of a bosonic quantum channel.

6.1 Direct fidelity estimation

In this section, I review the method of direct fidelity estimation [41, 31] by applying local Pauli measurements. The sample complexity of estimating fidelity of a general n-qubit target pure state

is less than that of quantum tomography by a factor of 2^n. This approach is also generalized to CV quantum states [31], which, however, cannot yield a reliable estimation via a finite number of copies.

Suppose ρ_{t} is an n-qubit target pure state. The fidelity between ρ_t and a prepared n-qubit state ρ_{p} is

$$F(\rho_{\mathrm{p}}, \rho_{\mathrm{t}}) = \mathrm{tr}\left(\rho_{\mathrm{p}}\rho_{\mathrm{t}}\right). \tag{6.1}$$

As the set of n-qubit Pauli operators $\left\{\frac{P_i}{\sqrt{d}}\right\}_{i=1}^{d^2}$ for

$$P_i \in \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}^{\otimes n} \tag{6.2}$$

and $d = 2^n$, forms an orthonormal basis of $d \times d$ density matrices, any state ρ can be written as

$$\rho = \sum_{i=1}^{d^2} \frac{1}{d} \chi_\rho(i) P_i, \tag{6.3}$$

where $\chi_\rho(i) = \mathrm{tr}(\rho P_i)$. Hence, we have

$$\mathrm{tr}(\rho_{\mathrm{t}}\rho_{\mathrm{p}}) = \frac{1}{d} \sum_{i=1}^{d^2} \chi_{\rho_{\mathrm{t}}}(i)\chi_{\rho_{\mathrm{p}}}(i), \tag{6.4}$$

Reformulating Eq. (6.4), we obtain

$$\mathrm{tr}(\rho_{\mathrm{t}}\rho_{\mathrm{p}}) = \sum_{i=1}^{d^2} p_i X_i, \tag{6.5}$$

where $p_i \coloneqq \frac{\chi_{\rho_{\mathrm{t}}}(i)^2}{d}$ and $X_i \coloneqq \frac{\chi_{\rho_{\mathrm{p}}}(i)}{\chi_{\rho_{\mathrm{t}}}(i)}$. As ρ_{t} is pure,

$$\mathrm{tr}(\rho_{\mathrm{t}}^2) = \sum_{i=1}^{d^2} p_i = 1, \tag{6.6}$$

which indicates that $\{p_i\}_{i=1}^{d^2}$ is a probability distribution. Thus, Eq. (6.5) implies that $\mathrm{tr}(\rho_{\mathrm{t}}\rho_{\mathrm{p}})$

equals the mean value $\bar{X}$ of variable X that takes a value of X_i with probability p_i. To estimate $\mathrm{tr}(\rho_\mathrm{t}\rho_\mathrm{p})$, we sample i from the probability distribution $\{p_i\}_{i=1}^{d^2}$ by l times to obtain l Pauli operators $P_{i_j}(1 \leq j \leq l)$. Then for each chosen P_{i_j}, we estimate $\chi_{\rho_\mathrm{p}}(i_j)$ by applying local Pauli measurements measuring P_{i_j} on m_{i_j} copies of ρ_p.

We show the procedure for direct fidelity estimation in Algorithm 1. All the input variables are specified by their types, including quantum types: quantum states $\mathcal{QS}[\mathscr{H}]$ and quantum channels $\mathcal{QC}[\mathscr{H}_{in}][\mathscr{H}_{out}]$.

Algorithm 1 Direct Fidelity Estimation [41, 31]

Input:

- $\rho_\mathrm{t} \in \mathbb{C}^{d\times d}$ ▷ classical description of ρ_t i.e. density matrix
- $\delta \in (0, \frac{1}{2})$ ▷ maximal failure probability
- $\varepsilon \in (0,1)$ ▷ estimation error bound
- $\rho_\mathrm{p} \in \mathcal{QS}[\mathscr{H}]$ ▷ $O\left(\frac{1}{\varepsilon^2\delta} + \frac{d\ln\frac{1}{\delta}}{\varepsilon^2}\right)$ copies of unknown quantum states ρ_p.

Output:

- $\tilde{F} \in \mathbb{R}$ ▷ Estimate of fidelity $F(\rho_\mathrm{p}, \rho_\mathrm{t})$

procedure DIRECTFIDELITYESTIMATION(ρ_t, δ, ε, ρ_p)
  for $j = 1 : l$ **do**
    Sample an interger $1 \leq i_j \leq d^2$ from probability distribution $\{p_i\}_{i=1}^{d^2}$;
    for $k = 1 : m_{i_j}$ **do**
      Apply a single-shot Pauli measurement measuring P_{i_j} on a copy of ρ_p, and obtain a measurement outcome $A_{i_j,k}$, which is either 1 or -1;
    end for
  end for
  return $\tilde{F} \leftarrow \sum_{j=1}^{l} \sum_{k=1}^{m_{i_j}} \frac{A_{i_j,k}}{l m_{i_j} \chi_{\rho_\mathrm{t}}(i_j)}$.
end procedure

Given estimation error bound $0 < \varepsilon < 1$ and maximal failure probability $0 < \delta < \frac{1}{2}$, the probability of an estimate falling outside the interval $(F(\rho_\mathrm{p}, \rho_\mathrm{t}) - \varepsilon, F(\rho_\mathrm{p}, \rho_\mathrm{t}) + \varepsilon)$ should be

$$\Pr(|\tilde{F} - F(\rho_\mathrm{p}, \rho_\mathrm{t})| \geq \varepsilon) \leq \delta. \tag{6.7}$$

To satisfy Eq. (6.7), we set

$$\Pr\left(\left|\frac{1}{l}\sum_{j=1}^{l} X_{i_j} - F(\rho_{\mathrm{p}},\rho_{\mathrm{t}})\right| \geq \frac{\varepsilon}{2}\right) \leq \frac{\delta}{2}. \tag{6.8}$$

and

$$\Pr\left(|\tilde{F} - \frac{1}{l}\sum_{j=1}^{l} X_{i_j}| \geq \frac{\varepsilon}{2}\right) \leq \frac{\delta}{2}. \tag{6.9}$$

Using Chebyshev's inequality for (6.8) yields the demanded number of samples of Pauli operators

$$l \geq \frac{8}{\varepsilon^2\delta}. \tag{6.10}$$

Using Hoeffding's inequality [57] for (6.9), we get for each i_j, the sample complexity for the measurement of P_{i_j} is

$$m_{i_j} \geq \frac{8\ln\frac{2}{\delta}}{l\varepsilon^2\chi_{i_j}(\rho_t)^2}. \tag{6.11}$$

From both Eqs. (6.10) and (6.11), the expected total sample complexity of ρ_p is

$$m = l\sum_{i=1}^{d^2} p_i m_i \geq \frac{8d\ln\frac{2}{\delta}}{\varepsilon^2}. \tag{6.12}$$

One can see that the expected sample complexity for direct fidelity estimation scales as $O(d)$, less than $O(d^2)$ of quantum tomography.

The idea of fidelity estimation is generalized to estimating average fidelity of a quantum channel. This generalization estimates the average fidelity between a prepared quantum channel and a target unitary channel. The sample complexity of this scheme is $O\left(\frac{1}{\varepsilon^2\delta} + \frac{d^2\ln\frac{1}{\delta}}{\varepsilon^2}\right)$ [41]. This scheme requires only tensor products of local Pauli eigenstates as inputs and measuring local Pauli operators at outputs.

This scheme is extended to estimating fidelity of CV quantum states as well, using

$$\mathrm{tr}(\rho_{\mathrm{t}}\rho_{\mathrm{p}}) = \int_{\mathbb{C}} \frac{\mathrm{d}^2\alpha}{\pi} \mathscr{W}_{\rho_{\mathrm{t}}}(\alpha)\mathscr{W}_{\rho_{\mathrm{p}}}(\alpha), \tag{6.13}$$

where $\mathscr{W}_\rho(\alpha)$ is the Wigner function (2.152) of density operator ρ. As, for a pure state ρ_t,

$$\pi \int_{\mathbb{C}} \mathrm{d}^2\alpha \mathscr{W}_{\rho_t}(\alpha)^2 = 1, \tag{6.14}$$

$\left\{p(\alpha) \coloneqq \pi \mathscr{W}_{\rho_t}(\alpha)^2; \alpha \in \mathbb{C}\right\}$ is a probability distribution over the phase space. Thus, we have

$$\mathrm{tr}(\rho_t \rho_p) = \int \mathrm{d}^2\alpha p(\alpha) \frac{\mathscr{W}_{\rho_p}(\alpha)}{\mathscr{W}_{\rho_t}(\alpha)}. \tag{6.15}$$

Using procedures analougous to fidelity estimation of multi-qubit states, one can estimate fidelity of a CV state by sampling a Wigner function.

Again, from Chebyshev's inequality, we need to sample l (6.10) phase-space points. Using Hoeffding's inequality, we know for each phase-space point α, we need

$$m_\alpha \geq \frac{8 \ln \frac{2}{\delta}}{\varepsilon^2 l \mathscr{W}_{\rho_t}(\alpha)^2} \tag{6.16}$$

number of measurements to estimate the value $\mathscr{W}_{\rho_p}(\alpha)$. However, as the entire phase space is not compact, the expected total sample complexity

$$m = l \int_{\mathbb{C}} \mathrm{d}^2\alpha p(\alpha) m_\alpha \geq \frac{\pi \ln \frac{2}{\delta}}{\varepsilon^2} \int_{\mathbb{C}} \mathrm{d}^2\alpha \tag{6.17}$$

is divergent for any CV target state ρ_t. Thus, with finite sample complexity, this scheme cannot yield a reliable estimation of fidelity of a CV quantum state.

This section has reviewed how to estimate the fidelity of a quantum state by only applying local Pauli measurements. This scheme is generalized to estimate the average fidelity of a quantum channel via feeding eigenstates of Pauli operators as inputs and applying Pauli measurements at outputs. However, I have shown that the direct adaption of this scheme into CV quantum states does not yield a reliable estimation scheme.

6.2 Verification of Gaussian states

This section begins with the definition of quantum-state verification. Then we review the mathematical definition of fidelity witness. Finally, we discuss the fidelity witness for Gaussian pure states and the verification protocol for Gaussian pure states.

Verification is the process of determining whether an implementation properly satisfies design specifications [89]. Verification, along with validation, is important for assessing the credibility of a product or a system. Quantum-state verification [11, 50, 110, 44, 92, 92, 126] aims to check whether an implementation of certain quantum state meets the specifications of a target quantum state or not.

Suppose the figure of merit for state verification is fidelity

$$F(\rho_{\mathrm{p}}, \rho_{\mathrm{t}}) = \mathrm{tr}\left(\rho_{\mathrm{p}}\rho_{\mathrm{t}}\right), \tag{6.18}$$

where ρ_{t} is pure: $\rho_{\mathrm{t}}^2 = \rho_{\mathrm{t}}$. There is a technology-limited verifier and an untrusted, powerful prover with significant but bounded quantum technology. The verifier provides the prover with the classical description of a pure state ρ_{t}, and the prover sends independent and identical copies of quantum state ρ_{p} to the verifier. Then by measurements, the verifier decides whether to accept ρ_{p} as a certified preparation of ρ_{t} or reject it. Reminiscent of interactive proof systems [45, 58], the completeness and soundness conditions of quantum-state verification are defined as follows.

Definition 6 ([11])**.** With respect to threshold fidelity $F_{\mathrm{t}} < 1$ and maximal failure probability $0 < \delta \leq \frac{1}{2}$, the verifier's verification test should satisfy

1. completeness: if $\rho_{\mathrm{p}} = \rho_{\mathrm{t}}$, the verifier accepts with probability at least $1-\delta$;

2. soundness: if $F(\rho_{\mathrm{p}}, \rho_{\mathrm{t}}) \leq F_{\mathrm{t}}$, the verifier rejects with probability at least $1-\delta$.

As ρ_{t} has zero measure in the topological space of density operators induced by fideity, to make the definition practically meaningful, the verifier should accept all states in a neighborhood of ρ_{t} with probability at least $1-\delta$.

In the multi-qubit case, $F(\rho_{\mathrm{p}},\rho_{\mathrm{t}})$ can be estimated [41, 31] by decomposing ρ_{t} into a linear combination of Pauli operators and measuring the overlap between ρ_{p} and each Pauli operator. This idea gives rise to verification schemes for ground states of Hamiltonians and certain stabilizer states by measuring single-qubit Pauli operators [110]. Adapting this idea into infinite-dimensional system, $F(\rho_{\mathrm{p}},\rho_{\mathrm{t}})$ can be estimated by measuring the Wigner function of ρ_{p} at different phase-space points [31]. Although experimentally viable [79], this method is not efficient.

To obtain an efficient verification scheme for Gaussian pure states, we introduce fidelity witness, which provides an economic way to detect $F(\rho_{\mathrm{p}},\rho_{\mathrm{t}})$. Analogous to entanglement witness [112, 59], a fidelity witness distinguishes ρ_{t} from the whole set $\{\rho_{\mathrm{p}};F(\rho_{\mathrm{p}},\rho_{\mathrm{t}})\leq F_{\mathrm{t}}\}$ for any threshold fidelity $F_{\mathrm{t}}<1$. Here we present the mathematical definition of fidelity witness.

Definition 7 ([44])**.** A self-adjoint operator W is a fidelity witness for ρ_{t} if

$$\mathcal{W}(\rho_{\mathrm{p}}) \coloneqq \mathrm{tr}\left(W\rho_{\mathrm{p}}\right) \tag{6.19}$$

satisfies

1. $\mathcal{W}(\rho_{\mathrm{p}})=1 \Longleftrightarrow \rho_{\mathrm{p}}=\rho_{\mathrm{t}}$; (6.20)

2. $\forall\rho_{\mathrm{p}},\mathcal{W}(\rho_{\mathrm{p}})\leq F(\rho_{\mathrm{p}},\rho_{\mathrm{t}})$. (6.21)

We see that

$$\mathrm{tr}\left(W\rho_{\mathrm{p}}\right) > F_{\mathrm{t}} \tag{6.22}$$

witnesses

$$F(\rho_{\mathrm{t}},\rho_{\mathrm{p}}) > F_{\mathrm{t}}, \tag{6.23}$$

whereas

$$\mathrm{tr}\left(W\rho_{\mathrm{p}}\right) \leq F_{\mathrm{t}} \tag{6.24}$$

does not imply any relation between $F(\rho_{\mathrm{t}},\rho_{\mathrm{p}})$ and F_{t}.

Now we explain how to verify a Gaussian pure state by measuring a fidelity witness. For any Gaussian pure state

$$\rho_{\mathrm{t}} = U_{\boldsymbol{S},\boldsymbol{d}} \left|0\right\rangle_{\mathscr{F}} \left\langle 0\right| U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}, \tag{6.25}$$

the observable

$$\mathbb{1} - U_{\boldsymbol{S},\boldsymbol{d}} \hat{n} U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} \tag{6.26}$$

is a fidelity witness, such that

$$F(\rho_{\mathrm{t}}, \rho_{\mathrm{p}}) \geq 1 - \left\langle U_{\boldsymbol{S},\boldsymbol{d}} \hat{n} U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} \right\rangle_{\rho_{\mathrm{p}}}, \tag{6.27}$$

where equality is achieved iff $\rho_{\mathrm{p}} = \rho_{\mathrm{t}}$. The above mean value is a linear combination of single-mode expectation values and two-mode correlations [11]

$$\left\langle U_{\boldsymbol{S},\boldsymbol{d}} \hat{n} U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} \right\rangle_{\rho_{\mathrm{p}}} = \frac{1}{2} \mathrm{tr} \left[\boldsymbol{S}^{-\top} \boldsymbol{S}^{-1} \left(\left\langle \hat{\boldsymbol{x}}^{\top} \hat{\boldsymbol{x}} \right\rangle_{\rho_{\mathrm{p}}} - 2 \bar{\boldsymbol{x}}_{\rho_{\mathrm{p}}} \boldsymbol{d} + \boldsymbol{d}^{\top} \boldsymbol{d} \right) \right] - \frac{N}{2}, \tag{6.28}$$

Thus, the right-hand side of inequality (6.27) can be estimated by local homodyne detections on ρ_{p}.

The verification protocol for Gaussian pure states is presented in Algorithm 2. This protocol requires $2mc_1 + 2\nu mc_2$ copies of ρ_{p}, where

$$c_1 \in O\left(\frac{m^2 \left\| \boldsymbol{S} \right\|_{\infty}^4 \left\| \boldsymbol{d} \right\|^2 \sigma_1^2}{\varepsilon^2 \ln(1/(1-\delta))} \right), \tag{6.29}$$

$$c_2 \in O\left(\frac{m^3 \nu^2 \left\| \boldsymbol{S} \right\|_{\infty}^4 \sigma_2^2}{\varepsilon^2 \ln(1/(1-\delta))} \right), \tag{6.30}$$

$\nu = 2\min\{k^2, m\}$, k is the maximum number of input modes to which an output mode is coupled and $\left\| \boldsymbol{S} \right\|_{\infty}$ equals $e^{r}_{\max}$, where $r_{\max}$ is the maximal single-mode squeezing parameter in $U_{\boldsymbol{S},\boldsymbol{d}}$. This protocol is a reliable verification protocol satisfying the completeness and soundness conditions in Def. 6 [11]. Furthermore, this protocol accepts any state close enough to ρ_{t}. If

$$F(\rho_{\mathrm{p}}, \rho_{\mathrm{t}}) \geq F_{\mathrm{t}} + \Delta, \tag{6.32}$$

Algorithm 2 Verification protocol for Gaussian pure states [11]

Input:

- $\boldsymbol{S} \in \mathrm{Sp}(2m, \mathbb{R})$ ▷ symplectic transformation of $U_{\boldsymbol{S},\boldsymbol{d}}$ in Eq. (6.25)
- $\boldsymbol{d} \in \mathbb{R}^{2m}$ ▷ displacement vector of $U_{\boldsymbol{S},\boldsymbol{d}}$ in Eq. (6.25)
- $F_{\mathrm{t}} \in (0,1)$ ▷ threshold fidelity
- $\delta \in \left(0, \frac{1}{2}\right]$ ▷ maximal failure probability
- $\varepsilon \in \left(0, \frac{1-F_{\mathrm{t}}}{2}\right)$ ▷ error bound
- $k \in \mathbb{N}^+$ ▷ maximum number of input modes to which an output mode is coupled.
- $\rho_{\mathrm{p}} \in \mathcal{QS}[\mathscr{F}^{\otimes m}]$ ▷ $2mc_1 + 2\nu mc_2$ copies of ρ_{p}
- $\sigma_1 > 0$ ▷ upper bound of the variance of any $\hat{\boldsymbol{x}}_l$ on ρ_{p}, where $1 \leq l \leq 2m$.
- $\sigma_2 > 0$ ▷ upper bound of the variance of any $\frac{1}{2}\left(\hat{\boldsymbol{x}}_u \hat{\boldsymbol{x}}_v + \hat{\boldsymbol{x}}_v \hat{\boldsymbol{x}}_u\right)$, where $1 \leq u \leq v \leq 2m$.

Output:

- $b \in \{0,1\}$ ▷ 0 means reject and 1 means accept.

procedure VERIFICATIONOFPUREGAUSSIANSTATES($\boldsymbol{S}$, $\boldsymbol{d}$, F_{t}, δ, ε, k, σ_1, σ_2, ρ_{p})
  for $l = 1 : 2m$ **do**
    for $i = 1 : c_1$ **do** ▷ To obtain an estimate $\bar{\boldsymbol{x}}^*_{\rho_{\mathrm{p}}}$ of $\bar{\boldsymbol{x}}_{\rho_{\mathrm{p}}}$.
      apply a single-shot homodyne detection for quadrature $\hat{\boldsymbol{x}}_l$ on one copy of ρ_{p};
    end for
    $\left(\bar{\boldsymbol{x}}^*_{\rho_{\mathrm{p}}}\right)_l \leftarrow \frac{1}{c_1}\sum_{i=1}^{c_1} \chi_i^{\hat{\boldsymbol{x}}_l}$; ▷ $\chi_i^{\hat{\boldsymbol{x}}_l}$ is ith measurement outcome with respect to $\hat{\boldsymbol{x}}_l$.
    for $i = 1 : c_2$ **do** ▷ To estimate the diagonal elements in $\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle_{\rho_{\mathrm{p}}}$.
      apply a single-shot homodyne detection for quadrature $\hat{\boldsymbol{x}}_l$ on one copy of ρ_{p};
    end for
    $\left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\mathrm{p}}}\right)_{ll} \leftarrow \frac{1}{c_2}\sum_{i=1}^{c_2} \left(\chi_i^{\hat{\boldsymbol{x}}_l}\right)^2$;
  end for

for $v = 1 : 2m$ **do** ▷ To estimate the off-diagonal elements in $\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle_{\rho_{\rm p}}$

  for $u = 1 : v-1$ and $(\boldsymbol{S}^{-\top}\boldsymbol{S}^{-1})_{u,v} \neq 0$ **do**

    if $(u,v) \neq (2j-1, 2j)$ **then**

      for $i = 1 : c_2$ **do**

        apply two single-shot homodyne detections for quadratures $\hat{\boldsymbol{x}}_u$ and $\hat{\boldsymbol{x}}_v$ simultaneously on one copy of $\rho_{\rm p}$;

      end for

      $\left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}}\right)_{vu} \leftarrow \frac{1}{c_2}\sum_{i=1}^{c_2} \chi_i^{\hat{\boldsymbol{x}}_u} \chi_i^{\hat{\boldsymbol{x}}_v}$; ▷ $\chi_i^{\hat{\boldsymbol{x}}_u}$ and $\chi_i^{\hat{\boldsymbol{x}}_v}$ are ith measurement outcomes

      $\left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}}\right)_{uv} \leftarrow \left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}}\right)_{vu}$;

    else

      for $i = 1 : c_2$ **do**

        apply a single-shot homodyne detection for quadrature $\frac{1}{\sqrt{2}}(\hat{\boldsymbol{x}}_u + \hat{\boldsymbol{x}}_v)$ on one copy of $\rho_{\rm p}$;

      end for

      $\left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}}\right)_{vu} \leftarrow \frac{1}{c_2}\sum_{i=1}^{c_2} \left(\chi_i^{\frac{1}{\sqrt{2}}(\hat{\boldsymbol{x}}_u + \hat{\boldsymbol{x}}_v)}\right)^2 - \frac{1}{2}\left(\bar{\boldsymbol{x}}^*_{\rho_{\rm p}}\right)^2_u - \frac{1}{2}\left(\bar{\boldsymbol{x}}^*_{\rho_{\rm p}}\right)^2_v$;

      ▷ $\chi_i^{\frac{1}{\sqrt{2}}(\hat{\boldsymbol{x}}_u + \hat{\boldsymbol{x}}_v)}$ is ith measurement outcome regarding $\frac{1}{\sqrt{2}}(\hat{\boldsymbol{x}}_u + \hat{\boldsymbol{x}}_v)$.

      $\left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}}\right)_{uv} \leftarrow \left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}}\right)_{vu}$;

    end if

  end for

end for

$\mathcal{W}(\rho_{\rm p})^* \leftarrow \frac{1}{2}\mathrm{tr}\left[\boldsymbol{S}^{-\top}\boldsymbol{S}^{-1}\left(\left\langle \hat{\boldsymbol{x}}^\top \hat{\boldsymbol{x}} \right\rangle^*_{\rho_{\rm p}} - 2\bar{\boldsymbol{x}}^*_{\rho_{\rm p}}\boldsymbol{d} + \boldsymbol{d}^\top \boldsymbol{d}\right)\right] - \frac{N}{2}$; ▷ Obtain an estimate $\mathcal{W}(\rho_{\rm p})^*$ of

$$\mathcal{W}(\rho_{\rm p}) = 1 - \left\langle U_{\boldsymbol{S},\boldsymbol{d}} \hat{n} U^\dagger_{\boldsymbol{S},\boldsymbol{d}} \right\rangle_{\rho_{\rm p}}, \tag{6.31}$$

if $\mathcal{W}(\rho_{\rm p})^* > F_{\rm t} + \varepsilon$ **then**

  return $b = 1$;

else

  return $b = 0$.

end if

end procedure

where

$$\Delta = \frac{2\varepsilon + \mathcal{W}(\rho_{\mathrm{t}}^{\perp})(F_{\mathrm{t}} - 1)}{1 - \mathcal{W}(\rho_{\mathrm{t}}^{\perp})} \tag{6.33}$$

and $\rho_{\mathrm{t}}^{\perp}$ is a density operator orthogonal to ρ_{t} satisfying

$$\rho_{\mathrm{p}} = F\rho_{\mathrm{t}} + (1-F)\rho_{\mathrm{t}}^{\perp}, \tag{6.34}$$

the verifier accepts ρ_{p} with probability at least $1-\delta$. As

$$F_{\mathrm{t}} + \Delta < 1, \tag{6.35}$$

the verifier, with a high probability, accepts any state in a neighborhood of ρ_{t} in the topological space of density operators.

In this section, we have explained how verification of quantum states can be cast into an adversarial game between a verifier and a prover. We have reviewed the mathematical definitions of fidelity witness as well as the verification protocol for multi-mode Gaussian pure states.

6.3 Benchmarking bosonic quantum channels

This section first reviews the general framework of quantum-process benchmarking. Second, we explain how an arbitrary benchmark test can be reformulated into a canonical test that employs one input state and measures one observable. Third, we discuss the canonical test for amplification and attenuation channels.

Here quantum-process benchmarking refers to measuring the performance of an experimental quantum process using a specific figure of merit, such as average fidelity, resulting in a value that is compared with theoretical values. Direct-fidelity estimation approach [41, 31] can be used to benchmark multi-qubit quantum channels by preparing product states and measuring single-qubit Pauli operators. On the other hand, quantum randomized benchmarking provides an efficient way to estimate the average gate fidelity of multi-qubit Clifford gates. However, neither of these

methods are readily adapted to benchmarking bosonic channels due to the finite-energy restriction [23, 124, 12, 107, 40].

Now we introduce a general framework of quantum-process benchmarking in terms of a quantum-state transformation game [124]. In order to measure the performance of a prover's quantum channel, denoted by $\mathcal{E}$, a verifier prepares a state ρ_x with probability p_x (in general, a probability measure), sends ρ_x through $\mathcal{E}$, applies certain measurement on $\mathcal{E}(\rho_x)$, and assign different scores to different measurement outcomes, where x is a label. We use x to denote the set of labels, and the cardinality of X can either be finite or be countably infinite or even uncountable. The expected score $s_{\mathcal{E}}$ quantifies the performance of channel $\mathcal{E}$.

For average-fidelity-based benchmarking, the verifier's measurement is described by the POVM

$$\{|\phi_x\rangle\langle\phi_x|, \mathbb{1} - |\phi_x\rangle\langle\phi_x|\},\ |\phi_x\rangle \in \mathscr{H}. \tag{6.36}$$

If the measurement outcome corresponds to $|\phi_x\rangle\langle\phi_x|$, then the verifier assigns score 1 to $\mathcal{E}$; otherwise, he assigns score 0. Then the expected score equals the average fidelity

$$s_{\mathcal{E}} = \bar{F}_{\mathcal{E}} \coloneqq \sum_{x\in X} p_x \langle\phi_x|\mathcal{E}(\rho_x)|\phi_x\rangle, \tag{6.37}$$

where, if x is an uncountable set, $\sum$ must be replaced by $\int$.

Rather than sampling different inputs ρ_x, any benchmark test can be reformulated into a new test that requires only the preparation of one input state σ_{AR} and the measurement of one observable $O_{\mathrm{A'R}}$ by adding a reference system R, where A and A$'$ denote channel input and channel output, respectively. The new test is equivalent to the original one, in the sense that, for any CPTP map $\mathcal{E}$, the expected score

$$s_{\mathcal{E}} = \mathrm{tr}\left[O_{\mathrm{A'R}}\mathcal{E}\otimes\mathcal{I}(\sigma_{\mathrm{AR}})\right], \tag{6.38}$$

where $\mathcal{I}$ is the identity channel on reference R. σ_{AR} and $O_{\mathrm{A'R}}$ in Eq. (6.38) are not unique: different combinations of input σ_{AR} and observable $O_{\mathrm{A'R}}$ lead to equivalent tests iff they yield the same

performance operator, which is defined below.

Definition 8 ([12])**.** For a benchmark test with input state σ_{AR} and observable $O_{\mathrm{A}'\mathrm{R}}$, the performance operator is

$$\Pi_{\mathrm{A}'\mathrm{A}} \coloneqq \mathrm{tr}_{\mathrm{R}}\left[(O_{\mathrm{A}'\mathrm{R}} \otimes \mathbb{1}_{\mathrm{A}})(\mathbb{1}_{\mathrm{A}'} \otimes \sigma_{\mathrm{AR}})\right]. \tag{6.39}$$

This performance operator (6.39) satisfies the condition that, for any quantum channel $\mathcal{E}$,

$$s_{\mathcal{E}} = \mathrm{tr}(\Pi_{\mathrm{A}'\mathrm{A}} C_{\mathcal{E}}^{\top_{\mathrm{A}}}), \tag{6.40}$$

for $C_{\mathcal{E}}^{\top_{\mathrm{A}}} = \sum_{ij} \mathcal{E}(|i\rangle\langle j|) \otimes |j\rangle\langle i|$ the Jamiołkowski operator of $\mathcal{E}$ [60].

As the combination of σ_{AR} and $O_{\mathrm{A}'\mathrm{R}}$ is not unique, an experimentally feasible input state σ_{AR} is preferred. Any benchmark test of $\mathcal{E}$ can be reformulated into a canonical test by preparing an entangled pure state $|\Psi\rangle_{\mathrm{AR}}$, applying $\mathcal{E}$ to system A, and applying measurements on $\mathcal{E} \otimes \mathcal{I}(|\Psi\rangle\langle\Psi|_{\mathrm{AR}})$ with the observable [12]

$$O_{\mathrm{A}'\mathrm{R}} = \left(\mathbb{1}_{\mathrm{A}'} \otimes \rho_{\mathrm{R}}^{-\frac{1}{2}} T_{\mathrm{AR}}^{\dagger}\right) \Pi_{\mathrm{A}'\mathrm{A}}^{\top_{\mathrm{A}}} \left(\mathbb{1}_{\mathrm{A}'} \otimes T_{\mathrm{AR}} \rho_{\mathrm{R}}^{-\frac{1}{2}}\right), \tag{6.41}$$

where

$$\rho_{\mathrm{R}} = \mathrm{tr}_{\mathrm{A}}(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}),\ \rho_{\mathrm{A}} = \mathrm{tr}_{\mathrm{R}}(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}) \tag{6.42}$$

and T_{AR} is a partial isometry such that

$$T_{\mathrm{AR}}^{\dagger} \rho_{\mathrm{A}} T_{\mathrm{AR}} = \rho_{\mathrm{R}}. \tag{6.43}$$

By plugging the performance operator for average-fidelity-based test

$$\Pi_{\mathrm{A}'\mathrm{A}} = \sum_{x \in X} p_x |\phi_x\rangle\langle\phi_x| \otimes \rho_x \tag{6.44}$$

into Eq. (6.41), we obtain the single observable to be measured, in order to estimate average fidelity.

In this chapter, I have reviewed direct fidelity estimation for both quantum states and quantum channels, as well as its adaption to CV states. Furthermore, I have reviewed concepts concerning quantum-state verification and fidelity witness. The exposition has elucidated how a multi-mode Gaussian pure state can be verified by measuring a fidelity witness. I have also discussed quantum-process benchmark and the canonical benchmark test.

Chapter 7

Efficient verification of bosonic quantum channels

This section aims to devise feasible, efficient verification schemes for bosonic quantum channels. To this end, in Sec. 7.1, we construct an average-fidelity witness that yields a tight lower bound for average fidelity plus a general framework for verifying optimal quantum channels. In Sec. 7.2, for both multi-mode unitary Gaussian channels and single-mode amplification channels, we present experimentally feasible average-fidelity witnesses and reliable verification schemes, for which sample complexity scales polynomially with respect to all channel specification parameters. Our verification scheme provides an approach to benchmark the performance of bosonic channels on a set of Gaussian-distributed coherent states by employing only two-mode squeezed vacuum states and local homodyne detections.

7.1 Definitions and framework

This section develops our general framework of verification of an optimal quantum channel. We introduce a new concept, called average-fidelity witness. We present our general protocol for quantum-channel verification and show this verification protocol satisfies completeness and soundness conditions.

Consider a state-transformation task

$$\rho_x \mapsto |\phi_x\rangle \tag{7.1}$$

with an input ensemble

$$\{(p_x, \rho_x); x \in X\} \tag{7.2}$$

as well as an output-target-state set

$$\{|\phi_x\rangle \langle\phi_x|; x \in X\}. \tag{7.3}$$

Suppose at least one optimal quantum channel $\mathcal{E}_{\text{opt}}$ exists in the sense that $\mathcal{E}_{\text{opt}}$ achieves the maximal average fidelity

$$\bar{F}_{\max} := \sup_{\mathcal{E}} \sum_{x \in X} p_x \langle\phi_x| \mathcal{E}(\rho_x) |\phi_x\rangle = \sum_{x \in X} p_x \langle\phi_x| \mathcal{E}_{\text{opt}}(\rho_x) |\phi_x\rangle . \tag{7.4}$$

In the finite-dimensional case, such an optimal quantum channel always exists [70, 24].

There is a technology-limited verifier and an untrusted, powerful prover with significant but bounded quantum technology. The verifier provides the prover with the classical description of the input ensemble (7.2) as well as the output-target-state set (7.3), and the prover sends independent and identical copies of quantum channels, $\mathcal{E}_{\text{p}}$, to the verifier. The verifier prepares input states and applies local measurements at outputs without any state-preparation and measurement (SPAM) errors, and then decides whether to accept $\mathcal{E}_{\text{p}}$ as an optimal quantum channel in terms of $\bar{F}_{\mathcal{E}_{\text{p}}}$, or reject it. We define completeness and soundness requirements for verification of optimal quantum channels as follows.

Definition 9. An optimal-quantum-channel verification, with respect to threshold average fidelity $\bar{F}_{\text{t}}$ and maximal failure probability δ, satisfies

1. completeness: if $\bar{F}_{\mathcal{E}_{\text{p}}} = \bar{F}_{\max}$, then the verifier accepts with probability no less than $1 - \delta$;

2. soundness: if $\bar{F}_{\mathcal{E}_\mathrm{p}} \leq \bar{F}_\mathrm{t}$, then the verifier rejects with probability no less than $1-\delta$.

To guarantee quantum-channel verification makes sense in practice, the verifier should accept any quantum channel in a neighbourhoood of $\mathcal{E}_\mathrm{opt}$ in the topological space of all CPTP maps induced by the average fidelity in Eq. (6.37).

In order to verify whether $\mathcal{E}_\mathrm{p}$ is optimal, one way is to follow the procedures of the canonical average-fidelity-based benchmark test in Subsec. 6.3. In general, however, $O_{\mathrm{A}'\mathrm{R}}$ in Eq. (6.41) is not feasibly measured. Here we define average-fidelity witness, which yields a tight lower bound of the average fidelity and develop a quantum-channel verification protocol involving measurement of an average-fidelity witness.

Definition 10. An observable $W_{\mathrm{A}'\mathrm{R}}$ is an average-fidelity witness for $\bar{F}_\mathcal{E}$ on the state $\mathcal{E}\otimes\mathcal{I}\left(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}\right)$ if

$$\mathcal{W}(\mathcal{E}) \coloneqq \mathrm{tr}\left[W_{\mathrm{A}'\mathrm{R}}\mathcal{E}\otimes\mathcal{I}\left(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}\right)\right] \tag{7.5}$$

satisfies

1. $\mathcal{W}(\mathcal{E}) = \bar{F}_\mathcal{E} \Longleftrightarrow \bar{F}_\mathcal{E} = \bar{F}_\mathrm{max}$; (7.6)

2. $\forall\mathcal{E}, \mathcal{W}(\mathcal{E}) \leq \bar{F}_\mathcal{E}$. (7.7)

Analogous to the fidelity witness, measuring the average-fidelity witness distinguishes the optimal quantum channels from all quantum channels, whose average fidelity is below the threshold.

The verification game between the verifier and the prover can also be interpreted by a query model: copies of quantum channel $\mathcal{E}$ are obtained via queries from a black box to decide whether $\mathcal{E}$ is optimal or not in terms of average fidelity. Given certain classical descriptions of input and target-output ensembles, the black box, each time, outputs one independent and identical copy of a quantum channel. The query complexity describes how many copies of $\mathcal{E}$ are demanded from the black box, in order to have a reliable answer on whether $\mathcal{E}$ is optimal or not. As estimating the mean value of an average-fidelity witness is sampling the mean value of an unknown distribution, we use sampling complexities, instead of query complexities, from now on, to infer how the number of

copies of $\mathcal{E}$ scales with the size of the classical description of input and target-output ensembles. We present our general framework of a verification protocol for optimal quantum channels in Algorithm 3.

Algorithm 3 General verification protocol for optimal quantum channels

Input:

- p_x ▷ Probability distribution
- classical description of ρ_x ▷ Input states
- classical description of $|\phi_x\rangle\langle\phi_x|$ ▷ Output target states
- $\bar{F}_{\mathrm{t}} \in (0, \bar{F}_{\max})$ ▷ threshold average fidelity
- $\delta \in \left(0, \frac{1}{2}\right)$ ▷ maximal failure probability
- $\varepsilon \in \left(0, \frac{\bar{F}_{\max} - \bar{F}_{\mathrm{t}}}{2}\right)$ ▷ error bound
- $\mathcal{E}_{\mathrm{p}} \in \mathcal{QC}[\mathscr{F}^{\otimes m}][\mathscr{F}^{\otimes m}]$ ▷ The sample complexity depends on both δ and ε.
- $|\Psi\rangle_{\mathrm{AR}} \in \mathcal{QS}[\mathscr{F}^{\otimes 2}]$ ▷ The number of copies of $|\Psi\rangle_{\mathrm{AR}}$ depends on that of $\mathcal{E}_{\mathrm{p}}$.

Output:

- $b \in \{0,1\}$ ▷ 0 means reject and 1 means accept.

procedure VERIFICATIONOFOPTIMALCHANNELS(p_x, x, classical description of ρ_x and $|\phi_x\rangle\langle\phi_x|$, $\bar{F}_{\mathrm{t}}$, δ, ε, $\mathcal{E}_{\mathrm{p}}$, $|\Psi\rangle_{\mathrm{AR}}$)
  send system A of each copy of $|\Psi\rangle_{\mathrm{AR}}$ through one copy of $\mathcal{E}_{\mathrm{p}}$;
  apply local measurements on each $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}\right)$ to measure $W_{\mathrm{A'R}}$;
    ▷ $W_{\mathrm{A'R}}$ is a tight lower bound of the observable $O_{\mathrm{A'R}}$ in Eq. (6.41).
  by processing measurement outcomes, obtain an estimate $\mathcal{W}(\mathcal{E}_{\mathrm{p}})^*$ of $\mathcal{W}(\mathcal{E}_{\mathrm{p}})$; ▷ With probability no less than $1-\delta$,

$$\mathcal{W}(\mathcal{E}_{\mathrm{p}})^* \in [\mathcal{W}(\mathcal{E}_{\mathrm{p}}) - \varepsilon, \mathcal{W}(\mathcal{E}_{\mathrm{p}}) + \varepsilon]. \tag{7.8}$$

  if $\mathcal{W}(\mathcal{E}_{\mathrm{p}})^* \geq \bar{F}_{\mathrm{t}} + \varepsilon$ **then**
    return $b = 1$;
  else
    return $b = 0$.
  end if
end procedure

This general verification protocol satisfies both the completeness and soundness conditions in definition 9. If $\mathcal{E}_{\mathrm{p}}$ is an optimal quantum channel, then $\mathcal{W}(\mathcal{E}_{\mathrm{p}}) = \bar{F}_{\max}$. Hence, with probability at least $1-\delta$,

$$\mathcal{W}(\mathcal{E}_{\mathrm{p}})^* \geq \bar{F}_{\max} - \varepsilon > \bar{F}_{\mathrm{t}} + 2\varepsilon - \varepsilon = \bar{F}_{\mathrm{t}} + \varepsilon. \tag{7.9}$$

If $\bar{F}_{\mathcal{E}_{\mathrm{p}}} \leq \bar{F}_{\mathrm{t}}$, with probability at least $1-\delta$,

$$\mathcal{W}(\mathcal{E}_{\mathrm{p}})^{*} \leq \mathcal{W}(\mathcal{E}_{\mathrm{p}}) + \varepsilon < s_{\mathcal{E}_{\mathrm{p}}} + \varepsilon \leq \bar{F}_{\mathrm{t}} + \varepsilon. \tag{7.10}$$

Using the decision-making procedure, we conclude that this protocol satisfies the completeness and soundness conditions.

From the continuity of the function $\mathcal{W}(\mathcal{E}_p)$ at optimal quantum channels, a neighborhood of optimal channels exists in the topological space of CPTP maps, such that $\forall\, \mathcal{E}_{\mathrm{p}}$ in this neighborhood satisfies

$$\mathcal{W}(\mathcal{E}_{\mathrm{p}}) \geq \bar{F}_{\mathrm{t}} + 2\varepsilon. \tag{7.11}$$

Hence, with probability at least $1-\delta$,

$$\mathcal{W}(\mathcal{E}_{\mathrm{p}})^{*} \geq \bar{F}_{\mathrm{t}} + \varepsilon. \tag{7.12}$$

It indicates that the verifier accepts any quantum channel in a neighborhood of the optimal channels, with high probability, in the topological space.

This section has presented our general scheme on how to verify an optimal quantum channel in terms of average fidelity. We have mathematically defined optimal-quantum-channel verification and average-fidelity witness. In the next section, we present examples of this general verification protocol by measuring experimentally feasible average-fidelity witnesses.

7.2 Verification of bosonic channels

In this section, we present two verification protocols, one for multi-mode Gaussian unitary channels, the other for single-mode amplification channels. All operations and sample complexities in the protocols are specified. The verification operations only require the preparation of two-mode squeezed vacuum states and the application of local homodyne detections. The sample complexities scale polynomially with respect to all channel-specification parameters. In both protocols,

we devise experimentally feasible average-fidelity witnesses, the mean values of which, can be sampled by local homodyne detections.

7.2.1 Verification of multi-mode Gaussian unitary channels

In this subsection, we present a verification protocol for multi-mode Gaussian unitary channels. Central to this verification protocol is an average-fidelity witness, and we show that the mean value of this witness can be estimated by sampling the means and the covariance matrix of quadrature operators.

Here we investigate a verification protocol for the optimal quantum channel in terms of average fidelity

$$\bar{F}(\mathcal{E},\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}) \coloneqq \int \frac{\mathrm{d}^{2m}\boldsymbol{\alpha}}{\pi^m}\lambda^m \mathrm{e}^{-\lambda|\boldsymbol{\alpha}|^2}\langle\boldsymbol{\alpha}|U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}\mathcal{E}(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)U_{\boldsymbol{S},\boldsymbol{d}}|\boldsymbol{\alpha}\rangle\rangle, \tag{7.13}$$

where

$$\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}(\rho) = U_{\boldsymbol{S},\boldsymbol{d}}\rho U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}, \tag{7.14}$$

is the unitary quantum channel and

$$|\boldsymbol{\alpha}\rangle \coloneqq |\alpha_1\rangle\otimes|\alpha_2\rangle\otimes\cdots\otimes|\alpha_m\rangle\,,\ \boldsymbol{\alpha}\coloneqq(\alpha_1,\alpha_2,\ldots,\alpha_m)\in\mathbb{C}^{\otimes m} \tag{7.15}$$

is a product of m coherent states. Evidently, $\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}$ achieves unity average fidelity (7.13).

The verification protocol for the optimal quantum channel in terms of the average fidelity (7.13) is presented in Algorithm 4. The schematic diagram of the verification scheme is shown in Fig. 7.1.

Now we devise an average-fidelity witness for the average fidelity in Eq. (7.13) and show that its mean value is a linear combination of $\boldsymbol{\gamma}$, $\boldsymbol{\Gamma}_1$ and $\boldsymbol{\Gamma}_2$. Hence, the mean value of the witness can be estimated by the measurement and classical-information processing schemes in Algorithm 4.

Theorem 11. *The observable*

$$\mathbb{1} - \frac{\lambda}{\lambda+1}U_{\boldsymbol{S},\boldsymbol{d}}\otimes\mathbb{1}\left(\sum_{i=1}^{m}S_{\kappa}\hat{n}_i\otimes\mathbb{1}S_{\kappa}^{\dagger}\right)U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}\otimes\mathbb{1}, \tag{7.17}$$

Algorithm 4 Verification protocol for multi-mode Gaussian unitary operations

Input:

- $\frac{1}{\lambda} > 0$ ▷ variance of the prior Gaussian distribution
- $\boldsymbol{S} \in \mathrm{Sp}(2m, \mathbb{R})$ ▷ symplectic transformation of target Gaussian unitary operation
- $\boldsymbol{d} \in \mathbb{R}^{2m}$ ▷ displacement vector of target Gaussian unitary operation
- $\bar{F}_{\mathrm{t}} \in (0,1)$ ▷ threshold average fidelity
- $\delta \in \left(0, \frac{1}{2}\right)$ ▷ maximal failure probability
- $\varepsilon \in \left(0, \frac{1-\bar{F}_{\mathrm{t}}}{2}\right)$ ▷ error bound
- $\mathcal{E}_{\mathrm{p}} \in \mathcal{QC}[\mathscr{F}][\mathscr{F}]$ ▷ $2mc_3 + m(2m+1)c_4 + 4m^2c_5$ copies of $\mathcal{E}_{\mathrm{p}}$
- $|\kappa\rangle_{\mathrm{TMSV}} \in \mathcal{QS}[\mathscr{F}^{\otimes 2}]$ ▷ $2m^2c_3 + m^2(2m+1)c_4 + 4m^3c_5$ copies of $|\kappa\rangle_{\mathrm{TMSV}}$, where

$$|\kappa\rangle_{\mathrm{TMSV}} = S_\kappa |0\rangle_{\mathscr{F}} \text{ for } \kappa = \operatorname{arctanh} \frac{1}{\sqrt{\lambda+1}} \tag{7.16}$$

- $\sigma_1 > 0$ ▷ upper bound of the variance of any $\hat{\boldsymbol{x}}_l^{\mathrm{A}'}$, $1 \le l \le 2m$, on $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$.
- $\sigma_2 > 0$ ▷ upper bound of the variance of any $\frac{1}{2}\left(\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\hat{\boldsymbol{x}}_v^{\mathrm{A}'} + \hat{\boldsymbol{x}}_v^{\mathrm{A}'}\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\right)$ and $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\hat{\boldsymbol{x}}_v^{\mathrm{R}}$ on $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$, where $1 \le u, v \le 2m$.

Output:

- $b \in \{0,1\}$ ▷ 0 means reject and 1 means accept.

procedure VERIFICATIONOFGAUSSIANUNITARYOPERATIONS($\frac{1}{\lambda}$, $\boldsymbol{S}$, $\boldsymbol{d}$, $\bar{F}_{\mathrm{t}}$, δ, ε, σ_1, σ_2, $\mathcal{E}_{\mathrm{p}}$, $|\kappa\rangle_{\mathrm{TMSV}}$)
  for each copy of $\mathcal{E}_{\mathrm{p}}$ **do**
    for $j = 1 : m$ **do**
      send one mode of one copy of $|\kappa\rangle_{\mathrm{TMSV}}$ into j-input of $\mathcal{E}_{\mathrm{p}}$;
      keep the other mode as a reference mode;
    end for
  end for
  for $l = 1 : 2m$ **do**
    for $i = 1 : c_3$ **do** ▷ To estimate $\boldsymbol{\gamma} := \bar{\boldsymbol{x}}_{\mathrm{A}'} \in \mathbb{R}^{2m}$.
      apply a single-shot homodyne detection for quadrature $\hat{\boldsymbol{x}}_l^{\mathrm{A}'}$ on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$;
    end for
    $\gamma_l^* \leftarrow \frac{1}{c_3}\sum_{i=1}^{c_3} \chi_i^{\hat{\boldsymbol{x}}_l^{\mathrm{A}'}}$;
  ▷ $\boldsymbol{\gamma}^*$ is an estimate of $\boldsymbol{\gamma}$. $\chi_i^{\hat{\boldsymbol{x}}_l^{\mathrm{A}'}}$ is ith measurement outcome with respect to quadrature $\hat{\boldsymbol{x}}_l^{\mathrm{A}'}$.
    for $i = 1 : c_4$ **do** ▷ To estimate the diagonal elements in $\boldsymbol{\Gamma}_1 := \left\langle \hat{\boldsymbol{x}}_{\mathrm{A}'}\hat{\boldsymbol{x}}_{\mathrm{A}'}^{\top} \right\rangle \in \mathbb{R}^{2m\times 2m}$.
      apply a single-shot homodyne detection for quadrature $\hat{\boldsymbol{x}}_l^{\mathrm{A}'}$ on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$;
    end for

$(\boldsymbol{\Gamma}_1^*)_{uu} \leftarrow \frac{1}{c_4}\sum_{i=1}^{c_4}\left(\chi_i^{\hat{\boldsymbol{x}}_u^{\mathrm{A}'}}\right)^2$; ▷ $\boldsymbol{\Gamma}_1^*$ is an estimate of $\boldsymbol{\Gamma}_1$.

end for

for $u = 1:2m$ **do** ▷ To estimate the off-diagonal elements in $\boldsymbol{\Gamma}_1$.

for $v = 1:u-1$ **do**

if $(u,v) \neq (2j, 2j-1)$ for $j \in \{1,2,\ldots,m\}$ **then**

for $i = 1:c_4$ **do**

apply two single-shot homodyne detections for quadratures $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}$ and $\hat{\boldsymbol{x}}_v^{\mathrm{A}'}$ simultaneously on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$;

end for

$(\boldsymbol{\Gamma}_1^*)_{uv} \leftarrow \frac{1}{c_4}\sum_{i=1}^{c_4}\chi_i^{\hat{\boldsymbol{x}}_u^{\mathrm{A}'}}\chi_i^{\hat{\boldsymbol{x}}_v^{\mathrm{A}'}}$;

else

for $i = 1:c_4$ **do**

apply a single-shot homodyne detection for quadrature $\frac{1}{\sqrt{2}}\left(\hat{\boldsymbol{x}}_u^{\mathrm{A}'} + \hat{\boldsymbol{x}}_v^{\mathrm{A}'}\right)$ on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$;

end for

$(\boldsymbol{\Gamma}_1^*)_{uv} \leftarrow \frac{1}{c_4}\sum_{i=1}^{c_4}\left(\chi_i^{\frac{1}{\sqrt{2}}\left(\hat{\boldsymbol{x}}_u^{\mathrm{A}'}+\hat{\boldsymbol{x}}_v^{\mathrm{A}'}\right)}\right)^2 - \frac{1}{2}(\boldsymbol{\gamma}_u^*)^2 - \frac{1}{2}(\boldsymbol{\gamma}_v^*)^2$;

end if

$(\boldsymbol{\Gamma}_1^*)_{vu} \leftarrow (\boldsymbol{\Gamma}_1^*)_{uv}$;

end for

end for

for $u = 1:2m$ **do** ▷ To estimate $\boldsymbol{\Gamma}_2 \coloneqq \left\langle \hat{\boldsymbol{x}}_{\mathrm{A}'}\hat{\boldsymbol{x}}_{\mathrm{R}}^{\top}\right\rangle \in \mathbb{R}^{2m\times 2m}$.

for $v = 1:2m$ **do**

for $i = 1:c_5$ **do**

apply two single-shot homodyne detection for $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}$ and $\hat{\boldsymbol{x}}_v^{\mathrm{R}}$ simultaneously on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$;

end for

$(\boldsymbol{\Gamma}_2^*)_{uv} \leftarrow \frac{1}{c_5}\sum_{i=1}^{c_5}\chi_i^{\hat{\boldsymbol{x}}_u^{\mathrm{A}'}}\chi_i^{\hat{\boldsymbol{x}}_v^{\mathrm{R}}}$; ▷ $\boldsymbol{\Gamma}_2^*$ is an estimate of $\boldsymbol{\Gamma}_2$.

$(\boldsymbol{\Gamma}_2^*)_{vu} \leftarrow (\boldsymbol{\Gamma}_2^*)_{uv}$;

end for

end for

$\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})^* \leftarrow -\frac{1}{2}\mathrm{tr}\left[\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}\left(\boldsymbol{\Gamma}_1^* - 2\boldsymbol{\gamma}^*\boldsymbol{d}^{\top} + \boldsymbol{d}\boldsymbol{d}^{\top}\right)\right] + \frac{1}{\sqrt{\lambda+1}}\mathrm{tr}\left(\boldsymbol{Z}^{\oplus m}\boldsymbol{S}^{-1}\boldsymbol{\Gamma}_2^*\right) + \frac{m(\lambda^2-2\lambda-4)}{2\lambda(\lambda+1)} + 1$;

▷ Obtain an estimate $\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})^*$ of $\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})$ in Eq. (7.54).

if $\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})^* \geq \bar{F}_{\mathrm{t}} + \varepsilon$ **then**

return $b = 1$;

else

return $b = 0$.

end if

end procedure

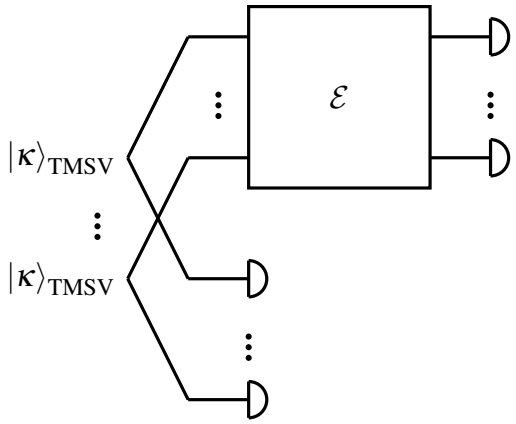


Figure 7.1: Our verification scheme for a multi-mode Gaussian unitary channel. Each $|\kappa\rangle_{\mathrm{TMSV}}$ denotes a two-mode squeezed vacuum state with squeezing parameter κ. One mode of each $|\kappa\rangle_{\mathrm{TMSV}}$ goes through a multi-mode unknown bosonic quantum channel, denoted by $\mathcal{E}$ and represented by a square. Homodyne detections, represented by semicircles, are applied at each output mode of $\mathcal{E}$ and the other mode of each $|\kappa\rangle_{\mathrm{TMSV}}$.

where

$$S_\kappa := \mathrm{e}^{\frac{\kappa}{2}\left(\hat{a}_1\hat{a}_2+\hat{a}_1^\dagger\hat{a}_2^\dagger\right)}, \tag{7.18}$$

is an average-fidelity witness for $\bar{F}(\mathcal{E},\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}})$ *on* $\mathcal{E}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$.

From now on, we use $W_{U_{\boldsymbol{S},\boldsymbol{d}}}$ to denote the average-fidelity witness (7.17). To show Theorem 11, we need Lemmas 12 and 13.

Lemma 12. *Given performance operator*

$$\Pi_{\mathrm{A'A}} = \int \frac{d^2\alpha}{\pi}\lambda \mathrm{e}^{-\lambda|\alpha|^2}\,|\mathfrak{g}\alpha\rangle\langle\mathfrak{g}\alpha|\otimes|\alpha\rangle\langle\alpha|, \tag{7.19}$$

where $\mathfrak{g}>0$*, and input state* $|\Psi\rangle_{\mathrm{AR}} = |\kappa\rangle_{\mathrm{TMSV}}$*, if* $\mathfrak{g}\leq\sqrt{\lambda+1}$*, then*

$$O_{\mathrm{A'R}} = S_\theta(G_\theta\otimes\mathbb{1})S_\theta^\dagger, \tag{7.20}$$

where

$$G_\theta = \sum_{n=0}^{\infty}\tanh^{2n}\theta\,|n\rangle\langle n| \tag{7.21}$$

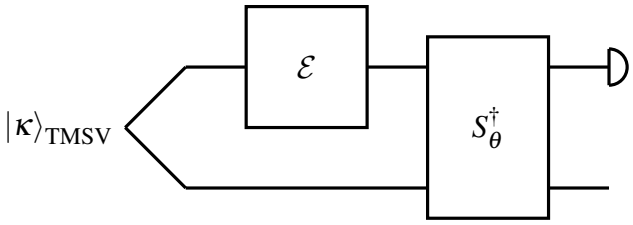


Figure 7.2: Previous benchmarking scheme for a single-mode bosonic amplification/attenuation channel [12]. $|\kappa\rangle_{\text{TMSV}}$ denotes a two-mode squeezed vacuum state with squeezing parameter κ. One mode of $|\kappa\rangle_{\text{TMSV}}$ goes through $\mathcal{E}$. The square, denoted by $\mathcal{E}$, represents a single-mode unknown bosonic quantum channel. The output mode of $\mathcal{E}$ and the other mode of $|\kappa\rangle_{\text{TMSV}}$ go through an online two-squeezing operation, denoted by $S_\theta^\dagger$ and represented by a rectangle. A heterodyne detection, represented by a semicircle, is applied at one final output mode, and the other output mode is discarded.

and

$$\theta = \operatorname{arctanh} \frac{\mathfrak{g}}{\sqrt{\lambda+1}}; \tag{7.22}$$

otherwise,

$$O_{\text{A}'\text{R}} = \tanh^2 \theta' S_{\theta'}(\mathbb{1} \otimes G_{\theta'}) S_{\theta'}^\dagger, \tag{7.23}$$

where

$$\theta' = \operatorname{arctanh} \frac{\sqrt{\lambda+1}}{\mathfrak{g}}. \tag{7.24}$$

Ref. [12] has shown the results in Lemma 12, except missing the constant $\tanh^2 \theta'$ in Eq. (7.23).

Proof. The purification of thermal state $\rho_{\text{A}} = \rho_T(\frac{1}{\lambda})$ is a two-mode squeezed vacuum state

$$|\Psi\rangle_{\text{AR}} = \sqrt{\frac{\lambda}{1+\lambda}} \sum_{n=0}^{\infty} \left(\frac{1}{1+\lambda}\right)^{\frac{n}{2}} |n\rangle_{\text{A}} |n\rangle_{\text{R}}. \tag{7.25}$$

The reduced states on A and R are

$$\rho_{\text{A}} = \rho_{\text{R}} = \frac{\lambda}{1+\lambda} \sum_{n=0}^{\infty} \left(\frac{1}{1+\lambda}\right)^{n} |n\rangle \langle n|. \tag{7.26}$$

Thus,

$$T_{\text{AR}} = \mathbb{1} \tag{7.27}$$

is an identity map on $\mathscr{H}$.

Plugging Eqs. (7.19), (7.26) and (7.27) into Eq. (6.41), we obtain [12]

$$O_{\mathrm{A'R}} = \int \frac{\mathrm{d}^2\alpha}{\pi} \Big| \frac{\mathfrak{g}\alpha}{\sqrt{\lambda+1}} \Big\rangle \Big\langle \frac{\mathfrak{g}\alpha}{\sqrt{\lambda+1}} \Big| \otimes |\bar{\alpha}\rangle \langle\bar{\alpha}| . \tag{7.28}$$

If $g \leq \sqrt{\lambda+1}$, we have

$$\forall \alpha \in \mathbb{C},\ S_\theta \mathbb{1} \otimes D\left(\frac{\bar{\alpha}}{\cosh\theta}\right) S_\theta^\dagger = D\left(\frac{\mathfrak{g}\alpha}{\sqrt{\lambda+1}}\right) \otimes D(\bar{\alpha}). \tag{7.29}$$

Then $O_{\mathrm{A'R}}$ (7.28) can be further simplified to

$$\begin{aligned} O_{\mathrm{A'R}} =& \int \frac{\mathrm{d}^2\alpha}{\pi} S_\theta \mathbb{1} \otimes D\left(\frac{\bar{\alpha}}{\cosh\theta}\right) S_\theta^\dagger |0\rangle_{\mathscr{F}} \langle 0| \otimes |0\rangle_{\mathscr{F}} \langle 0| S_\theta \mathbb{1} \otimes D\left(\frac{\bar{\alpha}}{\cosh\theta}\right)^\dagger S_\theta^\dagger \\ =& \cosh^2\theta \int \frac{\mathrm{d}^2\alpha}{\pi} S_\theta \left(\mathbb{1} \otimes D(\alpha)\right) S_\theta^\dagger |0\rangle_{\mathscr{F}} \langle 0| \otimes |0\rangle_{\mathscr{F}} \langle 0| S_\theta \left(\mathbb{1} \otimes D(\alpha)^\dagger\right) S_\theta^\dagger \\ =& S_\theta G_\theta \otimes \mathbb{1} S_\theta^\dagger. \end{aligned} \tag{7.30}$$

In Eq. (7.30), we use the fact that the Heisenberg-Weyl group forms a unitary 1-design [18, 127]; i.e.,

$$\int \frac{\mathrm{d}^2\alpha}{\pi} D(\alpha) \rho D(\alpha)^\dagger = \mathbb{1}, \tag{7.31}$$

for any single-mode density operator ρ.

If $\mathfrak{g} \geq \sqrt{\lambda+1}$,

$$\forall \alpha \in \mathbb{C},\ S_{\theta'} \left(D\left(\frac{\alpha}{\sinh\theta'}\right) \otimes \mathbb{1}\right) S_{\theta'}^\dagger = D\left(\frac{\mathfrak{g}\alpha}{\sqrt{\lambda+1}}\right) \otimes D(\bar{\alpha}), \tag{7.32}$$

for $\theta' = \operatorname{arctanh}\frac{\sqrt{\lambda+1}}{\mathfrak{g}}$. $O_{\mathrm{A'R}}$ in Eq. (7.28) can be simplified to

$$\begin{aligned} O &= \int \frac{\mathrm{d}^2\alpha}{\pi} S_{\theta'} \left(D\left(\frac{\alpha}{\sinh\theta'}\right) \otimes \mathbb{1} \right) S_{\theta'}^\dagger \left|0\right\rangle_{\mathscr{F}} \left\langle 0\right| \otimes \left|0\right\rangle_{\mathscr{F}} \left\langle 0\right| S_{\theta'} \left(D\left(\frac{\alpha}{\sinh\theta'}\right)^\dagger \otimes \mathbb{1} \right) S_{\theta'}^\dagger \\ &= \sinh^2\theta' \int \frac{\mathrm{d}^2\alpha}{\pi} S_{\theta'} \left(D(\alpha) \otimes \mathbb{1} \right) S_{\theta'}^\dagger \left|0\right\rangle_{\mathscr{F}} \left\langle 0\right| \otimes \left|0\right\rangle_{\mathscr{F}} \left\langle 0\right| S_{\theta'} \left(D(\alpha)^\dagger \otimes \mathbb{1} \right) S_{\theta'}^\dagger \\ &= \tanh^2\theta' S_{\theta'} \mathbb{1} \otimes G_{\theta'} S_{\theta'}^\dagger, \end{aligned} \tag{7.33}$$

where we use Eq. (7.31) again to obtain Eq. (7.33). Thus, we have proved Lemma 12. □

Lemma 12 implies that by applying two-mode squeezing and measuring G_θ at one mode, the verifier can directly estimate the average fidelity. As

$$G_\theta = \coth^2\theta \int \frac{\mathrm{d}^2\alpha}{\pi} \mathrm{e}^{-\frac{|\alpha|^2}{\sinh^2\theta}} \left|\alpha\right\rangle \left\langle\alpha\right|, \tag{7.34}$$

the mean value of G_θ can be estimated by using heterodyne detections [12]. This benchmark scheme also requires quantum memory to keep the entanglement between the output mode and the reference mode, and online two-mode squeezing to squeeze the combination of an unknown quantum state at the output mode and a thermal state at the reference mode. The schematic diagram of this method, devised in [12], is shown in Fig. 7.2. However, the combination of quantum memory, online squeezing, and heterodyne detections is experimentally challenging.

To devise an experimentally feasible verification scheme, we find lower bounds of the observables in Lemma 12 using the lemma below.

Lemma 13. *For any $\theta > 0$, $m \in \mathbb{N}^+$,*

$$G_\theta^{\otimes m} \geq \mathbb{1} - \frac{\sum_{i=1}^m \hat{n}_i}{\cosh^2\theta}. \tag{7.35}$$

As far as we know, the inequality in Lemma 13 is novel and has not appeared in any previous literatures.

Proof. We first prove that $G_\theta \geq \mathbb{1} - \frac{\hat{n}}{\bar{n}_T+1}$. This can be seen by

$$\begin{aligned}\mathbb{1} - \frac{\hat{n}}{\bar{n}_T+1} &= \sum_{n=0}^{\infty} \left(1 - \frac{n}{\bar{n}_T+1}\right) |n\rangle\langle n| \\ &= \sum_{n=0}^{\infty} \frac{\bar{n}_T+1-n}{\bar{n}_T+1} |n\rangle\langle n| \\ &= \sum_{n=0}^{\infty} (1 - n\,\mathrm{sech}^2\theta) |n\rangle\langle n|. \end{aligned} \tag{7.36}$$

From the binomial inequality,

$$1 - n\,\mathrm{sech}^2\theta \leq \left(1 - \mathrm{sech}^2\theta\right)^n = \tanh^{2n}\theta. \tag{7.37}$$

Combining Eqs. (7.21) and (7.36), we have

$$G_\theta \geq \mathbb{1} - \frac{\hat{n}}{\bar{n}_T+1}. \tag{7.38}$$

Next we use this result to prove the lemma by induction. Suppose

$$G_\theta^{\otimes(m-1)} \geq \mathbb{1} - \frac{\sum_{i=1}^{m-1}\hat{n}_i}{\bar{n}_T+1}, \tag{7.39}$$

then

$$G_\theta^{\otimes m} \geq \left(\mathbb{1} - \frac{\sum_{i=1}^{m-1}\hat{n}_i}{\bar{n}_T+1}\right)\left(\mathbb{1} - \frac{\hat{n}_m}{\bar{n}_T+1}\right) \geq \mathbb{1} - \frac{\sum_{i=1}^{m}\hat{n}_i}{\bar{n}_T+1}. \tag{7.40}$$

Thus, we have proved Lemma 13. □

Combining Lemma 13 with Lemma 12, we obtain the observable in Eq. (7.17). Now we prove Theorem 11.

Proof. From Eq. (6.44), we know that the performance operator, in the test of average fidelity $\bar{F}\left(\mathcal{E}, \mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}\right)$, is

$$\Pi_{\mathrm{A'A}} = \int \frac{\mathrm{d}^{2m}\boldsymbol{\alpha}}{\pi^m} \lambda^m \mathrm{e}^{-\lambda|\boldsymbol{\alpha}|^2} U_{\boldsymbol{S},\boldsymbol{d}} |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}| U_{\boldsymbol{S},\boldsymbol{d}}^\dagger \otimes |\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|. \tag{7.41}$$

Using Eq. (7.20) for the tensor product of m modes, we obtain the observable

$$O_{\mathrm{A'R}} = U_{\boldsymbol{S},\boldsymbol{d}} \otimes \mathbb{1} S_{\boldsymbol{\kappa}}^{\otimes m} G_{\boldsymbol{\kappa}}^{\otimes m} \otimes \mathbb{1} S_{\boldsymbol{\kappa}}^{\dagger \otimes m} U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} \otimes \mathbb{1}, \tag{7.42}$$

such that

$$\bar{F}(\mathcal{E}, \mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}) = \mathrm{tr}\left[O_{\mathrm{A'R}} \mathcal{E} \otimes \mathcal{I}\left(|\boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}|_{\mathrm{TMSV}}^{\otimes m} \right) \right]. \tag{7.43}$$

In Eq. (7.42), each $G_{\boldsymbol{\kappa}}$ acts on one output mode, each $S_{\boldsymbol{\kappa}}$ acts on one output mode and the associated reference mode, and $U_{\boldsymbol{S},\boldsymbol{d}}$ acts on the m output modes. To perform the operator multiplication in Eq. (7.42), the operators must be represented on the Hilbert spaces with one specific order, like $\mathrm{A}'_1, \ldots, \mathrm{A}'_m, \mathrm{R}_1, \ldots, \mathrm{R}_m$.

Plugging inequality (7.35) into Eqs. (7.42) and (7.43) yields

$$\bar{F}(\mathcal{E}, \mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}) \geq \mathrm{tr}\left[W_{U_{\boldsymbol{S},\boldsymbol{d}}} \mathcal{E} \otimes \mathcal{I}\left(|\boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}|_{\mathrm{TMSV}}^{\otimes m} \right) \right], \tag{7.44}$$

which proves condition (7.7). On the other hand, from Eqs. (7.42) and (7.43), we have

$$\bar{F}(\mathcal{E}, \mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}) = \mathrm{tr}\left\{ G_{\boldsymbol{\theta}} \, \mathrm{tr}_{\mathrm{R}}\left[S_{\boldsymbol{\kappa}}^{\dagger \otimes m} U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} \otimes \mathbb{1} \mathcal{E} \otimes \mathcal{I}\left(|\boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}|_{\mathrm{TMSV}}^{\otimes m} \right) U_{\boldsymbol{S},\boldsymbol{d}} \otimes \mathbb{1} S_{\boldsymbol{\kappa}}^{\otimes m} \right] \right\}. \tag{7.45}$$

Using Eq. (7.21), we know that $\mathcal{E}$ is an optimal channel, i.e., $\bar{F}(\mathcal{E}, \mathcal{U}_{\boldsymbol{S},\boldsymbol{d}})$ achieves one, iff

$$\mathrm{tr}_{\mathrm{R}}\left[S_{\boldsymbol{\kappa}}^{\dagger \otimes m} U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} \otimes \mathbb{1} \mathcal{E} \otimes \mathcal{I}\left(|\boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}|_{\mathrm{TMSV}}^{\otimes m} \right) U_{\boldsymbol{S},\boldsymbol{d}} \otimes \mathbb{1} S_{\boldsymbol{\kappa}}^{\otimes m} \right] = |0\rangle_{\mathscr{F}} \langle 0|^{\otimes m}, \tag{7.46}$$

which is further equivalent to

$$\mathrm{tr}\left[W_{U_{\boldsymbol{S},\boldsymbol{d}}} \mathcal{E} \otimes \mathcal{I}\left(|\boldsymbol{\kappa}\rangle \langle \boldsymbol{\kappa}|_{\mathrm{TMSV}}^{\otimes m} \right) \right] = 1. \tag{7.47}$$

This proves condition (7.6). Thus, $W_{U_{\boldsymbol{S},\boldsymbol{d}}}$ is an average-fidelity witness for $\bar{F}(\mathcal{E}, \mathcal{U}_{\boldsymbol{S},\boldsymbol{d}})$. □

Next we show that the expectation value of the average-fidelity witness

$$\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}}) \coloneqq \mathrm{tr}\left[W_{U_{\boldsymbol{S},\boldsymbol{d}}}\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)\right] \tag{7.48}$$

is a linear combination of the mean values of quadrature operators, $\boldsymbol{\gamma}$, and the covariances of quadrature operators, $\boldsymbol{\Gamma}_1$ and $\boldsymbol{\Gamma}_2$. We rewrite each photon number operator in terms of position and momentum operators,

$$\hat{n} = \frac{\hat{\boldsymbol{x}}^{\top}\hat{\boldsymbol{x}} - m}{2}. \tag{7.49}$$

By applying the inverse transformations of (2.186)

$$S_{\kappa}^{\otimes m}\begin{bmatrix}\hat{\boldsymbol{x}}_{\mathrm{A}'}\\ \hat{\boldsymbol{x}}_{\mathrm{R}}\end{bmatrix}S_{\kappa}^{\otimes m\dagger} = \begin{bmatrix}\cosh\kappa\mathbb{1}^{\oplus m} & -\sinh\kappa\boldsymbol{Z}^{\oplus m}\\ -\sinh\kappa\boldsymbol{Z}^{\oplus m} & \cosh\kappa\mathbb{1}^{\oplus m}\end{bmatrix}\begin{bmatrix}\hat{\boldsymbol{x}}_{\mathrm{A}'}\\ \hat{\boldsymbol{x}}_{\mathrm{R}}\end{bmatrix}, \tag{7.50}$$

and the inverse transformation of (2.167)

$$U_{\boldsymbol{S},\boldsymbol{d}}\hat{\boldsymbol{x}}_{\mathrm{A}'}U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger} = \boldsymbol{S}^{-1}(\hat{\boldsymbol{x}}_{\mathrm{A}'} - \boldsymbol{d}), \tag{7.51}$$

we write $W_{U_{\boldsymbol{S},\boldsymbol{d}}}$ in terms of $\hat{\boldsymbol{x}}_{\mathrm{A}'}$ and $\hat{\boldsymbol{x}}_{\mathrm{R}}$,

$$W_{U_{\boldsymbol{S},\boldsymbol{d}}} = \cosh^2\kappa(\hat{\boldsymbol{x}}_{\mathrm{A}'}^{\top} - \boldsymbol{d}^{\top})\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}(\hat{\boldsymbol{x}}_{\mathrm{A}'} - \boldsymbol{d}) - \sinh(2\kappa)\hat{\boldsymbol{x}}_{\mathrm{R}}^{\top}\boldsymbol{Z}^{\oplus m}\boldsymbol{S}^{-1}(\hat{\boldsymbol{x}}_{\mathrm{A}'} - \boldsymbol{d}) + \sinh^2\kappa\hat{\boldsymbol{x}}_{\mathrm{R}}^{\top}\hat{\boldsymbol{x}}_{\mathrm{R}}. \tag{7.52}$$

As each reference mode is in a thermal state $\rho_T(\frac{1}{\lambda})$, for each $1 \leq l \leq 2m$,

$$\left\langle\left(\hat{\boldsymbol{x}}_l^{\mathrm{R}}\right)^2\right\rangle = \frac{\lambda+2}{\lambda}. \tag{7.53}$$

Using this fact and Eq. (7.16), we obtain

$$\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}}) = -\frac{1}{2}\mathrm{tr}\left[\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}\left(\boldsymbol{\Gamma}_1 - 2\boldsymbol{\gamma}\boldsymbol{d}^{\top} + \boldsymbol{d}\boldsymbol{d}^{\top}\right)\right] + \frac{1}{\sqrt{\lambda+1}}\mathrm{tr}\left(\boldsymbol{Z}^{\oplus m}\boldsymbol{S}^{-1}\boldsymbol{\Gamma}_2\right) + \frac{m(\lambda^2-2\lambda-4)}{2\lambda(\lambda+1)} + 1. \tag{7.54}$$

Eq. (7.54) implies that the mean value of the average-fidelity witness can be estimated by sampling the means and the covariance matrix of quadrature operators, as shown in Algorithm 4.

Theorem 14. *The verification protocol in Algorithm 4 requires* $2mc_3 + m(2m+1)c_4 + 4m^2c_5$ *copies of* $\mathcal{E}_{\mathrm{p}}$*, where*

$$c_3 \in O\left(\frac{m^4 \|\boldsymbol{S}\|_\infty^4 \|\boldsymbol{d}\|^2 \sigma_1^2}{\varepsilon^2 \ln(1/(1-\delta))}\right), \tag{7.55}$$

$$c_4 \in O\left(\frac{m^4 \|\boldsymbol{S}\|_\infty^4 \sigma_2^2}{\varepsilon^2 \ln(1/(1-\delta))}\right), \tag{7.56}$$

$$c_5 \in O\left(\frac{m^4 \|\boldsymbol{S}\|_\infty^2 \sigma_2^2}{\varepsilon^2 \ln(1/(1-\delta))}\right). \tag{7.57}$$

Proof. We denote the estimation errors as

$$\boldsymbol{\epsilon} := \boldsymbol{\gamma} - \boldsymbol{\gamma}^*, \tag{7.58}$$

$$\boldsymbol{E}_1 := \boldsymbol{\Gamma}_1 - \boldsymbol{\Gamma}_1^*, \tag{7.59}$$

$$\boldsymbol{E}_2 := \boldsymbol{\Gamma}_2 - \boldsymbol{\Gamma}_2^*. \tag{7.60}$$

The distance between $\mathcal{W}$ and experimental value $\mathcal{W}^*$ can be bounded

$$\begin{aligned}
\left|\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}}) - \mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})^*\right| \leq & \frac{1}{2}\left|\mathrm{tr}\left[\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}\left(\boldsymbol{E}_1 - 2\boldsymbol{\epsilon}\boldsymbol{d}^\top\right)\right]\right| + \frac{1}{\sqrt{\lambda+1}}\left|\mathrm{tr}\left(\boldsymbol{Z}^{\oplus m}\boldsymbol{S}^{-1}\boldsymbol{E}_2\right)\right| \\
\leq & \frac{1}{2}\left\|\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}\right\|_\infty \left\|\boldsymbol{E}_1 - 2\boldsymbol{\epsilon}\boldsymbol{d}^\top\right\|_1 + \frac{1}{\sqrt{\lambda+1}}\left\|\boldsymbol{Z}^{\oplus m}\boldsymbol{S}^{-1}\right\|_\infty \|\boldsymbol{E}_2\|_1
\end{aligned} \tag{7.61}$$

$$\leq \frac{1}{2}\left\|\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}\right\|_\infty (\|\boldsymbol{E}_1\|_1 + 2\|\boldsymbol{\epsilon}\|_1 \|\boldsymbol{d}\|_1) + \frac{1}{\sqrt{\lambda+1}}\left\|\boldsymbol{S}^{-1}\right\|_\infty \|\boldsymbol{E}_2\|_1, \tag{7.62}$$

where we use

$$|\mathrm{tr}(\boldsymbol{A}\boldsymbol{B})| \leq \|\boldsymbol{A}\|_\infty \|\boldsymbol{B}\|_1 \tag{7.63}$$

in (7.61), and

$$\|\boldsymbol{AB}\|_1 \leq \|\boldsymbol{A}\|_1 \|\boldsymbol{B}\|_1 \tag{7.64}$$

in (7.62) for any matrices $\boldsymbol{A}$ and $\boldsymbol{B}$.

From the singular value decomposition of the symplectic matrix $\boldsymbol{S}$, we obtain

$$\left\|\boldsymbol{S}^{-1}\right\|_\infty = \|\boldsymbol{S}\|_\infty \tag{7.65}$$

and

$$\left\|\boldsymbol{S}^{-\mathrm{T}}\boldsymbol{S}^{-1}\right\|_\infty = \|\boldsymbol{S}\|_\infty^2. \tag{7.66}$$

Plugging the inequalities

$$\|\boldsymbol{E}_1\|_1 \leq 2m \|\boldsymbol{E}_1\|_{\max}, \tag{7.67}$$

$$\|\boldsymbol{E}_2\|_1 \leq 2m \|\boldsymbol{E}_2\|_{\max}, \tag{7.68}$$

$$\|\boldsymbol{d}\|_1 \leq \sqrt{2m} \|\boldsymbol{d}\|, \tag{7.69}$$

$$\|\boldsymbol{\epsilon}\|_1 \leq 2m \|\boldsymbol{\epsilon}\|_\infty, \tag{7.70}$$

into Eq. (7.62), we have

$$\left|\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}}) - \mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})^*\right| \leq (2m)^{\frac{3}{2}} \|\boldsymbol{S}\|_\infty^2 \|\boldsymbol{\epsilon}\|_\infty \|\boldsymbol{d}\| + m\|\boldsymbol{S}\|_\infty^2 \|\boldsymbol{E}_1\|_{\max} + \frac{2m\|\boldsymbol{S}\|_\infty}{\sqrt{\lambda+1}} \|\boldsymbol{E}_2\|_{\max}. \tag{7.71}$$

To guarantee that

$$P\left(\left|\mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}}) - \mathcal{W}_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}})^*\right| \leq \varepsilon\right) \geq 1-\delta, \tag{7.72}$$

where $P(\cdot)$ denotes the probability of an event, we suppose each term on the right-hand side of (7.71) is less than $\frac{\varepsilon}{3}$ with probability no less than $(1-\delta)^{\frac{1}{3}}$. To determine sample complexity, we use the following lemma [11].

Lemma 15. *Suppose $O_1, O_2, \ldots, O_l$ are observables on state ρ with mean values $\langle O_j \rangle_\rho$ and vari-*

ances bound by $\sigma > 0$; i.e.,

$$\forall j,\ \mathrm{tr}\left(O_j^2\rho\right) - \langle O_j\rangle_\rho^2 \leq \sigma. \tag{7.73}$$

For each j, $\chi_i^{O_j}$ denotes the ith measurement outcome of O_j on ρ, and then the finite sample mean over c measurements of O_j is

$$\langle O_j\rangle_\rho^* = \frac{1}{c}\sum_{i=1}^{c}\chi_i^{O_j}. \tag{7.74}$$

For any $\varepsilon > 0$, $0 < \delta \leq \frac{1}{2}$, to make

$$P\left(\forall j, \left|\langle O_j\rangle_\rho^* - \langle O_j\rangle_\rho\right| \leq \varepsilon\right) \geq 1-\delta, \tag{7.75}$$

the number of measurements should satisfy that

$$c \geq \frac{\sigma^2(l+1)}{\varepsilon^2 \ln\left(1/(1-\delta)\right)}. \tag{7.76}$$

From this lemma, we know that, to make

$$P\left((2m)^{\frac{3}{2}}\|\boldsymbol{S}\|_\infty^2\|\boldsymbol{\epsilon}\|_\infty\|\boldsymbol{d}\| \leq \frac{\varepsilon}{3}\right) \geq (1-\delta)^{\frac{1}{3}}, \tag{7.77}$$

the verifier applies c_3 (7.55) measurements on each $\hat{\boldsymbol{x}}_l^{\mathrm{A}'}(1 \leq l \leq 2m)$, respectively, to estimate $\boldsymbol{\gamma}$. Similarly, to make

$$P\left(m\|\boldsymbol{S}\|_\infty^2\|\boldsymbol{E}_1\|_{\max} \leq \frac{\varepsilon}{3}\right) \geq (1-\delta)^{\frac{1}{3}}, \tag{7.78}$$

and

$$P\left(\frac{2m\|\boldsymbol{S}\|_\infty}{\sqrt{\lambda+1}}\|\boldsymbol{E}_2\|_{\max} \leq \frac{\varepsilon}{3}\right) \geq (1-\delta)^{\frac{1}{3}}, \tag{7.79}$$

the verifier applies c_4 (7.56) measurements on each $\frac{1}{2}\left(\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\hat{\boldsymbol{x}}_v^{\mathrm{A}'} + \hat{\boldsymbol{x}}_v^{\mathrm{A}'}\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\right)$, and c_5 (7.57) measurements on each $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\hat{\boldsymbol{x}}_v^{\mathrm{R}}$, where $1 \leq u, v \leq 2m$. □

Now I explain the detailed measurement scheme in this verification protocol. All the measurements in the protocol can be accomplished by $m+5$ local homodyne settings. For each $1 \leq l \leq 2m$,

the mean value of $\hat{x}_l$ can be sampled by a local homodyne detection on either position or momentum basis. Sampling $2m$ quadrature mean values require two local homodyne settings: one is measuring position on all m modes of A', the other is measuring momentum on all m modes of A'. For each $1 \leq u, v \leq 2m$, mean value of $\hat{\boldsymbol{x}}_u^{\mathrm{A}'} \hat{\boldsymbol{x}}_v^{\mathrm{R}}$ can be sampled by performing local homodyne detections regarding $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}$ and $\hat{\boldsymbol{x}}_v^{\mathrm{R}}$, respectively, and then multiplying two measurement outcomes. Sampling mean values of $\hat{\boldsymbol{x}}_u^{\mathrm{A}'} \hat{\boldsymbol{x}}_v^{\mathrm{R}}$ require two additional homodyne settings: one is measuring position on all m modes of R; the other is measuring momentum on all m modes of R.

For each $1 \leq v < u \leq 2m$, such that $(u, v) \neq (2j, 2j-1)$ for $1 \leq j \leq m$, sampling mean value of $\hat{\boldsymbol{x}}_u^{\mathrm{A}'} \hat{\boldsymbol{x}}_v^{\mathrm{A}'}$ can be accomplished by applying local homodyne detections regarding $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}$ and $\hat{\boldsymbol{x}}_v^{\mathrm{A}'}$, respectively, and then multiplying measurement outcomes. These measurements need the combination of position measurement at one mode and momentum measurement at another mode. Hence, at least m more local homodyne settings are required: each one setting measures position at one distinct mode and momenta at all other modes.

For each $1 \leq u \leq 2m$, sampling mean value of $\left(\hat{\boldsymbol{x}}_u^{\mathrm{A}'}\right)^2$ can be accomplished by performing homodyne detection with respect to $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}$ and squaring the measurement outcomes. These homodyne settings are same as the settings for sampling mean values of $\hat{\boldsymbol{x}}_u^{\mathrm{A}'}$. When $(u, v) = (2j, 2j-1)$, $\frac{1}{2}\left(\hat{\boldsymbol{x}}_u^{\mathrm{A}'} \hat{\boldsymbol{x}}_v^{\mathrm{A}'} + \hat{\boldsymbol{x}}_v^{\mathrm{A}'} \hat{\boldsymbol{x}}_u^{\mathrm{A}'}\right)$ is

$$\frac{1}{2}\left(\hat{q}_j^{\mathrm{A}'} \hat{p}_j^{\mathrm{A}'} + \hat{p}_j^{\mathrm{A}'} \hat{q}_j^{\mathrm{A}'}\right). \tag{7.80}$$

To sample mean value of observable (7.80), one can sample mean value of

$$\frac{1}{\sqrt{2}}(\hat{q}_j^{\mathrm{A}'} + \hat{p}_j^{\mathrm{A}'}), \tag{7.81}$$

by noting that

$$\frac{1}{2}(\hat{q}\hat{p} + \hat{p}\hat{q}) = \frac{1}{2}(\hat{q} + \hat{p})^2 - \frac{1}{2}\hat{q}^2 - \frac{1}{2}\hat{p}^2, \tag{7.82}$$

and that mean value of $\left(\hat{q}_j^{\mathrm{A}'}\right)^2$ and $\left(\hat{p}_j^{\mathrm{A}'}\right)^2$ have been sampled by the approach we explained above. Sampling mean value of observable (7.81), for each j, can be accomplished by one additional mea-

surement setting that is to perform homodyne detection at each mode of A' in a 45-degree rotated basis. Thus, all measurements in Algorithm 4 can be accomplished by $m+5$ local homodyne settings.

This subsection has presented a verification protocol for multi-mode Gaussian unitary channels including all operations and sample complexities. Central to the verification protocol, we have devised an average-fidelity witness and show that its mean value can be estimated by applying local homodyne detections. Our protocol greatly simplifies the experimental setting to detect the average fidelity without requiring quantum memory or online squeezing. The sample complexity of this protocol scales polynomially with the number of modes, the maximal squeezing parameter and the phase-space displacement of the target Gaussian unitary operation.

7.2.2 Verification of single-mode amplification channels

In this subsection, we present a verification protocol for single-mode amplification channels. We devise an average-fidelity witness for this verification protocol and show that its mean value is a linear combination of the covariances of quadrature operators.

Quantum amplification channels [95] are important for quantum cloning and other quantum information processing protocols. We investigate a verification protocol for the optimal quantum channel in terms of average fidelity

$$\bar{F}_{\mathfrak{g}}(\mathcal{E}) = \int \frac{\mathrm{d}^2\alpha}{\pi} \lambda \mathrm{e}^{-\lambda|\alpha|^2} \langle \mathfrak{g}\alpha | \mathcal{E}(|\alpha\rangle\langle\alpha|) | \mathfrak{g}\alpha \rangle , \tag{7.83}$$

where $\mathfrak{g} > \lambda + 1$ is the amplification gain. Chiribella and Xie showed that the optimal amplification channel can be achieved by a Gaussian amplification channel, using two-mode squeezing, and the maximum achievable average fidelity (7.83) is [24]

$$\bar{F}_{\mathfrak{g}}^{\max} = \frac{\lambda+1}{\mathfrak{g}^2}. \tag{7.84}$$

We present our verification protocol in Algorithm 5.

Algorithm 5 Verification protocol for single-mode amplification channel

Input:

- $\frac{1}{\lambda} > 0$ ▷ Variance of the prior Gaussian distribution
- $\mathfrak{g} > \lambda + 1$ ▷ amplification gain.
- $\bar{F}_{\mathrm{t}} \in \left(0, \frac{\lambda+1}{\mathfrak{g}^2}\right)$ ▷ threshold average fidelity.
- $\delta \in \left(0, \frac{1}{2}\right)$ ▷ maximal failure probability.
- $\varepsilon \in \left(0, \frac{\lambda+1-\mathfrak{g}^2\bar{F}_{\mathrm{t}}}{2\mathfrak{g}^2}\right)$ ▷ error bound.
- $\mathcal{E}_{\mathrm{p}}$ ▷ $2c_6+2c_7$ copies of $\mathcal{E}_{\mathrm{p}}$ from the prover
- $|\kappa\rangle_{\mathrm{TMSV}}$ ▷ $2c_6+2c_7$ copies of $|\kappa\rangle_{\mathrm{TMSV}}$
- $\sigma_2 > 0$ ▷ the upper bound of the variances of $\hat{q}^2_{\mathrm{A}'}$, $\hat{p}^2_{\mathrm{A}'}$, $\hat{q}_{\mathrm{A}'}\hat{q}_{\mathrm{R}}$ and $\hat{p}_{\mathrm{A}'}\hat{p}_{\mathrm{R}}$ on $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)$.

Output:

- b ▷ $b \in \{0,1\}$, 0 means reject and 1 means accept.

procedure VERIFICATIONOFAMPLIFICATIONCHANNEL($\frac{1}{\lambda}$, $\mathfrak{g}$, $\bar{F}_{\mathrm{t}}$, δ, ε, σ_2, $\mathcal{E}_{\mathrm{p}}$, $|\kappa\rangle_{\mathrm{TMSV}}$)

send one mode of each copy of $|\kappa\rangle_{\mathrm{TMSV}}$ into a copy of $\mathcal{E}_{\mathrm{p}}$, and keep the other mode as a reference mode;

for $i = 1 : c_6$ **do**

apply a single-shot homodyne detection for quadrature $\hat{q}_{\mathrm{A}'}$ on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)$;

end for

$\langle\hat{q}^2_{\mathrm{A}'}\rangle^* \leftarrow \frac{1}{c_6}\sum_{i=1}^{c_6}\left(\chi_i^{\hat{q}_{\mathrm{A}'}}\right)^2$; ▷ $\langle\hat{q}^2_{\mathrm{A}'}\rangle^*$ is an estimate of $\langle\hat{q}^2_{\mathrm{A}'}\rangle$.

for $i = 1 : c_6$ **do**

apply a single-shot homodyne detection for quadrature $\hat{p}_{\mathrm{A}'}$ on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)$;

end for

$\langle\hat{p}^2_{\mathrm{A}'}\rangle^* \leftarrow \frac{1}{c_6}\sum_{i=1}^{c_6}\left(\chi_i^{\hat{p}_{\mathrm{A}'}}\right)^2$; ▷ $\langle\hat{p}^2_{\mathrm{A}'}\rangle^*$ is an estimate of $\langle\hat{p}^2_{\mathrm{A}'}\rangle$.

for $i = 1 : c_7$ **do**

apply two single-shot homodyne detections for quadratures $\hat{q}_{\mathrm{A}'}$ and $\hat{q}_{\mathrm{R}}$ simultaneously on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)$;

end for

14: $\langle \hat{q}_{\mathrm{A}'} \hat{q}_{\mathrm{R}} \rangle^* \leftarrow \frac{1}{c_7} \sum_{i=1}^{c_7} \chi_i^{\hat{q}_{\mathrm{A}'}} \chi_i^{\hat{q}_{\mathrm{R}}}$; ▷ $\langle \hat{q}_{\mathrm{A}'} \hat{q}_{\mathrm{R}} \rangle^*$ is an estimate of $\langle \hat{q}_{\mathrm{A}'} \hat{q}_{\mathrm{R}} \rangle$.

15: **for** $i = 1 : c_7$ **do**

16: apply two single-shot homodyne detections for quadratures $\hat{p}_{\mathrm{A}'}$ and $\hat{p}_{\mathrm{R}}$ simultaneously on one copy of $\mathcal{E}_{\mathrm{p}} \otimes \mathcal{I}(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}})$;

17: **end for**

18: $\langle \hat{p}_{\mathrm{A}'} \hat{p}_{\mathrm{R}} \rangle^* \leftarrow \frac{1}{c_7} \sum_{i=1}^{c_7} \chi_i^{\hat{p}_{\mathrm{A}'}} \chi_i^{\hat{p}_{\mathrm{R}}}$; ▷ $\langle \hat{p}_{\mathrm{A}'} \hat{p}_{\mathrm{R}} \rangle^*$ is an estimate of $\langle \hat{p}_{\mathrm{A}'} \hat{p}_{\mathrm{R}} \rangle$.

19: $\mathcal{W}(\mathcal{E}_{\mathrm{p}})^* \leftarrow \frac{\lambda+1}{\mathfrak{g}^2} \left[\frac{(\lambda-4)\mathfrak{g}^2 - \lambda^2 - \lambda}{2\lambda\mathfrak{g}^2} - \frac{\lambda+1}{\mathfrak{g}^2} \left(\langle \hat{q}_{\mathrm{A}'}^2 \rangle^* + \langle \hat{p}_{\mathrm{A}'}^2 \rangle^* \right) + \frac{\sqrt{\lambda+1}}{\mathfrak{g}} \left(\langle \hat{q}_{\mathrm{A}'} \hat{q}_{\mathrm{R}} \rangle^* - \langle \hat{p}_{\mathrm{A}'} \hat{p}_{\mathrm{R}} \rangle^* \right) \right]$
▷ Obtain an estimate $\mathcal{W}(\mathcal{E}_{\mathrm{p}})^*$ of $\mathcal{W}(\mathcal{E}_{\mathrm{p}})$ in Eq. (7.92).

20: **if** $\mathcal{W}(\mathcal{E}_{\mathrm{p}})^* \geq \bar{F}_{\mathrm{t}} + \varepsilon$ **then**

21: **return** $b = 1$;

22: **else**

23: **return** $b = 0$.

24: **end if**

25: **end procedure**

Central to our verification protocol, we devise an average-fidelity witness and show that its mean value can be estimated by the measurement and classical-information processing scheme in Algorithm 5.

Theorem 16. *The observable*

$$\frac{\lambda+1}{\mathfrak{g}^2} \left(\mathbb{1} - \frac{\mathfrak{g}^2 - \lambda - 1}{\mathfrak{g}^2} S_{\theta'} \mathbb{1} \otimes \hat{n} S_{\theta'}^\dagger \right) \tag{7.85}$$

is an average-fidelity witness for $\bar{F}_{\mathfrak{g}}(\mathcal{E})$ *on* $\mathcal{E} \otimes \mathcal{I}(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}})$.

Henceforth, we use W_{amp} to denote the average-fidelity witness (7.85). Lemma 12 implies that the average fidelity of an amplification channel can be estimated by applying quantum memory, online two-mode squeezing and heterodyne detections as shown in Fig. 7.2. However, this method is experimentally challenging. Measuring the average-fidelity witness in Theorem 16 provides an experimentally feasible method.

Proof. From Eq. (7.23), we know

$$\bar{F}_{\mathfrak{g}}(\mathcal{E}) = \frac{\lambda+1}{\mathfrak{g}^2} \operatorname{tr} \left[S_{\theta'} \mathbb{1} \otimes G_{\theta'} S_{\theta'}^\dagger \mathcal{E} \otimes \mathcal{I}(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}) \right]. \tag{7.86}$$

Plugging in inequality (7.35), we have

$$\forall \mathcal{E},\ \mathrm{tr}\left[W_{\mathrm{amp}}\mathcal{E}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)\right]\leq \bar{F}_{\mathfrak{g}}(\mathcal{E}), \tag{7.87}$$

which proves condition (7.7). On the other hand, from Eqs. (7.21) and (7.86), we know that $\mathcal{E}$ is optimal; i.e., $\bar{F}_{\mathfrak{g}}(\mathcal{E})=\frac{\lambda+1}{\mathfrak{g}^2}$, iff

$$\mathrm{tr}_{\mathrm{A}'}\left[S^{\dagger}_{\theta'}\mathcal{E}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)S_{\theta'}\right]=|0\rangle_{\mathscr{F}}\langle 0|\,. \tag{7.88}$$

Eq. (7.88) is further equivalent to

$$\mathrm{tr}\left[W_{\mathrm{amp}}\mathcal{E}\otimes\mathcal{I}(|r\rangle\langle r|)\right]=\frac{\lambda+1}{\mathfrak{g}^2}, \tag{7.89}$$

which proves condition (7.6). Thus, we conclude that W_{amp} is an average-fidelity witness for $\bar{F}_{\mathfrak{g}}(\mathcal{E})$. □

Next, we show that the expectation value of the average-fidelity witness

$$\mathcal{W}_{\mathrm{amp}}(\mathcal{E}_{\mathrm{p}}):=\mathrm{tr}\left[W_{\mathrm{amp}}\mathcal{E}_{\mathrm{p}}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)\right] \tag{7.90}$$

is a linear combination of quadrature covariances. From Eq. (7.49) and transformation (7.50), we have

$$W_{\mathrm{amp}}=\frac{\lambda+1}{\mathfrak{g}^2}\left[\mathbb{1}-\frac{\lambda+1}{\mathfrak{g}^2}\hat{\boldsymbol{x}}^{\top}_{\mathrm{A}'}\hat{\boldsymbol{x}}_{\mathrm{A}'}+\frac{\sqrt{\lambda+1}}{\mathfrak{g}}\hat{\boldsymbol{x}}^{\top}_{\mathrm{R}}\boldsymbol{Z}\hat{\boldsymbol{x}}_{\mathrm{A}'}-\frac{1}{2}\hat{\boldsymbol{x}}^{\top}_{\mathrm{R}}\hat{\boldsymbol{x}}_{\mathrm{R}}+\frac{\mathfrak{g}^2-\lambda-1}{2\mathfrak{g}^2}\right]. \tag{7.91}$$

Combining Eqs. (7.24) and (7.53) yeilds

$$\mathcal{W}_{\mathrm{amp}}(\mathcal{E}_{\mathrm{p}})=\frac{\lambda+1}{\mathfrak{g}^2}\left[\frac{(\lambda-4)\mathfrak{g}^2-\lambda^2-\lambda}{2\lambda\mathfrak{g}^2}-\frac{\lambda+1}{\mathfrak{g}^2}\left(\langle\hat{q}^2_{\mathrm{A}'}\rangle+\langle\hat{p}^2_{\mathrm{A}'}\rangle\right)+\frac{\sqrt{\lambda+1}}{\mathfrak{g}}\left(\langle\hat{q}_{\mathrm{A}'}\hat{q}_{\mathrm{R}}\rangle-\langle\hat{p}_{\mathrm{A}'}\hat{p}_{\mathrm{R}}\rangle\right)\right]. \tag{7.92}$$

Eq. (7.92) implies that the mean value of the average-fidelity witness can be estimated by sampling

the covariances of the quadrature operators, as shown in Algorithm 5.

Theorem 17. *The protocol in Algorithm 5 requires $2c_6+2c_7$ copies of $\mathcal{E}_{\mathrm{p}}$, where*

$$c_6 \in O\left(\frac{\mathfrak{g}^4\sigma_2^2}{\varepsilon^2\ln(1/(1-\delta))}\right) \tag{7.93}$$

and

$$c_7 \in O\left(\frac{\mathfrak{g}^6\sigma_2^2}{\varepsilon^2\ln(1/(1-\delta))}\right). \tag{7.94}$$

Proof. We denote the estimation errors of $\langle\hat{q}_{\mathrm{A}'}^2\rangle$, $\langle\hat{p}_{\mathrm{A}'}^2\rangle$, $\langle\hat{q}_{\mathrm{A}'}\hat{q}_{\mathrm{R}}\rangle$ and $\langle\hat{p}_{\mathrm{A}'}\hat{p}_{\mathrm{R}}\rangle$ as E_1, E_2, E_{11} and E_{22}. The estimation error between $\mathcal{W}(\mathcal{E}_{\mathrm{p}})$ and $\mathcal{W}(\mathcal{E}_{\mathrm{p}})^*$ is bounded by

$$\left|\mathcal{W}(\mathcal{E}_{\mathrm{p}})-\mathcal{W}(\mathcal{E}_{\mathrm{p}})^*\right| \leq \frac{\mathfrak{g}^2}{\lambda+1}\max\{\|E_1\|,\|E_2\|\}+2\left(\frac{\mathfrak{g}}{\sqrt{\lambda+1}}\right)^3\max\{\|E_{11}\|,\|E_{22}\|\}. \tag{7.95}$$

To make

$$P\left(\left|\mathcal{W}(\mathcal{E}_{\mathrm{p}})-\mathcal{W}(\mathcal{E}_{\mathrm{p}})^*\right|\leq\varepsilon\right)\geq 1-\delta, \tag{7.96}$$

we suppose each term at the right-hand side of (7.95) is less than $\frac{\varepsilon}{2}$ with probability no less than $\sqrt{1-\delta}$. From Lemma 15, we know that, to make

$$P\left(\frac{\mathfrak{g}^2}{\lambda+1}\max\{\|E_1\|,\|E_2\|\}\leq\frac{\varepsilon}{2}\right)\geq\sqrt{1-\delta}, \tag{7.97}$$

and

$$P\left(2\left(\frac{\mathfrak{g}}{\sqrt{\lambda+1}}\right)^3\max\{\|E_{11}\|,\|E_{22}\|\}\leq\frac{\varepsilon}{2}\right)\geq\sqrt{1-\delta}, \tag{7.98}$$

the verifier needs c_6 (7.93) measurements on $\hat{q}_{\mathrm{A}'}^2$ and $\hat{p}_{\mathrm{A}'}^2$, respectively, and c_7 (7.94) measurements on $\hat{q}_{\mathrm{A}'}\hat{q}_{\mathrm{R}}$ and $\hat{p}_{\mathrm{A}'}\hat{p}_{\mathrm{R}}$, respectively.

□

We have presented the verification protocols of two typical kinds of bosonic channels as examples of the general framework in Sec. 7.1. Rather than estimating the average fidelity directly, both

two verification protocols estimate the mean value of an average-fidelity witness, which ascertains a lower bound the average fidelity. The measurement of the average-fidelity witness requires only the preparation of two-mode squeezed vacuum states and the application of homodyne detections. As the measurements on the reference modes can be applied immediately after the preparation of two-mode squeezed vacuum states, our verification protocols do not require any quantum memory to remain the entanglement between the channel-output modes and the reference modes. The sample complexities of both quantum channels and two-mode squeezed vacuum state inputs in both two protocols are efficient with respect to all specification parameters of the target channels.

7.3 Discussion

We have presented a general verification framework for an optimal quantum channel by unifying the favourable features of quantum-state verification [11] and quantum-process benchmarking [12]. To develop our quantum-channel-verification framework, standard fidelity witness for quantum states has been generalized to an average fidelity witness for quantum channels per Definition 10. Rather than sampling a set of input states, our quantum-channel verification protocols require only one certain entangled input state and local measurements of an average-fidelity witness. Our verification protocols satisfy both completeness and soundness conditions per Definition 9, and hence are reliable quantum-channel verification schemes.

We have presented the applications of our framework for the verification of two types of CPTP maps: multi-mode Gaussian unitary channels and single-mode amplification channels, both used widely in CV quantum computing and quantum communication. We devise average-fidelity witnesses for these two types of quantum channels in Theorems 11 and Theorem 16, respectively, by truncating a thermal-state density operator in Lemma 13 and reformulating the witness in terms of quadrature operators. Sample complexity for verifying multi-mode Gaussian unitary channels scales polynomially with respect to the number of modes m, maximum squeezing $\|\boldsymbol{S}\|_\infty$ and phase-space displacement $\|\boldsymbol{d}\|$. On the other hand, sample complexity to verify single-mode amplifica-

tion channels scales polynomially with respect to amplification gain g. Sample complexities in both verification protocols are proportional to $\frac{1}{\varepsilon^2 \ln(1/(1-\delta))}$ due to classical sampling error. Our measurement procedure comprises only local homodyne detections and is much simpler than the related work [12], as neither online two-mode squeezing nor quantum memories are required.

7.4 Conclusion

We have presented experimentally feasible verification protocols for bosonic channels with polynomially scaling sample complexities. Different from quantum process tomography, our verification protocol's benchmark is average fidelity over an infinite set of gaussian-distributed coherent states. Our experimental setting uses only two-mode squeezed vacuum states and local homodyne detections, which are feasible using current technology. Our verification protocols are reliable in the sense that a deceitful prover fails to cheat a prover and an honest prover typically passes the prover's test.

The essential step of our verification protocols is to measure an average-fidelity witness, whose mean value can distinguish an optimal quantum channel from all other quantum channels, whose average fidelity is below a certain threshold. We apply our quantum-channel verification framework to verifying both multi-mode Gaussian unitary channels and single-mode amplification channels. Owing to extensive usage of Gaussian unitary operations, like squeezing, in CV quantum information processing and the remarkable utilization of amplification channels in quantum communication [17, 123], our verification protocols are important for testing components in CV quantum computing and quantum communication.

Our quantum-channel-verification framework can be applied to verify other types of quantum channels, for example, attenuation channels and optimal quantum cloning machines [28]. Furthermore, our approach can be extended to verify non-Gaussian cubic phase gates [48, 116], which is essential for universal CV quantum computing, by estimating higher-order quadrature cumulants [75, 40]. Sample complexity, introduced here, can be further reduced by restricting the nature

of the quantum channel and using statistical techniques, like importance sampling [44, 40]. As this paper mainly focuses on CV quantum information, verification of linear optical devices for the significant application of BosonSampling is not studied here; however, verification of linear optical devices with single-photon inputs is an interesting direction to explore and could be quite related to our work here.

Chapter 8

Conclusions

8.1 Summaries

In this thesis, we [121] have developed a protocol for the distribution of quantum information in spacetime. We have shown that our protocol, under certain revisions, can be applied to different generalized summoning protocols, implying that our CSS code forms an essential tool for quantum information processing tasks related to summoning. By noting the fact that, in general case, any two spacetime regions must share at least one quantum share to accomplish summoning, our CSS code is the most efficient code for quantum summoning, among all the physically possible codes, as each pair of spacetime regions share exactly one qubit. Furthermore, we have presented both the encoding and the decoding circuits for the CSS code and our encoding circuit reduces the gate complexity compared to the previous best result.

Our results provide further operational interpretation of the distribution of quantum information in spacetime, as space complexity and gate complexity becomes essential problems when studying quantum information problems in subtle spacetime structure, like black holes [55, 7, 51]. On the other hand, our comprehensive investigation of quantum summoning lay the foundation for physicists to construct quantum communication protocols for relativistic quantum cryptography purposes.

For relativistic QSS, we [6] apply a rigid accelerating cavity model to study the effects of non-inertial motion of localized quantum systems on the fidelity of a QSS protocol. Specifically, we formulate the noisy evolution of quantum information encoded in a single-mode Fock space inside an accelerating cavity as a Gaussian lossy channel and calculate how the concatenation of noisy quantum channels affect the fidelity of QSS. This formulation can be utilized to study other relativistic quantum communication protocols besides QSS. Our results relax the common assumption of ignorance of relativistic effects on quantum information processing and provide a theoretical foundation for relativistic quantum communications.

Finally, we [122] present verification schemes for bosonic quantum channels, the sample complexity of which, scales polynomially in terms of all channel parameters. Essentially, we propose average-fidelity witness, which yields a tight lower bound of average fidelity. By estimating average-fidelity witness, our protocol significantly reduces sample complexity compared to tomography and partial characterization approaches, and also greatly simplifies experimental settings utilizing only two-mode squeezed states and homodyne detections. As both Gaussian unitary operations and amplifying channels are commonly used in CV quantum computing and quantum communication, our verification protocols provide an important approach for verification of CV quantum devices.

8.2 Outlook

In this thesis, I have used fidelity as a figure of merit to quantify the performance of a quantum channel. From the perspective of quantum communication, it is more interesting to study how relativistic effects have an influence on the classical capacity and the quantum capacity of a quantum channel. To investigate how to witness a lower bound of the classical capacity and the quantum capacity of a quantum channel is quite interesting as well. Both these research directions can be quite related to what I have done in this thesis.

We have assumed that, in Chapter 7, all the quantum channels are identical and independent,

but this assumption can be failed due to time-dependent errors in channel preparation and a cheating prover intending to prepare multiple channels. How to verify a bosonic quantum channel without this assumption is an interesting open problem. Another essential assumption in our verification scheme is that all the state preparation and measurements are ideal, which is impossible in practice. Verification protocols that are robust to SPAM errors [68, 81, 82] will be significant for benchmarking CV quantum gates.

Bibliography

[1] Gerardo Adesso, Sammy Ragy, and Antony R. Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Syst. Inf. Dyn.*, 21(21):1440001, 2014.

[2] Emily Adlam and Adrian Kent. Quantum paradox of choice: More freedom makes summoning a quantum state harder. *Phys. Rev. A*, 93:062327, 2016.

[3] Mehdi Ahmadi, David Edward Bruschi, and Ivette Fuentes. Quantum metrology for relativistic quantum fields. *Phys. Rev. D*, 89:065028, Mar 2014.

[4] Mehdi Ahmadi, David Edward Bruschi, Carlos Sabín, Gerardo Adesso, and Ivette Fuentes. Relativistic quantum metrology: Exploiting relativity to improve quantum measurement technologies. *Sci. Rep.*, 4:4996, 2014.

[5] Mehdi Ahmadi, Krzysztof Lorek, Agata Chęcińska, Alexander R. H. Smith, Robert B. Mann, and Andrzej Dragan. Effect of relativistic acceleration on localized two-mode gaussian quantum states. *Phys. Rev. D*, 93:124031, Jun 2016.

[6] Mehdi Ahmadi, Ya-Dong Wu, and Barry C. Sanders. Relativistic (2,3)-threshold quantum secret sharing. *Phys. Rev. D*, 96:065018, Sep 2017.

[7] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. Black holes: complementarity or firewalls? *J. High Energy Phys.*, 2013(2):62, 2013.

[8] Paul M. Alsing and G. J. Milburn. Teleportation with a uniformly accelerated partner. *Phys. Rev. Lett.*, 91:180404, 2003.

[9] Joseph B Altepeter, David Branning, Evan Jeffrey, TC Wei, Paul G Kwiat, Robert T Thew, Jeremy L O'Brien, Michael A Nielsen, and Andrew G White. Ancilla-assisted quantum process tomography. *Phys. Rev. Lett.*, 90(19):193601, 2003.

[10] Ulrik L Andersen, Jonas S Neergaard-Nielsen, Peter Van Loock, and Akira Furusawa. Hybrid discrete-and continuous-variable quantum information. *Nat. Phys.*, 11(9):713, 2015.

[11] Leandro Aolita, Christian Gogolin, Martin Kliesch, and Jens Eisert. Reliable quantum certification of photonic state preparations. *Nat. Commun.*, 6:8498, 2015.

[12] Ge Bai and Giulio Chiribella. Test one to test many: a unified approach to quantum benchmarks. *Phys. Rev. Lett.*, 120(15):150502, 2018.

[13] Stephen D. Bartlett, Barry C. Sanders, Samuel L. Braunstein, and Kae Nemoto. Efficient classical simulation of continuous variable quantum information processes. *Phys. Rev. Lett.*, 88:097904, Feb 2002.

[14] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[15] N. D. Birrell and P. C. W. Davies. *Quantum Fields in Curved Space*. Cambridge Monographs on Mathematical Physics. Cambridge University Press, 1982.

[16] George Robert Blakley et al. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, 1979.

[17] Rémi Blandino, Anthony Leverrier, Marco Barbieri, Jean Etesse, Philippe Grangier, and Rosa Tualle-Brouri. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A*, 86:012327, Jul 2012.

[18] Robin Blume-Kohout and Peter S Turner. The curious nonexistence of gaussian 2-designs. *Commun. Math. Phys.*, 326(3):755–771, 2014.

[19] H. Bombin and M. A. Martin-Delgado. Homological error correction: Classical and quantum codes. *J. Math. Phys.*, 48(5):052105, 2007.

[20] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, Jun 2005.

[21] David Edward Bruschi, Ivette Fuentes, and Jorma Louko. Voyage to alpha centauri: Entanglement degradation of cavity modes due to motion. *Phys. Rev. D*, 85:061701, Mar 2012.

[22] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, Aug 1996.

[23] Giulio Chiribella and Gerardo Adesso. Quantum benchmarks for pure single-mode gaussian states. *Phys. Rev. Lett.*, 112(1):010501, 2014.

[24] Giulio Chiribella and Jinyu Xie. Optimal design and quantum benchmarks for coherent state amplifiers. *Phys. Rev. Lett.*, 110(21):213602, 2013.

[25] J. M. Chow, J. M. Gambetta, L. Tornberg, Jens Koch, Lev S. Bishop, A. A. Houck, B. R. Johnson, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf. Randomized benchmarking and process tomography for gate errors in a solid-state qubit. *Phys. Rev. Lett.*, 102:090502, Mar 2009.

[26] Isaac L Chuang and Michael A Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.*, 44(11-12):2455–2467, 1997.

[27] Richard Cleve, Daniel Gottesman, and Hoi-Kwong Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83:648–651, Jul 1999.

[28] PT Cochrane, Timothy Cameron Ralph, and A Dolińska. Optimal cloning for finite distributions of coherent states. *Phys. Rev. A*, 69(4):042313, 2004.

[29] MJ Collett. Exact density-matrix calculations for simple open systems. *Phys. Rev. A*, 38(5):2233, 1988.

[30] A. Cross, G. Smith, J. A. Smolin, and B. Zeng. Codeword stabilized quantum codes. *IEEE Trans. Inf. Theory*, 55(1):433–438, Jan 2009.

[31] Marcus P da Silva, Olivier Landon-Cardinal, and David Poulin. Practical characterization of quantum devices without tomography. *Phys. Rev. Lett.*, 107(21):210404, 2011.

[32] GM D'Ariano and P Lo Presti. Quantum tomography for measuring experimentally the matrix elements of an arbitrary quantum operation. *Phys. Rev. Lett.*, 86(19):4195, 2001.

[33] Paul CW Davies. Scalar production in schwarzschild and rindler metrics. *J. Phys. A*, 8(4):609, 1975.

[34] Dennis Dieks. Communication by EPR devices. *Phys. Lett. A*, 92(6):271–272, 1982.

[35] Reinhard Diestel. *Graph Theory*, volume 173 of *Graduate Texts in Mathematics*. Springer-Verlag, Heidelberg, 2016.

[36] T. G. Downes, T. C. Ralph, and N. Walk. Quantum communication with an accelerated partner. *Phys. Rev. A*, 87:012327, Jan 2013.

[37] Andrzej Dragan, Jason Doukas, and Eduardo Martín-Martínez. Localized detection of quantum entanglement through the event horizon. *Phys. Rev. A*, 87:052326, May 2013.

[38] Andrzej Dragan, Jason Doukas, Eduardo Martín-Martínez, and David Edward Bruschi. Localized projective measurement of a quantum field in non-inertial frames. *Class. Quantum Grav.*, 30(23):235006, 2013.

[39] Hong-Yi Fan. Operator ordering in quantum optics theory and the development of dirac's symbolic method. *J. Opt. B: Quantum Semiclassical Opt.*, 5(4):R147, 2003.

[40] Renato Farias and Leandro Aolita. Average channel-fidelity witnesses for benchmarking continuous-variable gates. *arXiv:1812.01968*, 2018.

[41] Steven T Flammia and Yi-Kai Liu. Direct fidelity estimation from few pauli measurements. *Phys. Rev. Lett.*, 106(23):230501, 2011.

[42] N. Friis, A. R. Lee, K. Truong, C. Sabín, E. Solano, G. Johansson, and I. Fuentes. Relativistic quantum teleportation with superconducting circuits. *Phys. Rev. Lett.*, 110:113602, Mar 2013.

[43] Nicolai Friis. *Cavity mode entanglement in relativistic quantum information*. PhD thesis, The University of Nottingham, 2013.

[44] M Gluza, M Kliesch, J Eisert, and L Aolita. Fidelity witnesses for fermionic quantum simulations. *Phys. Rev. Lett.*, 120(19):190501, 2018.

[45] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[46] Daniel Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.

[47] Daniel Gottesman. Theory of quantum secret sharing. *Phys. Rev. A*, 61:042311, Mar 2000.

[48] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Phys. Rev. A*, 64:012310, Jun 2001.

[49] Brian C Hall. *Quantum Theory for Mathematicians*, volume 267 of *Graduate Texts in Mathematics*. Springer, New York, 2013.

[50] D Hangleiter, M Kliesch, M Schwarz, and J Eisert. Direct certification of a class of quantum simulations. *Quant. Sci. Tech.*, 2(1):015004, 2017.

[51] D. Harlow. Jerusalem lectures on black holes and quantum information. *Rev. Mod. Phys.*, 88:015002, Feb 2016.

[52] Patrick Hayden and Alex May. Summoning information in spacetime, or where and when can a qubit be? *J. Phys. A*, 49(17):175304, 2016.

[53] Patrick Hayden and Alex May. Localizing and excluding quantum information; or, how to share a quantum secret in spacetime. *Quantum*, 3:196, 2019.

[54] Patrick Hayden, Sepehr Nezami, Grant Salton, and Barry C. Sanders. Spacetime replication of continuous variable quantum information. *New J. Phys.*, 18(8):083043, 2016.

[55] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *J. High Energy Phys.*, 2007(09):120, 2007.

[56] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, Mar 1999.

[57] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. In *The Collected Works of Wassily Hoeffding*, pages 409–426. Springer, 1994.

[58] Steven Homer and Alan L Selman. *Computability and Complexity Theory*. Springer, New York, 2011.

[59] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81(2):865, 2009.

[60] Andrzej Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3(4):275–278, 1972.

[61] J. R. Johansson, G. Johansson, C. M. Wilson, and Franco Nori. Dynamical casimir effect in superconducting microwave circuits. *Phys. Rev. A*, 82:052509, Nov 2010.

[62] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New J. Phys.*, 13(11):113015, 2011.

[63] Adrian Kent. Quantum tasks in minkowski space. *Class. Quantum Grav.*, 29(22):224013, 2012.

[64] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109:130501, Sep 2012.

[65] Adrian Kent. A no-summoning theorem in relativistic quantum theory. *Quantum Inf. Process.*, 12(2):1023–1032, 2013.

[66] Adrian Kent. Unconstrained summoning for relativistic quantum information processing. *Phys. Rev. A*, 98:062332, Dec 2018.

[67] Adrian Kent. Summoning, no-signalling and relativistic bit commitments. *Entropy*, 21(5):534, 2019.

[68] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. Randomized benchmarking of quantum gates. *Phys. Rev. A*, 77:012307, Jan 2008.

[69] Ioannis Kogias, Yu Xiang, Qiongyi He, and Gerardo Adesso. Unconditional security of entanglement-based continuous-variable quantum secret sharing. *Phys. Rev. A*, 95:012315, Jan 2017.

[70] Robert Konig, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *IEEE Trans. Inf. Theory*, 55(9):4337–4347, 2009.

[71] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Barry C. Sanders, and Ping Koy Lam. Tripartite quantum state sharing. *Phys. Rev. Lett.*, 92:177903, 2004.

[72] Andrew M. Lance, Thomas Symul, Warwick P. Bowen, Tom*áš* Tyc, Barry. C Sanders, and Ping Koy Lam. Continuous variable (2, 3) threshold quantum secret sharing schemes. *New J. Phys.*, 5(1):4, 2003.

[73] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge university press, Cambridge, 1997.

[74] Joel Lindkvist, Carlos Sabín, Ivette Fuentes, Andrzej Dragan, Ida-Maria Svensson, Per Delsing, and Göran Johansson. Twin paradox with macroscopic clocks in superconducting circuits. *Phys. Rev. A*, 90:052113, Nov 2014.

[75] Nana Liu, Tommaso F Demarie, Si-Hui Tan, Leandro Aolita, and Joseph F Fitzsimons. Client-friendly continuous-variable blind and verifiable quantum computing. *arXiv:1806.09137*, 2018.

[76] Mirko Lobino, Dmitry Korystov, Connor Kupchak, Eden Figueroa, Barry C Sanders, and AI Lvovsky. Complete characterization of quantum-optical processes. *Science*, 322(5901):563–566, 2008.

[77] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and relativity. *Phys. Rev. Lett.*, 111:180504, Nov 2013.

[78] Alexander I Lvovsky. Phys 673: Quantum and nonlinear optics lecture notes, November 2017.

[79] Alexander I Lvovsky and Michael G Raymer. Continuous-variable optical quantum-state tomography. *Rev. Mod. Phys.*, 81(1):299, 2009.

[80] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. Optical quantum memory. *Nat. photonics*, 3(12):706, 2009.

[81] Easwar Magesan, J. M. Gambetta, and Joseph Emerson. Scalable and robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.*, 106:180504, May 2011.

[82] Easwar Magesan, Jay M. Gambetta, and Joseph Emerson. Characterizing quantum gates via randomized benchmarking. *Phys. Rev. A*, 85:042311, Apr 2012.

[83] Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Phys. Rev. A*, 78:042309, Oct 2008.

[84] Genta Masada, Kazunori Miyata, Alberto Politi, Toshikazu Hashimoto, Jeremy L O'Brien, and Akira Furusawa. Continuous-variable entanglement on a chip. *Nat. Photonics*, 9(5):316, 2015.

[85] Alex May. Quantum tasks in holography. *arXiv:1902.06845*, 2019.

[86] Yoshichika Miwa, Jun-ichi Yoshikawa, Noriaki Iwata, Mamoru Endo, Petr Marek, Radim Filip, Peter van Loock, and Akira Furusawa. Exploring a new regime for processing optical qubits: squeezing and unsqueezing single photons. *Phys. Rev. Lett.*, 113(1):013601, 2014.

[87] Michael A Nielsen. A simple formula for the average gate fidelity of a quantum dynamical operation. *Phys. Lett. A*, 303(4):249–252, 2002.

[88] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, Cambridge, 2010.

[89] William L Oberkampf and Christopher J Roy. *Verification and Validation in Scientific Computing*. Cambridge University Press, Cambridge, 2010.

[90] Jeremy L O'Brien, GJ Pryde, Alexei Gilchrist, DFV James, Nathan K Langford, TC Ralph, and AG White. Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.*, 93(8):080502, 2004.

[91] Juan Ortigoso. Twelve years before the quantum no-cloning theorem. *Am. J. Phys.*, 86(3):201–205, 2018.

[92] Sam Pallister, Noah Linden, and Ashley Montanaro. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.*, 120(17):170502, 2018.

[93] James L. Park. The concept of transition in quantum mechanics. *Found. Phys.*, 1(1):23–33, Mar 1970.

[94] Asher Peres and Daniel R. Terno. Quantum information and relativity theory. *Rev. Mod. Phys.*, 76:93–123, Jan 2004.

[95] Raphael C Pooser, Alberto M Marino, Vincent Boyer, Kevin M Jones, and Paul D Lett. Low-noise amplification of a continuous-variable quantum state. *Phys. Rev. Lett.*, 103(1):010501, 2009.

[96] JF Poyatos, J Ignacioi Cirac, and Peter Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.*, 78(2):390, 1997.

[97] John Preskill. *Lecture Notes for Physics 229: Quantum Information and Computation*. CreateSpace Independent Publishing Platform, North Charleston, 2015.

[98] Timothy Proctor, Kenneth Rudinger, Kevin Young, Mohan Sarovar, and Robin Blume-Kohout. What randomized benchmarking actually measures. *Phys. Rev. Lett.*, 119(13):130502, 2017.

[99] Saleh Rahimi-Keshari, Artur Scherer, Ady Mann, Ali T Rezakhani, AI Lvovsky, and Barry C Sanders. Quantum process tomography with coherent states. *New J. Phys.*, 13(1):013006, 2011.

[100] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. Measurement-based quantum computation on cluster states. *Phys. Rev. A*, 68:022312, Aug 2003.

[101] Benedikt Richter, Krzysztof Lorek, Andrzej Dragan, and Yasser Omar. Effect of acceleration on localized fermionic gaussian states: From vacuum entanglement to maximally entangled states. *Phys. Rev. D*, 95:076004, Apr 2017.

[102] Steven Roman. *Advanced Linear Algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer Science+Business Media, New York, 2005.

[103] Erhan Saglamyurek, Neil Sinclair, Jeongwan Jin, Joshua A Slater, Daniel Oblak, Félix Bussieres, Mathew George, Raimund Ricken, Wolfgang Sohler, and Wolfgang Tittel. Broadband waveguide quantum memory for entangled photons. *Nature*, 469(7331):512, 2011.

[104] Bahaa EA Saleh and Malvin Carl Teich. *Fundamentals of photonics*. John Wiley & Sons, New York, 2019.

[105] Alessio Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods*. CRC Press, Boca Raton, 2017.

[106] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[107] Kunal Sharma and Mark M Wilde. Characterizing the performance of continuous-variable gaussian quantum gates. *arXiv:1810.12335*, 2018.

[108] Andrew Steane. Multiple-particle interference and quantum error correction. *Proc. Royal Soc. A*, 452(1954):2551–2577, 1996.

[109] Shuntaro Takeda and Akira Furusawa. Universal quantum computing with measurement-induced continuous-variable gate sequence in a loop-based architecture. *Phys. Rev. Lett.*, 119(12):120504, 2017.

[110] Yuki Takeuchi and Tomoyuki Morimae. Verification of many-qubit states. *Phys. Rev. X*, 8(2):021060, 2018.

[111] Edwin F. Taylor and John Archibald Wheeler. *Spacetime Physics: Introduction to Special Relativity*. W. H. Freeman, New York, 1992.

[112] Barbara M Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A*, 271(5-6):319–326, 2000.

[113] Tomáš Tyc, David J Rowe, and Barry C Sanders. Efficient sharing of a continuous-variable quantum secret. *J. Phys. A*, 36(27):7625, 2003.

[114] W. G. Unruh. Notes on black-hole evaporation. *Phys. Rev. D*, 14:870–892, Aug 1976.

[115] Joel J Wallman and Steven T Flammia. Randomized benchmarking with confidence. *New J. Phys.*, 16(10):103032, 2014.

[116] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[117] R F Werner. All teleportation and dense coding schemes. *J. Phys. A*, 34(35):7081, 2001.

[118] Mark M Wilde. *Quantum information theory*. Cambridge University Press, Cambridge, 2013.

[119] Christopher M Wilson, Göran Johansson, Arsalan Pourkabirian, Michael Simoen, J Robert Johansson, Tim Duty, F Nori, and Per Delsing. Observation of the dynamical casimir effect in a superconducting circuit. *Nature*, 479(7373):376, 2011.

[120] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[121] Ya-Dong Wu, Abdullah Khalid, and Barry C Sanders. Efficient code for relativistic quantum summoning. *New J. Phys.*, 20(6):063052, 2018.

[122] Ya-Dong Wu and Barry C Sanders. Efficient verification of bosonic quantum channels via benchmarking. *New J. Phys.*, 21(7):073026, 2019.

[123] Guo-Yong Xiang, TC Ralph, AP Lund, N Walk, and Geoff J Pryde. Heralded noiseless linear amplification and distillation of entanglement. *Nat. Photonics*, 4(5):316, 2010.

[124] Yuxiang Yang, Giulio Chiribella, and Gerardo Adesso. Certifying quantumness: Benchmarks for the optimal processing of generalized coherent and squeezed states. *Phys. Rev. A*, 90(4):042319, 2014.

[125] Jun-ichi Yoshikawa, Toshiki Hayashi, Takayuki Akiyama, Nobuyuki Takei, Alexander Huck, Ulrik L Andersen, and Akira Furusawa. Demonstration of deterministic and high fidelity squeezing of quantum information. *Phys. Rev. A*, 76(6):060301, 2007.

[126] Huangjun Zhu and Masahito Hayashi. Efficient verification of pure quantum states with applications to hypergraph states. *arXiv:1806.05565*, 2019.

[127] Quntao Zhuang, Thomas Schuster, Beni Yoshida, and Norman Y. Yao. Scrambling and complexity in phase space. *Phys. Rev. A*, 99:062334, Jun 2019.

Appendix A

Copyright permissions

This appendix includes the relevant copyright permissions for published papers whose materials are included in this thesis. The publishers' policies granting permission for an author to include published materials in thesis are given in the links below:

- NJP: https://iopscience.iop.org/journal/1367-2630/page/NJP%20copyright%20statement
- PRD: https://journals.aps.org/prd/copyrightFAQ.html#thesis