2015

Rényi Quantum Conditional Mutual Information and Parity Quantum Optical Metrology

Kaushik Parasuram Seshadreesan
Louisiana State University and Agricultural and Mechanical College, kaushik.sesh@gmail.com

RÉNYI QUANTUM CONDITIONAL MUTUAL INFORMATION AND PARITY QUANTUM OPTICAL METROLOGY

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Physics and Astronomy

by
Kaushik P. Seshadreesan
M.Sc. (Hons.), Birla Institute of Technology and Science Pilani, 2009
B.E. (Hons.), Birla Institute of Technology and Science Pilani, 2009
August 2015

I dedicate this thesis to the loving memory of my grandparents Rangam paati, Manimma paati, Ramaswamy thatha and Parasuram thatha.

Acknowledgements

I am deeply grateful to my advisor Jonathan P. Dowling for his terrific guidance, unparalleled support and constant encouragement throughout my PhD. With his electric personality and a philosophy built on the pillars of optimism and pragmatism, Jon has had a huge impact on me. It is hard to account for all the intangibles about scientific research and its marketing that I have imbibed from Jon. Jon is, and will always be, my inspiration.

I am thankful to Hwang Lee, one of my two co-advisors, for his invaluable guidance through many hours of enriching discussions on quantum optics and metrology.

I owe my sincere thanks to Mark M. Wilde, my other co-advisor. Mark has had a huge influence on my approach to carrying out scientific research. He has inspired me to become a thorough and meticulous researcher. I thank him for mentoring me in quantum information theory, for his constant support and encouragement, and for including me in his research collaborations with Mario Berta and Masahiro Takeoka.

I am thankful to Girish S. Agarwal for kindly agreeing to host me at Oklahoma State University during the Spring of 2013, and for his able guidance and continued support.

I am thankful to Masahiro Takeoka for giving me the opportunity to pursue research at the National Institute of Information and Communications Technology, Tokyo, Japan during the Summer of 2015, and for mentoring me in quantum key distribution and quantum information theory.

I thank the members of my dissertation committee; A. R. P. Rau, for the many enlightening lectures on relativistic quantum mechanics and discussions on Rényi squashed entanglement and quantum discord; Thomas R. Corbitt for including me in the LIGO-Caltech quantum optomechanics telecons; and Ambar N. Sengupta for his interest in my dissertation topic and useful inputs.

I thank Petr Anisimov, who was a postdoctoral researcher in the group at the time I began, for being a terrific mentor, and for giving me a great head start to research in quantum physics. Special thanks to Sai Vinjanampathy, former group member, for being a "big brother" to me, and for the many enriching discussions on quantum information. I am thankful to my collaborators Mario Berta, Sejong Kim, Moochan Kim, Keith Motes, Jonathan Olson, Peter Rohde and Christoph Wildfeuer. I thank all the folks at the Quantum Science and Technologies Group, with whom I shared office space at different times and also spent many happy hours at the North Gate; thank you Ashkhan Balouchi, Katherine Brown, Tom Cooney, Siddhartha Das, Bryan Gard, Manish Gupta, Kebei Jiang, Nick Lanning, Jonny Olson, Haoyu Qi, Bhaskar Roy-Bardhan, Robi Singh, Zhihao Xiao and Chenglong You for all the great memories.

I acknowledge support from the Board of Regents of Louisiana Graduate Research Fellowship, the Graduate School Dissertation Year Fellowship, and Graduate Research Assistantships from Jonathan Dowling and Mark Wilde. I acknowledge generous travel support from the Coates Foundation at LSU, Jonathan Dowling and Mark Wilde. Further, I thank all the support staff at the Physics Department for their kind and able support; Arnell Jackson for helping keep up with the graduate school requirements, Ophelia Dudley for helping with travel arrangements and Laurie Rea for helping with the processing of applications for various travel grants and the LSU Dissertation fellowship.

Back when I began graduate school in 2009, there were a few people who made it all worthwhile through competition and camaraderie. This includes my fellow Physics graduate pals Anamaria, Bhaskar, Brajesh, Joe, Kundan and Lyuda, with whom I spent a lot of time working on homework assignments or discussing physics. All along, when the going at school got tough and I sought some unwinding, there were my great pals: The gangs of Batonpur! Many thanks and cheers to Ahalya, Anuja, Anvita, Bhaskar, Brajesh, Kundan, Prathvind, Rahul, Richie, Saroj, Sarthak and Venky; for all the good times and great memories during the past six years.

I thank the Ranganathans of Cypress, Texas, for becoming family to me here in the US, and for caring for me. They have been home away from home for me during the past six years. I thank Bunakka and Srinivasan athimber for their constant love and support, and for showing faith in me. I thank my sister Amrutha for being my first student of science, my soundboard, my punchbag (quite literally in our younger days), and for always backing my abilities. I thank Varsha, my girlfriend and "nonlocal" companion, for being the spring of love and joy in my life. The way our love blossomed is nothing short of "spooky action at a distance"! I thank her for the constant belief in me and in my abilities. Finally, I thank my parents for always being there for me, for their constant love and support—my amma, Nalini Seshadreesan for being a pillar of strength for me at difficult times and for being my compass during times when I felt lost; my appa, the real Seshadreesan, for providing me the best opportunities growing up.

Table of Contents

Abstract

This is a two-part thesis strung together by a common underlying theme—quantum correlations. We present some new characterizations and quantifications of quantum correlations and an application of one such correlation—entanglement—for quantum technology.

In Part I of the thesis, we use a Rényi generalization of the quantum conditional mutual information (QCMI) to define and study new measures of quantum entanglement and quantum discord. In particular, using a quantity derived from a Rényi QCMI, we introduce: a) the geometric squashed entanglement, a faithful entanglement measure, which is a lower bound on the squashed entanglement and which reduces to the geometric measure of entanglement for pure quantum states, b) the surprisal of measurement recoverability, a discord-like measure, which is similarly a lower bound on the quantum discord. The surprisal of measurement recoverability enhances our understanding of quantum discord in terms of the ability to recover one share of a bipartite quantum system after it has been measured.

In Part II, we discuss entanglement-enhanced quantum sensing. In particular, we consider optical interferometric sensors that use photon-number parity detection. Using the quantum and classical Cramér-Rao bounds (QCRB and CCRB) on phase precision as the figures of merit, we characterize a class of two-mode pure states for which photon-number parity measurement is optimal for phase estimation. These states turn out to be a subset of the class of path-symmetric states—a class for which photon-number counting-based measurements are known to be optimal. Further, we gauge the performance of the particular interferometry based on coherent light mixed with squeezed vacuum light and photon-number parity measurement. We show that photon-number parity is an optimal measurement for the above state in the sense that the detection scheme is capable of achieving the best phase precision offered by the state (given by its QCRB). The state by itself is also known to be capable of optimal phase precision for any state in linear interferometry for a given photon budget, called the Heisenberg limit. Thus, we demonstrate Heisenberg-limited phase estimation for the state with photon-number parity detection.

Chapter 1
Introduction

Quantum theory undoubtedly finds a place among the most important scientific developments of the twentieth century. Its roots can be traced back to the seminal works of stalwarts such as Planck, Einstein, Bohr, and de Broglie (only to name a few). Quantum theory was then formalized independently by Heisenberg as matrix mechanics, and Schrödinger as wave mechanics. These two formalisms were later shown to be equivalent by Dirac, who then introduced a unified formalism, one that is widely used today as non-relativistic quantum mechanics. Quantum mechanics has been successfully applied to obtain a deeper understanding of the structure of the atom, its constituent sub-atomic particles, the elements of the periodic table, the interaction of different atoms to form molecules, and numerous other micro and macroscopic physical phenomena. From a technological viewpoint, the mere departure from classical physics marked by the emergence of quantum mechanics as a fundamental theory of nature during the mid to late years of the twentieth century paved the way to a series of advancements, which culminated in the development of semiconductor electronics and the modern age of information and computation. This phenomenon has been called by some as the *first quantum revolution* [52].

Quantum mechanics is fundamentally different from classical physics. If there is one essential concept in quantum mechanics that distinguishes it from classical mechanics, it is the *non-commutativity* of conjugate observables. Take the position and momentum of a physical system for example. The operators corresponding to these attributes in quantum theory do not commute; their commutator is given by

$$[\hat{x}, \hat{p}] = i\hbar,$$

where $\hat{x}$ and $\hat{p}$ are the position and momentum operators, respectively, and $\hbar = 1.055 \times 10^{-34}$J-s is the Dirac constant (which is $1/(2\pi)$ times the Planck constant $h = 6.63 \times 10^{-34}$J-s). This non-commutativity imposes a fundamental limitation on how precisely the position and momentum of a subatomic particle can be simultaneously determined. The much celebrated *uncertainty principle* given by Heisenberg quantifies this fact as

$$\Delta x \Delta p \geq \hbar/2,$$

where Δx and Δp are the uncertainties in the simultaneous estimates of position and momentum of a quantum system, respectively. Thus quantum mechanics forbids the simultaneous measurement of position and momentum with arbitrary precision. This is in contrast with classical mechanics, where the state of a particle is in given by its position and momentum coordinates in phase space, assuming that they can be determined simultaneously with arbitrarily high precisions. The state of a system in quantum mechanics, instead, is described by a wavefunction in either the position or the momentum eigenbasis. The quantum mechanical wavefunction encodes the probability amplitudes of the various possible measurement outcomes of an observable in the form of a *superposition*. For example, the wavefunction of a quantum system in the position eigenbasis encodes the probability amplitudes of the various possible locations at which the system could be found. Further, given a Hamiltonian describing the dynamics of the system, the wavefunction transforms into a new wavefunction, resulting in new probability amplitudes for the various possible measurement outcomes. Thus, quantum mechanics is inherently a *stochastic* theory. This too is in contrast with classical mechanics, which is a fully deterministic theory, wherein, given the initial position and momentum of a system and the Hamiltonian, the position and momentum at all future times can be determined precisely.

1.1 Quantum Correlations

Another salient, distinguishing feature of quantum mechanics is the novel types of correlations allowed to exist between quantum systems, which are beyond what is allowed in classical physics. This thesis is about such "nonclassical" or "quantum" correlations. If the mere emergence of quantum mechanics marked a first quantum revolution, then we are currently in the middle of what is a *second quantum revolution*, where a large global effort is underway towards harnessing such quantum correlations towards novel technologies for information processing and computation [52].

Quantum entanglement. Following the invention of quantum mechanics, Schrödinger in 1935 realized that the mathematical structure of quantum mechanics presented some serious peculiarities. He observed that a joint quantum state describing two quantum systems may be such that it is non-factorable into a product of *local* quantum states on the individual systems. He called this feature *entanglement*. Entangled quantum states are such that a measurement on one of, say two systems in an entangled quantum state, could instantly *steer* the other system to a particular state depending on the measurement that was performed on the first system and its outcome, independent of how separated the two entangled systems are in distance at the time of the measurement. This peculiar feature, however, became a cause of concern among many contemporary physicists of the time. In fact, it cast enough doubt in the minds of Einstein, Podolsky and Rosen that they decided to call quantum mechanics incomplete. They based their argument on the then already well-established uncertainty principle. Consider two parties, Alice and Bob, each holding one of two systems that are in an entangled state. Alice performs a measurement of one of two conjugate observables on her system, while Bob measures the other observable. Since the two systems are entangled, this way they could together learn about both conjugate properties of each system simultaneously with arbitrary precision, which is in violation with the uncertainty principle. This paradox became famously known as the EPR paradox. EPR reconciled the paradox by claiming that quantum mechanics was incomplete and that *reality* in nature was necessarily *local* and that there perhaps exist some local hidden variables, which contain information about the outcomes of all possible measurements on the individual systems. Decades later, Bell discovered a way to compare the predictions of quantum theory with those of any local hidden variable theory in a quantitative fashion. These are the now famous Bell's inequalities, which are bounds on allowed correlations in any local hidden variable theory. Bell showed that these bounds could be violated by entangled quantum states, thus establishing that in theory quantum mechanics allowed for correlations that could not always be replicated by a local hidden variable model. Numerous experiments have now confirmed that nature indeed violates the bounds predicted by local hidden variable theories and, moreover, the results of these experiments agree with the predictions of quantum mechanics.

Quantum discord. Entanglement is the most prominent manifestation of quantum correlations, but it is not the only type of quantum correlation. For example, there is quantum discord, which is defined for a multiparty quantum state based on the difference between the total amount of correlations in the state and those that can be accounted for within classical physics—with the difference being attributed to purely quantum correlations. Quantum discord includes entanglement-type correlations, but goes beyond and captures other weaker quantum correlations that result from *non-orthogonality* of quantum states too. Non-orthogonality of quantum states can be understood as the following: while in classical physics a collection of distinct states (well-defined position and momentum coordinates) are completely distinguishable (or orthogonal mathematical speaking), a collection of distinct quantum states could have overlap and thus may not be completely distinguishable from one another. This possibility with quantum states already takes us out of the realms of classical physics when it comes to multiparty correlations.

Quantum correlations as a resource for information processing. Quantum mechanics, being a fundamental theory of nature, has a bearing on our ability to process information physically. Thus, quantum mechanics has direct consequences for computational, communication and cryptographic technologies. In this regard, the classical theories of computation, communication, and cryptography have been revisited to study the effects of quantum mechanics with regard to their ultimate possible performances. This has lead to exciting new possibilities in these areas, such as quantum algorithms for fast integer factorization, fast database search, quantum teleportation, superdense coding and quantum key distribution [171, 75, 14, 56, 12]. The same is also true for metrology, i.e., the study of precision measurements. The theory of parameter estimation, which underlies metrology has been similarly revisited based on quantum mechanics, which has enabled enhanced parameter estimation. Some of these novel and enhanced quantum technologies rely on the use of quantum entanglement as a resource. For example, in linear metrology, probe systems prepared in suitable entangled quantum states enable estimation of unknown quantities of interest at precisions beyond what is known to be possible classically, the latter being known as the shot-noise limit.

Characterizing quantum correlations using the synergy with quantum information theory. We mentioned earlier how all information-processing technologies must take into account the effects of quantum mechanics since information processing ultimately happened on a physical substrate, whose laws are governed by quantum mechanics. On the other hand, it has been realized that the notion of information, and information processing abilities of a physical substrate can also very helpful towards improving our understanding of quantum mechanics. For example, the entropy, which is a fundamental measure of information, and various other information quantities which are linear combinations of entropies, find crucial meaning in the context of characterizing and quantifying quantum correlations. Therefore, the benefits of the cross-over between quantum mechanics and information theory in the form of quantum information theory are mutual to both theories.

1.2 Outline and Contributions

The specific topics discussed in this thesis lie at the interface of quantum information theory, quantum estimation theory and quantum optics. We divide the chapters into two parts.

Part I focuses on the characterization and quantification of quantum correlations. We consider the information quantity called the quantum conditional mutual information (QCMI), which is widely used in quantum information theory. The QCMI captures the correlation that can exist between three quantum systems that are together described by a quantum state. (A detailed introduction to the QCMI is provided in Appendix A.) As with any other information-theoretic quantity, the QCMI is traditionally defined in terms of the von Neumann entropies. It has been a long-standing open question to obtain Rényi generalizations of the QCMI. Recently, in a joint work with Mario Berta and Mark Wilde, the present author proposed and studied several Rényi generalizations of the QCMI [18, 17]. (A detailed account of these Rényi QCMIs is provided in Appendix B.) In Part I, we use one of those Rényi QCMIs and its variant to define bipartite entanglement measures, i.e., quantifiers of entanglement for two-party systems. The measures we define are related to the squashed entanglement, which is a previously proposed measure based on the QCMI. The squashed entanglement is known to be a good quantifier of entanglement, satisfying many desired properties of an entanglement measure. We also define measures of quantum discord based on the Rényi QCMI. In particular, we define and study a measure of quantum entanglement called the *geometric squashed entanglement*, and a quantum discord-like measure called the *surprisal of measurement recoverability*.

On the other hand, Part II focuses on entanglement-enhanced quantum technologies for sensing. (A detailed introduction to quantum-enhanced sensing is provided in Appendix C.) We consider the optical entanglement generated by the mixing of coherent light and squeezed vacuum light, and study phase estimation at precisions better than the classical shot noise limit in Mach Zehnder interferometry. In particular, we focus on the detection scheme, which is based on the measurement of photon-number parity in one of the two output modes. We determine the Cramér-Rao bound, which is a figure of merit in quantum parameter estimation theory, for the interferometry with coherent light and squeezed-vacuum light, and photon-number parity measurement. We show that this can attain the best estimation performance that is possible with the given state. We also consider the general problem of whether photon-number parity is optimal whenever photon number detection is optimal. We show that this is true for almost all states for which photon number detection is optimal.

Below we give an outline of the thesis.

- Chapter 2 - Preliminaries. In this chapter, we present a brief introduction to the mathematical machinery of quantum mechanics, quantum information theory, the theory of entanglement measures, quantum optics and quantum parameter estimation for the convenience of the reader.

- Chapter 3 - Rényi Squashed Entanglement and Rényi Quantum Discord. In this chapter, we use a Rényi QCMI (see Appendix B) to define a squashed entanglement and a quantum discord. By taking as a conjecture that the Rényi QCMI of a tripartite state ρ_{ABC} is monotone under local completely positive and trace preserving (CPTP) maps on both systems A and B, we prove various properties of these quantities and establish them as valid measures of quantum correlation (up to the conjecture). This is joint work with Mario Berta and Mark Wilde, and can be found in [164].

- Chapter 4 - Fidelity of Recovery, Geometric Squashed Entanglement and Measurement Recoverability. Although the Rényi squashed entanglement and Rényi quantum discord of Chapter 3 are well-behaved correlation measures, they rely on an unproven conjecture, namely that the Rényi QCMI of a tripartite state ρ_{ABC} is monotone under local CPTP maps on both systems A and B. In this chapter, we consider a variant of a particular Rényi QCMI to define a squashed entanglement and a quantum discord. We call them the geometric squashed entanglement and the surprisal of measurement recoverability. These quantities satisfy nearly all the same properties as their traditional counterparts. The underlying quantity behind these measures, which is monotone under local CPTP maps on both systems A and B, is the fidelity of recovery. The fidelity of recovery for a tripartite state ρ_{ABC} quantifies how well one can recover the full state on all three systems if system A is lost and a recovery quantum channel acts only on system C. This is joint work with Mark Wilde, and can be found in [167].

- Chapter 5 - Optimal Phase Estimation with Parity Detection. This chapter contains the original results of Part II of the thesis. In here, we discuss two-mode optical interferometry with the non-classical detection strategy based on photon-number parity measurement. In particular, we ask the question "For what class of two-mode pure states is the photon-number parity observable optimal for phase estimation?" We answer this question in light of Hofmann's work on the analogous question for photon-number detection-based measurement observables. Hofmann, in his work, derived a condition called path symmetry as a sufficient condition on a two-mode pure state so that photon-number counting-based measurement observables are optimal for the state. We analyze the performance of photon-number parity detection for Hofmann's path-symmetric states. We show that photon-number parity is an optimal measurement for a restricted class of path-symmetric states, and that there exists a bias phase at which the optimality is achieved locally. We also discuss the particular interferometry with coherent light mixed with squeezed vacuum light, which is known to achieve the Heisenberg limit when the inputs are mixed in equal intensities. We show that photon-number parity is optimal for this scheme and enables Heisenberg-limited phase estimation with the state. This chapter is based on joint work with Petr Anisimov, Sejong Kim, Hwang Lee and Jonathan Dowling, and can be found in [165, 166].

- Chapter 6 - Conclusions and Outlook. In this chapter, we summarize our main contributions and discuss some possible directions for future work.

Chapter 2
Preliminaries

In this chapter, we give a brief introduction to some essential concepts and the mathematical machinery of quantum mechanics, quantum information theory, the theory of entanglement measures, quantum optics and quantum parameter estimation theory for the convenience of the reader.

2.1 Quantum Mechanics: The Mathematical Machinery

2.1.1 Bounded linear operators, norms and functions

Let $\mathcal{B}(\mathcal{H})$ denote the algebra of bounded linear operators acting on a Hilbert space $\mathcal{H}$. We restrict ourselves to finite-dimensional Hilbert spaces in Part I of the thesis, while Part II involves infinite-dimensional Hilbert spaces. For $\alpha \geq 1$, the α-norm of an operator X is defined as

$$\|X\|_\alpha \equiv \left[\operatorname{Tr}\{(\sqrt{X^\dagger X})^\alpha\}\right]^{1/\alpha}, \tag{2.1.1}$$

and we use the same notation even for the case $\alpha \in (0,1)$, when it is not a norm. Let $\mathcal{B}(\mathcal{H})_+$ denote the subset of positive semi-definite operators, and let $\mathcal{B}(\mathcal{H})_{++}$ denote the subset of positive definite operators. We also write $X \geq 0$ if $X \in \mathcal{B}(\mathcal{H})_+$ and $X > 0$ if $X \in \mathcal{B}(\mathcal{H})_{++}$.

We take the usual convention that $f(A) = \sum_{i:a_i \neq 0} f(a_i) |i\rangle\langle i|$ when given a function f and a Hermitian operator A with spectral decomposition $A = \sum_i a_i |i\rangle\langle i|$. So this means that A^{-1} is interpreted as a generalized inverse, so that $A^{-1} = \sum_{i:a_i\neq 0} a_i^{-1} |i\rangle\langle i|$, $\log(A) = \sum_{i:a_i>0} \log(a_i) |i\rangle\langle i|$, $\exp(A) = \sum_i \exp(a_i) |i\rangle\langle i|$, etc. The above convention for $f(A)$ leads to the convention that A^0 denotes the projection onto the support of A, i.e., $A^0 = \sum_{i:a_i\neq 0} |i\rangle\langle i|$, where the support of a positive semi-definite operator is defined as the subspace spanned by eigenvectors corresponding to nonzero eigenvalues. We employ the shorthand $\operatorname{supp}(A)$ and $\ker(A)$ to refer to the support and kernel of an operator A, respectively, where the latter is the subspace orthogonal to the support.

2.1.2 Quantum states

States in quantum mechanics are most generally described by linear operators known as density operators. An operator ρ is in the set $\mathcal{S}(\mathcal{H})$ of density operators if $\rho \in \mathcal{B}(\mathcal{H})_+$ and $\operatorname{Tr}\{\rho\} = 1$, and an operator ρ is in the set $\mathcal{S}(\mathcal{H})_{++}$ of strictly positive definite density operators if $\rho \in \mathcal{B}(\mathcal{H})_{++}$ and $\operatorname{Tr}\{\rho\} = 1$. The tensor product of two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ is denoted by $\mathcal{H}_A \otimes \mathcal{H}_B$ or $\mathcal{H}_{AB}$. Given a multipartite density operator $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, we unambiguously write $\rho_A = \operatorname{Tr}_B\{\rho_{AB}\}$ for the reduced density operator on system A. (Note that when we write ρ_A, an identity operator is implicit, and the expression should be interpreted as $\rho_A \otimes I_B$.) We use ρ_{AB}, σ_{AB}, τ_{AB}, ω_{AB}, etc. to denote general density operators in $\mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, while ψ_{AB}, ϕ_{AB}, etc. denote rank-one density operators (pure states $|\psi\rangle_{AB}$,

$|\phi\rangle_{AB}$, etc., respectively) in $\mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ (with it implicit, clear from the context, and the above convention implying that ψ_A, φ_A, ϕ_A may be mixed if $|\psi\rangle_{AB}$, $|\phi\rangle_{AB}$ are pure).

Schmidt decomposition. Any bipartite pure state $|\psi\rangle_{AB}$ in $\mathcal{H}_{AB}$ can be written in its Schmidt form as

$$|\psi\rangle_{AB} \equiv \sum_{i=0}^{d-1} \sqrt{\lambda_i}\, |i\rangle_A\, |i\rangle_B\,, \tag{2.1.2}$$

where $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ form orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, the coefficients λ_i are real numbers satisfying $1 \geq \lambda_i \geq 0\, \forall i$, $\sum_{i=0}^{d-1} \lambda_i = 1$, and d is the Schmidt rank of the state. A bipartite pure state is said to be entangled if its Schmidt rank is larger than 1.

Purification. Consider a density operator on system A, whose spectral decomposition is given by

$$\rho_A = \sum_x p_X(x)\, |x\rangle \langle x|_A\,.$$

A purification of ρ_A is a pure bipartite state $|\psi\rangle_{RA}$ on the original system A and a reference system R that satisfies the following property:

$$\rho_A = \mathrm{Tr}_R \left\{ |\psi\rangle \langle \psi|_{RA} \right\}.$$

An example of a purification of ρ_A is given by

$$|\psi\rangle_{RA} = \sum_x \sqrt{p_X(x)}\, |x\rangle_R\, |x\rangle_A\,.$$

2.1.3 Quantum channels

A linear map $\mathcal{N}_{A\to B} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is positive if $\mathcal{N}_{A\to B}(\sigma_A) \in \mathcal{B}(\mathcal{H}_B)_+$ whenever $\sigma_A \in \mathcal{B}(\mathcal{H}_A)_+$. A linear map $\mathcal{N}_{A\to B} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is strictly positive if $\mathcal{N}_{A\to B}(\sigma_A) \in \mathcal{B}(\mathcal{H}_B)_{++}$ whenever $\sigma_A \in \mathcal{B}(\mathcal{H}_A)_{++}$. Let id_A denote the identity map acting on a system A. A linear map $\mathcal{N}_{A\to B}$ is completely positive if the map $\mathrm{id}_R \otimes \mathcal{N}_{A\to B}$ is positive for a reference system R of arbitrary size. A linear map $\mathcal{N}_{A\to B}$ is trace preserving if $\mathrm{Tr}\{\mathcal{N}_{A\to B}(\tau_A)\} = \mathrm{Tr}\{\tau_A\}$ for all input operators $\tau_A \in \mathcal{B}(\mathcal{H}_A)$. If a linear map is completely positive and trace-preserving (CPTP), we call it a quantum channel or quantum operation.

2.1.4 Quantum measurements

A quantum measurement is a quantum channel which has a quantum input and a classical output. The most general quantum measurement is a positive operator-valued measure (POVM), which is a set $\{\Lambda^x\}$ of positive semi-definite operators such that $\sum_x \Lambda^x = I$. Given a state ρ and a POVM $\{\Lambda^x\}$, the probability of obtaining the outcome x is given by

$$p(x) = \mathrm{Tr}\{\Lambda^x \rho\}\,.$$

2.1.5 Some important classes of quantum states

Maximally entangled states. By a maximally entangled state, we mean a bipartite pure state of the form

$$|\Phi\rangle_{AB} \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B . \tag{2.1.3}$$

Private states. A state $\gamma_{ABA'B'}$ is a private state [94, 96] if Alice and Bob can extract a secret key from it by performing local von Neumann measurements on the A and B systems of $\gamma_{ABA'B'}$, such that the resulting secret key is product with any purifying system of $\gamma_{ABA'B'}$. The systems A' and B' are known as "shield systems" because they aid in keeping the key secure from any eavesdropper possessing the purifying system. A private state of $\log d$ private bits can be written in the following form [94, 96]:

$$\gamma_{ABA'B'} = U_{ABA'B'} \left(\Phi_{AB} \otimes \rho_{A'B'}\right) U^{\dagger}_{ABA'B'}, \tag{2.1.4}$$

where Φ_{AB} is the projection onto a maximally entangled state of Schmidt rank d and

$$U_{ABA'B'} = \sum_{i,j} |i\rangle \langle i|_A \otimes |j\rangle \langle j|_B \otimes U^{ij}_{A'B'}, \tag{2.1.5}$$

is called the "twisting unitary". The unitaries that make up $U_{ABA'B'}$ can be chosen such that $U^{ij}_{A'B'} = V^{j}_{A'B'}$ or $U^{ij}_{A'B'} = V^{i}_{A'B'}$. This implies that the unitary $U_{ABA'B'}$ can be implemented either as

$$U_{ABA'B'} = \sum_{i} |i\rangle \langle i|_A \otimes I_B \otimes V^{i}_{A'B'} \tag{2.1.6}$$

or

$$U_{ABA'B'} = I_A \otimes \sum_{i} |i\rangle \langle i|_B \otimes V^{i}_{A'B'}. \tag{2.1.7}$$

2.2 Quantum Information Theory: Tools

2.2.1 Distance measures

Trace distance. The trace distance between two quantum states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ is equal to

$$\|\rho - \sigma\|_1 = \operatorname{Tr}\left\{\sqrt{(\rho - \sigma)^{\dagger} (\rho - \sigma)}\right\}. \tag{2.2.1}$$

The trace distance is bound as follows:

$$0 \le \|\rho - \sigma\|_1 \le 2, \tag{2.2.2}$$

with it being equal to zero if the state are equivalent, and equal to two if they have support on orthogonal subspaces. It has a direct operational interpretation in terms of the distinguishability of these states. If ρ or σ are prepared with equal probability and the task is to distinguish them via some quantum measurement, then the optimal success probability in doing so is equal to $\left(1 + \|\rho - \sigma\|_1 / 2\right) / 2$.

The trace distance obeys a triangle inequality, namely, if ρ, σ and τ are three quantum states, then

$$\left\|\rho-\sigma\right\|_1 \leq \left\|\rho-\tau\right\|_1 + \left\|\tau-\sigma\right\|_1 . \tag{2.2.3}$$

It is monotone non-increasing under quantum operations on state ρ and σ, i.e.,

$$\left\|\mathcal{N}\left(\rho\right)-\mathcal{N}\left(\sigma\right)\right\|_1 \leq \left\|\rho-\sigma\right\|_1 , \tag{2.2.4}$$

where $\mathcal{N}$ is a quantum channel.

Fidelity. The fidelity between two quantum states $\rho, \sigma \in \mathcal{S}\left(\mathcal{H}\right)$ is equal to

$$F\left(\rho,\sigma\right) \equiv \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1^2 . \tag{2.2.5}$$

The fidelity is bound as follows:

$$0 \leq F\left(\rho,\sigma\right) \leq 1, \tag{2.2.6}$$

with it being equal to one if and only if the states are identical and equal to zero if and only if their respective supports are orthogonal. It captures how well a purification of the state ρ can pass as a purification of the state σ. For pure states $|\psi\rangle$ and $|\phi\rangle$, the fidelity reduces to the overlap between the two states

$$F\left(|\psi\rangle, |\phi\rangle\right) \equiv \left|\langle\psi|\, \phi\rangle\right|^2 . \tag{2.2.7}$$

For a pure state $|\psi\rangle$ and a mixed state σ, it reduces to the expectation of σ with respect to $|\psi\rangle$

$$F\left(|\psi\rangle, \sigma\right) \equiv \langle\psi|\, \sigma\, |\psi\rangle . \tag{2.2.8}$$

For two mixed states ρ_A and σ_A on system A, the fidelity is also equal to the following optimized overlap between purifications $|\psi_\rho\rangle_{RA}$ and $|\phi_\sigma\rangle_{RA}$ of the respective states

$$F\left(\rho,\sigma\right) \equiv \max_{|\psi_\rho\rangle_{RA}, |\phi_\sigma\rangle_{RA}} \left|\langle\psi_\rho|\, \phi_\sigma\rangle\right|^2 \tag{2.2.9}$$

$$= \max_U \left|\langle\psi_\rho|\, U_R \otimes I_A \,|\phi_\sigma\rangle\right|^2 , \tag{2.2.10}$$

a result due to Uhlmann, where U_R is a unitary acting on the purifying system R.

Among other properties, the fidelity is multiplicative over tensor product states, i.e.

$$F\left(\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2\right) = F\left(\rho_1, \sigma_1\right) F\left(\rho_2, \sigma_2\right) . \tag{2.2.11}$$

The square root of the fidelity is jointly concave in the state, i.e.

$$\sqrt{F\left(\sum_x p_X\left(x\right)\rho_x, \sum_x p_X\left(x\right)\sigma_x\right)} \geq \sum_x p_X\left(x\right)\sqrt{F\left(\rho_x,\sigma_x\right)}. \tag{2.2.12}$$

Also it is concave in the state, i.e.

$$F\left(\lambda\rho_1 + \left(1-\lambda\right)\rho_2, \sigma\right) \geq \lambda F\left(\rho_1,\sigma\right) + \left(1-\lambda\right) F\left(\rho_2,\sigma\right) . \tag{2.2.13}$$

The fidelity is monotone non-decreasing under quantum operations on state ρ and σ, i.e.,

$$F\left(\rho,\sigma\right) \leq F\left(\mathcal{N}\left(\rho\right), \mathcal{N}\left(\sigma\right)\right) , \tag{2.2.14}$$

where $\mathcal{N}$ is a quantum channel.

Theorem 2.1. *The following bounds hold between the fidelity and the trace distance of two quantum states ρ and σ:*

$$1-\sqrt{F(\rho,\sigma)} \leq \frac{1}{2}\|\rho-\sigma\|_1 \leq \sqrt{1-F(\rho,\sigma)}. \tag{2.2.15}$$

Proof. See [196, Theorem 9.3.1]. ■

Corollary 2.2. *Suppose ρ is ϵ-close to σ in trace distance, i.e.,$\|\rho-\sigma\|_1 \leq \epsilon$, then the fidelity between ρ and σ is greater than $1-\epsilon$, i.e., $F(\rho,\sigma) \geq 1-\epsilon$. Also, suppose $F(\rho,\sigma) \geq 1-\epsilon$, then $\|\rho-\sigma\|_1 \leq \sqrt{2}\epsilon$.*

2.2.2 Entropic (Information) measures

von Neumann entropy. The von Neumann entropy of a quantum state ρ_A is defined as

$$H(\rho) = H(A)_\rho \equiv -\operatorname{Tr}\{\rho \log \rho\}. \tag{2.2.16}$$

It is equivalent to the Shannon entropy of the spectral distribution of the state. That is, if the spectral decomposition of the state is

$$\rho_A = \sum_x p_X(x) |\psi_x\rangle \langle\psi_x|_A, \tag{2.2.17}$$

then

$$H(A)_\rho = -\sum_x p_X(x) \log p_X(x). \tag{2.2.18}$$

Consider that Alice prepares a quantum state from the ensemble $\{p_X(x), |\psi_x\rangle\}$ at random and sends to Bob, who does not know a priori which state was prepared. The von Neumann entropy then captures the average amount of "surprisal" or "information" gained by Bob upon receiving the state in terms of number of qubits of information (assuming the log is to the base two). The entropy of a quantum state ρ_A is bound as

$$\log|A| \geq H(A)_\rho \geq 0, \tag{2.2.19}$$

where $|A|$ is the dimension of A. It is equal to zero when ρ is a pure state and is equal to $\log|A|$ when the state is maximally mixed, i.e.,

$$\rho_A = \sum_{x=1}^{|A|} \frac{1}{|A|} |\psi_x\rangle \langle\psi_x|_A. \tag{2.2.20}$$

The entropy is concave in the state, i.e.,

$$H(\rho) \geq \sum_x p_X(x) H(\rho_x), \tag{2.2.21}$$

where $\rho = \sum_x p_X(x) \rho_x$. It is invariant under the action of unitary operations on the state, i.e.,

$$H(\rho) = H\left(U\rho U^\dagger\right). \tag{2.2.22}$$

It is additive on tensor product states, i.e.

$$H(\rho \otimes \sigma) = H(\rho) + H(\sigma), \tag{2.2.23}$$

and sub-additive in general, i.e., for a bipartite state ρ_{AB}

$$H(AB)_\rho \leq H(A)_\rho + H(B)_\rho. \tag{2.2.24}$$

Rényi entropy. The Rényi entropy is a one-parameter generalization of the von Neumann entropy and is defined for a state ρ_A as

$$H_\alpha(A)_\rho \equiv \frac{1}{1-\alpha} \log \operatorname{Tr}\{\rho^\alpha\} \tag{2.2.25}$$

$$= \frac{\alpha}{1-\alpha} \log \|\rho\|_\alpha, \tag{2.2.26}$$

for $\alpha \in (0,1) \cup (1,\infty)$ (with it being defined for $\alpha \in \{0,1,\infty\}$ in the limit as α tends to zero, one and infinity, respectively.) For a state ρ, whose spectral decomposition is given by

$$\rho_A = \sum_x p_X(x) |\psi_x\rangle \langle\psi_x|_A, \tag{2.2.27}$$

the Rényi entropy is equal to

$$H_\alpha(A)_\rho = \frac{1}{1-\alpha} \log \sum_x p_X(x)^\alpha. \tag{2.2.28}$$

In the limit $\alpha \to 1$, the Rényi entropy converges to the von Neumann entropy. Similar to the von Neumann entropy, the Rényi entropy is also bound as

$$\log|A| \geq H_\alpha(A)_\rho \geq 0, \tag{2.2.29}$$

where $|A|$ is the dimension of A. It is equal to zero when ρ is a pure state and is equal to $\log|A|$ when the state is maximally mixed as in (2.2.20). It is also invariant under the action of unitary operations on the state, i.e.,

$$H_\alpha(\rho) = H_\alpha\left(U\rho U^\dagger\right), \tag{2.2.30}$$

and additive on tensor product states, i.e.

$$H_\alpha(\rho \otimes \sigma) = H_\alpha(\rho) + H_\alpha(\sigma). \tag{2.2.31}$$

Unlike the von Neumann entropy, the Rényi entropy does not obey subadditivity in general.

Relative entropy. For $\rho \in \mathcal{S}(\mathcal{H})$ (a density operator) and $\sigma \in \mathcal{B}(\mathcal{H})_+$ (a positive semi-definite operator), the Umegaki relative entropy [189] is defined as

$$D(\rho\|\sigma) \equiv \begin{cases} \operatorname{Tr}\{\rho[\log\rho - \log\sigma]\} & \text{if } \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \\ +\infty & \text{otherwise} \end{cases}. \tag{2.2.32}$$

The relative entropy $D(\rho\|\sigma)$ is non-negative if $\mathrm{Tr}\{\rho\} \geq \mathrm{Tr}\{\sigma\}$, a result known as Klein's inequality [117]. Thus, when $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ (i.e. when both ρ and σ are density operators), the relative entropy is non-negative, and furthermore, it is equal to zero if and only if $\rho = \sigma$.

The above definition is consistent with the following limit:

$$\lim_{\xi \searrow 0} \mathrm{Tr}\left\{\rho\left[\log \rho - \log\left(\sigma + \xi I\right)\right]\right\} = D(\rho\|\sigma), \tag{2.2.33}$$

where I is the identity operator acting on $\mathcal{H}$. The statement in (2.2.33) follows because the quantity

$$\lim_{\xi \searrow 0} \mathrm{Tr}\left\{\rho \log\left(\sigma + \xi I\right)\right\} \tag{2.2.34}$$

is finite and equal to $\mathrm{Tr}\{\rho \log \sigma\}$ if $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$. Otherwise, (2.2.34) is infinite.

The relative entropy is sometimes referred to as the "mother of all entropies" since other entropic quantities can be written in terms of the relative entropy. For example, the quantum entropy, conditional entropy and mutual information can be written respectively as

$$H(A)_\rho = -D(\rho_A\|I_A), \tag{2.2.35}$$

$$H(A|B)_\rho \equiv H(AB)_\rho - H(B)_\rho = -\min_{\sigma_B} D(\rho_{AB}\|I_A \otimes \sigma_B), \tag{2.2.36}$$

$$I(A;B)_\rho \equiv H(A)_\rho + H(B)_\rho - H(AB)_\rho = \min_{\sigma_B} D(\rho_{AB}\|\rho_A \otimes \sigma_B), \tag{2.2.37}$$

Theorem 2.3. *[Pinsker inequality] The relative entropy is an upper bound on the trace distance:*

$$\frac{1}{2\ln 2}\left(\|\rho - \sigma\|_1\right)^2 \leq D\left(\rho\,\|\sigma\right).$$

Proof. See [196, Theorem 11.9.5]. ■

Rényi relative entropy. For $\rho \in \mathcal{S}(\mathcal{H})$ (a density operator) and $\sigma \in \mathcal{B}(\mathcal{H})_+$ (a positive semi-definite operator), the Rényi relative entropy of order $\alpha \in [0,1) \cup (1,\infty)$ [140] is defined as

$$D_\alpha(\rho\|\sigma) \equiv \begin{cases} \frac{1}{\alpha-1}\log \mathrm{Tr}\left\{\rho^\alpha \sigma^{1-\alpha}\right\} & \text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \text{ or } (\alpha \in [0,1) \text{ and } \rho \not\perp \sigma) \\ +\infty & \text{otherwise} \end{cases}, \tag{2.2.38}$$

with the support conditions established in [183]. It is traditionally defined for $\alpha \in \{0, 1, \infty\}$ in the limit as α approaches 0, 1, and ∞, respectively. The Rényi relative entropy $D_\alpha(\rho\|\sigma)$ is non-negative for all $\alpha \in [0,1) \cup (1,2]$ whenever $\mathrm{Tr}\{\rho\} \geq \mathrm{Tr}\{\sigma\}$. This implies that it is always non-negative when $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ (i.e. when both ρ and σ are density operators). Furthermore, it is equal to zero if and only if $\rho = \sigma$.

The above definition is consistent with the following limit for $\alpha \in [0,1) \cup (1,\infty)$

$$\lim_{\xi \searrow 0} \frac{1}{\alpha - 1} \log \mathrm{Tr}\left\{\left[\mathrm{Tr}\left\{P\right\}\right]^{-1} P^\alpha \left(Q + \xi I\right)^{1-\alpha}\right\} = D_\alpha(P\|Q), \tag{2.2.39}$$

as can be checked by a proof similar to [132, Lemma 13].

Sandwiched Rényi relative entropy. For $\rho \in \mathcal{S}(\mathcal{H})$ (a density operator) and $\sigma \in \mathcal{B}(\mathcal{H})_+$ (a positive semi-definite operator), the sandwiched Rényi relative entropy of order $\alpha \in (0,1) \cup (1,\infty)$ is defined as [132, 198]

$$\widetilde{D}_\alpha(\rho\|\sigma) \equiv \begin{cases} \frac{1}{\alpha-1}\log\left[\operatorname{Tr}\left\{\left(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right)^\alpha\right\}\right] & \begin{array}{c}\text{if } \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \text{ or} \\ (\alpha \in (0,1) \text{ and } \rho \not\perp \sigma)\end{array} \\ +\infty & \text{otherwise}\end{cases}. \tag{2.2.40}$$

The sandwiched Rényi relative entropy $\widetilde{D}_\alpha(\rho\|\sigma)$ is non-negative for all $\alpha \in [1/2,1) \cup (1,\infty)$ whenever $\operatorname{Tr}\{\rho\} \geq \operatorname{Tr}\{\sigma\}$, so that it is always non-negative for density operators ρ and σ. Furthermore, it is equal to zero if and only if $\rho = \sigma$. The sandwiched Rényi relative entropy has found a number of applications in quantum information theory recently in the context of strong converse theorems [198], [131], [76], [184].

The above definition is consistent with the following limit

$$\lim_{\xi \searrow 0} \frac{1}{\alpha-1}\log\left[\operatorname{Tr}\left\{\left[(\sigma+\xi I)^{(1-\alpha)/2\alpha}\rho\,(\sigma+\xi I)^{(1-\alpha)/2\alpha}\right]^\alpha\right\}\right] = \widetilde{D}_\alpha(\rho\|\sigma), \tag{2.2.41}$$

as proved in [132, Lemma 13]. Whenever $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma)$ or ($\alpha \in (0,1)$ and $\rho \not\perp \sigma$), it admits the following alternate forms:

$$\widetilde{D}_\alpha(\rho\|\sigma) \equiv \frac{1}{\alpha-1}\log\left[\operatorname{Tr}\left\{\left(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right)^\alpha\right\}\right] \tag{2.2.42}$$

$$= \frac{\alpha}{\alpha-1}\log\left\|\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right\|_\alpha \tag{2.2.43}$$

$$= \frac{\alpha}{\alpha-1}\log\left\|\rho^{1/2}\sigma^{(1-\alpha)/\alpha}\rho^{1/2}\right\|_\alpha. \tag{2.2.44}$$

The most important property of the Rényi and sandwiched Rényi relative entropies, which makes them useful for applications is given in the following theorem:

Theorem 2.4. *The Rényi relative entropy and the sandwiched Rényi relative entropy obey monotonicity under quantum operations for $\alpha \in [0,1) \cup (1,2]$ and $\alpha \in [1/2,1) \cup (1,\infty)$, respectively, i.e., for a quantum operation $\mathcal{N}$,*

$$D_\alpha(\rho\|\sigma) \geq D_\alpha(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))\ \forall\alpha \in [0,1) \cup (1,2], \tag{2.2.45}$$

$$\widetilde{D}_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))\ \forall\alpha \in [1/2,1) \cup (1,\infty). \tag{2.2.46}$$

Proof. See [140] and [65] (also [11, 131, 198, 132] for other proofs of this for more limited ranges of α), respectively. ■

Rényi conditional entropy and Rényi mutual information. The Rényi conditional entropy for a bipartite state ρ_{AB} is defined for $\alpha \in (0,1) \cup (1,\infty)$ as

$$H_\alpha(A|B) \equiv -\min_{\sigma_B} D_\alpha(\rho_{AB}\|I_A \otimes \sigma_B) \tag{2.2.47}$$

$$= \frac{\alpha}{1-\alpha}\log\operatorname{Tr}\left\{\left(\operatorname{Tr}_A\{\rho_{AB}^\alpha\}\right)^{1/\alpha}\right\}, \tag{2.2.48}$$

where D_α is the Rényi relative entropy defined in (2.2.38) and the second equality follows from a Sibson identity [169]. The Rényi quantum mutual information of a bipartite state ρ_{AB} is defined for $\alpha \in (0,1) \cup (1,\infty)$ as

$$I_\alpha (A;B)_\rho \equiv \min_{\sigma_B} D_\alpha \left(\rho_{AB} \| \rho_A \otimes \sigma_B\right) \tag{2.2.49}$$

$$= \frac{\alpha}{\alpha - 1} \log \operatorname{Tr} \left\{ \left(\operatorname{Tr}_A \left\{ \rho_A^{1-\alpha} \rho_{AB}^{\alpha} \right\} \right)^{\frac{1}{\alpha}} \right\}, \tag{2.2.50}$$

where D_α is the Rényi relative entropy defined in (2.2.38) and the second equality follows from a Sibson identity [76, Corollary 8].

2.3 A Brief Review on Entanglement Measures

Entanglement is widely argued as **the** characteristic feature of quantum mechanics. Given the role of entanglement as a resource for quantum information processing, it is important to be able to quantify how entangled a quantum state is. The topic of entanglement measures [96] precisely deals with this question. The theory of entanglement tries to compare and establish an order among states based on their entanglement content. There exist two main approaches to the theory of entanglement measures:

1. Quantification based on single-copy and asymptotic manipulation of quantum states using Local operations and classical communication (LOCC, described below),

2. Quantification based on real-valued mathematical functions that obey certain axioms (which of course includes monotonicity under LOCC).

We now provide a brief overview of both these approaches. Note that we restrict our discussion to the case of finite-dimensional, bipartite, systems.

2.3.1 Entanglement quantification based on LOCC manipulations

What is LOCC? LOCC is a widely used paradigm in entanglement theory. As the name suggests, LOCC defines the set of allowed quantum operations that can be performed locally on the different parts of a bi- or multi-partite quantum state in quantum information processing. A salient feature of LOCC is that it elevates entanglement to the status of a physical resource. Without the LOCC constraint, any bipartite state can be transformed into any other using a suitable nonlocal quantum map.

A typical LOCC protocol consists of compositions of the following operations:

1. Alice performs a quantum instrument, which is a map that has both a quantum as well as a classical output. She forwards the classical output to Bob, who then performs a quantum operation conditioned on the classical data received.

2. Alternatively, Bob performs the initial instrument and transfers the classical data to Alice, who then performs a quantum operation conditioned on the classical data.

Let us now describe LOCC transformations mathematically. Consider a general noisy evolution of a quantum state that produces both a quantum and a classical output. A map that effects such an evolution—often referred to as a *quantum instrument*—can be described using linear completely positive operators $\mathcal{E}_k$, whose sum is trace preserving. For example, the action of a quantum instrument $(\mathcal{E}_k)$ on a density operator ρ_A can be written as

$$\rho_A \rightarrow \tilde{\rho}_{AA'} := \sum_k (\mathcal{E}_k)(\rho_A) \otimes |k\rangle\langle k|_{A'}, \tag{2.3.1}$$

where $\tilde{\rho}_{AA'}$ is a valid density operator, and system A' holds the classical output k. LOCC transformations of a bipartite quantum state ρ_{AB} refer to all those transformations effected within the constraints of use of only unilocal quantum instruments $(\mathcal{E}_k)$ and $(\mathcal{F}_{k'})$ on the subsystems A and B, respectively, along with the ability to exchange the classical outputs k and k' between A and B. Clearly, the set of LOCC transformations is a subset of the set of all allowed quantum maps on the state ρ_{AB}.

Maximally entangled states. Recall the bipartite maximally entangled states of (2.1.3). In fact, for a given dimensionality, these states are not unique, but a class in themselves, which are local unitarily connected to each other. The reason why we know they are maximally entangled is that any pure, or mixed, and entangled, or separable, state can be prepared from them by means of LOCC transformations alone. Since entanglement cannot increase, but only decrease under LOCC transformations, it is clear why such states are more entangled than other entangled states.

Examples of measures based on LOCC manipulations. State manipulation under LOCC transformations can be used to establish a distinction between maximal and non-maximal entangled states as is evident from the very notion of maximally entangled states described above. Going beyond it does not enable comparison between the entanglement content of two arbitrary non-maximally entangled quantum states. This is because LOCC transformations are discontinuous in the space of bipartite density operators; so, given a single copy of two non-maximally entangled quantum states, it may not be possible to transform either into the other. Hence, it may not be possible to conclude which of two given non-maximally entangled states is more entangled, as ideally wished, using LOCC transformations. However, it turns out that by considering a large number of copies of the entangled states, in the asymptotic limit, one can establish a comparison of the entanglement content of even such non-maximally entangled states using LOCC transformations. For example, say we have n and m copies of entangled states ρ and σ, respectively. Consider the transformation $\rho^{\otimes n} \rightarrow \sigma_m$ effected by LOCC transformations on $\rho^{\otimes n}$, where $||\sigma^{\otimes m} - \sigma_m||_1 < \epsilon$, n, m are large numbers and $\epsilon > 0$. A rate $r = m/n$ for the above transformation is said to be *achievable* if there exists LOCC transformations such that, in the limit $n \rightarrow \infty$, the error $\epsilon \rightarrow 0$. Now, one can use the optimal achievable rate r_{sup} to define a measure of the entanglement content of state ρ relative to that of state σ. Two of the most commonly used entanglement measures defined in this fashion in the asymptotic limit are the *entanglement cost* and the *distillable entanglement*.

For a given bipartite entangled state ρ_{AB} on systems A and B, the *entanglement cost* is defined the best rate $r = m/n$ at which m copies of a *2-qubit* maximally entangled state can be transformed approximately into $\rho_{AB}^{\otimes n}$, i.e.,

$$E_C(\rho) = \inf\{r : \lim_{n\to\infty}[\inf_{\Lambda} D(\rho_{AB}^{\otimes n}, \Lambda(|\Phi\rangle\langle\Phi|_{AB}^{\otimes m}))]\}, \tag{2.3.2}$$

where Λ is an LOCC transformation, $|\Phi\rangle_{AB}$ is the *2-qubit* maximally entangled state, and D is any suitable distance measure. It turns out that this measure is the regularization of another entanglement measure called the *entanglement of formation* [81], which is defined as

$$E_f(\rho) = \min_{p(x),|\psi_x\rangle} \sum_x p(x) E_{\text{ent}}(|\psi_x\rangle\langle\psi_x|_{AB}), \tag{2.3.3}$$

where $\rho_{AB} = \sum_x p(x)|\psi_x\rangle\langle\psi_x|_{AB}$ is a spectral decomposition of ρ, and $E_{\text{ent}}(|\psi\rangle\langle\psi|_{AB})$ is the *entropy of entanglement* of the pure state $|\psi\rangle_{AB}$, which is nothing but the von Neumann entropy of the reduced density matrix of $|\psi\rangle_{AB}$ on either of the two systems A or B. That is, the entanglement cost can be shown to be

$$E_C(\rho) = \lim_{n\to\infty} \frac{E_f(\rho_{AB}^{\otimes n})}{n}. \tag{2.3.4}$$

The *distillable entanglement* of a state ρ_{AB} can be defined as

$$E_D(\rho) = \sup\{r : \lim_{n\to\infty}[\inf_{\Lambda\in\text{LOCC}} ||\Lambda(\rho_{AB}^{\otimes n}) - |\Phi\rangle\langle\Phi|_{AB}^{\otimes m}||]\}, \tag{2.3.5}$$

where Λ denotes the set of all possible LOCC transformations and $|\Phi\rangle_{AB}$ is the *2-qubit* maximally entangled state. In analogy with the entanglement cost, this measure is to be understood as the maximum rate at which one may obtain *2-qubit* maximally entangled states from n copies of the state ρ using LOCC transformations.

Pure states: Total order. It is easy to observe that the entanglement cost and the distillable entanglement are defined based on two opposite processes, namely transforming multiple copies of *2-qubit* maximally entangled states into n copies of the state of interest ρ_{AB}, and vice versa. The natural question that arises is whether the two processes become equivalent, or *reversible* under any particular circumstances. It turns out that they do become reversible for pure states ρ_{AB}, and further, the entanglement cost and the distillable entanglement for pure states become identical—both reducing to the entanglement entropy of ρ_{AB}, namely $-\operatorname{Tr}\{\rho_A \log \rho_A\}$. Therefore, given two pure states $|\psi_1\rangle$ and $|\psi_2\rangle$, when one considers a transformation from many copies of one state to many copies of the other via the intermediate step of distilling many *2-qubit* maximally entangled states, reversibility is maintained, which helps to establish a conclusive order between the states in their entanglement content based on the optimal achievable rate of the transformation (which involves nothing but the entropy of entanglement of the relevant pure states).

However, reversibility is lost in the case of mixed states, and hence it becomes difficult to establish total order for mixed entangled states using single-copy or asymptotic state manipulation using LOCC transformations. Hence, one looks for alternative ways to quantify entanglement in mixed states. This leads us to the axiomatic approach, which we discuss next.

2.3.2 Axiomatic approach to entanglement measures

In this approach to entanglement measures, one tries to define real-valued functions that satisfy certain basic axioms which seem reasonable to characterize entanglement, such as convexity, LOCC monotonicity, asymptotic continuity, faithfulness, additivity, and monogamy. We now describe these axioms one by one.

Convexity. Consider a set of distinctly identifiable bipartite quantum states $\{\rho^x_{AB}\}^n_{x=1}$, and another state ρ_{AB}, which is their convex sum $\rho = \sum_x p(x)\rho^x_{AB}$. The process of going from the former (set of identifiable states) to the latter (convex sum) involves a loss of information, which would decrease the amount of entanglement. In line with this observation, we expect the following relation to hold for any entanglement measure defined on the space of these states

$$E(\rho_{AB}) \leq \sum_x p(x)E(\rho^x_{AB}), \tag{2.3.6}$$

where E refers to the entanglement measure.

LOCC monotonicity. Consider a bipartite quantum state ρ_{AB}, and two unilocal quantum instruments $(\mathcal{E}_{k_1})$ and $(\mathcal{F}_{k_2})$, which act on the subsystems A and B, respectively, in order to effect an LOCC transformation. Since entanglement cannot increase under LOCC transformations, we expect the following relation to hold between the input and output states of the LOCC transformation for any entanglement measure E

$$E(\rho_{AC}) \geq \sum_{k_1,k_2} p(k_1,k_2)E(\tilde{\rho}^{k_1,k_2}_{AC}), \tag{2.3.7}$$

where $p(k_1,k_2) = \mathrm{Tr}\{\mathcal{E}^{k_1}_A \otimes \mathcal{E}^{k_2}_C(\rho_{AC})\}$, $\tilde{\rho}^{k_1,k_2}_{AC} = \frac{1}{p(k_1,k_2)}(\mathcal{E}^{k_1}_A \otimes \mathcal{E}^{k_2}_C)(\rho_{AC})$, and k_1, k_2 are classical outputs.

Remark 2.5. *A quantity is an entanglement monotone if it is an LOCC monotone and it is convex [192].*

Additivity. A measure E is additive if $E(\rho \otimes \sigma) = E(\rho) + E(\sigma)$ for state ρ and σ.

Asymptotic continuity. An ideal property for an entanglement measure to possess is that, in the case of pure states, it should reduce to the entropy of entanglement, since the latter represents the optimal reversible rate of conversion between pure states in the asymptotic limit. Asymptotic continuity over pure states is a property that, along with additivity, LOCC monotonicity, and normalization over pure states, guarantees this. For a measure E, and pure states $|\psi\rangle$ and $|\phi\rangle$ such that $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1 \leq \epsilon$, where $\epsilon > 0$ is small, the asymptotic continuity condition can be written as

$$\frac{E(|\psi\rangle\langle\psi|^{\otimes n}) - E(|\phi\rangle\langle\phi|^{\otimes n})}{1 + \log d} \to 0 \tag{2.3.8}$$

when $\epsilon \to 0$, where d is the dimensionality of the Hilbert space. This is related to the Fannes-Audenaert inequality, which states that for density operators ρ and σ on the same d-dimensional Hilbert space with $T \equiv \frac{1}{2}\|\rho - \sigma\|_1$,

$$|H(\rho) - H(\sigma)| \leq T\log(d-1) + H_2(T). \tag{2.3.9}$$

Faithfulness. A measure E is said to be faithful if $E(\rho_{AB})$ is equal to zero if and only if the state ρ_{AB} is separable, i.e., $E(\rho_{AB}) = 0$ if and only if

$$\min_{\sigma_{AB} \in \mathcal{S}_{A:B}} ||\rho_{AB} - \sigma_{AB}|| = 0, \tag{2.3.10}$$

where $\mathcal{S}_{A:B}$ is the set of separable states over the space of systems A and B.

Monogamy. A well-known property of entanglement is that it is monogamous, i.e., if a quantum system is entangled with another, then its possible entanglement with a third system gets constrained. For example, in the extreme case of maximal entanglement, if a system is maximally entangled with another, then it simply cannot be entangled with a third system. It is ideal for an entanglement measure to capture monogamy. One way for a measure E to achieve this is by satisfying inequalities of the form:

$$E(A;B)_\rho + E(A;C)_\rho \leq E(A;BC)_\rho, \tag{2.3.11}$$

where ρ^{ABC} is a tripartite quantum state.

2.4 Quantum Optics: Brief Introduction, Optical States

A quantized mode of the electromagnetic field is completely described by its creation and annihilation operators, $\hat{a}$ and $\hat{a}^\dagger$, which satisfy the commutation relation $\left[\hat{a}, \hat{a}^\dagger\right] = 1$. They are defined by their action on the number states of the mode, $|n\rangle$—also called Fock states, given by:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \qquad \hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{2.4.1}$$

Pure states of the single-mode field (vectors in Hilbert space) can be expressed in terms of the action of a suitable function of the mode creation and annihilation operators on the vacuum state $|0\rangle$. For example, a Fock state $|n\rangle$ is $\frac{\hat{a}^\dagger}{\sqrt{n!}}|0\rangle$, where $|0\rangle$ is the vacuum state. The coherent state is

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle, \tag{2.4.2}$$

where $\hat{D}(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right)$ is called the displacement operator, and α is a complex number that denotes the amplitude of the state. Both the Fock states and the coherent states form complete bases (the coherent states in fact form an over-complete basis). Therefore, any pure state of the quantum single-mode field can be expressed in terms of these states. More generally, any state of the single-mode field, including mixed states, which are ensembles of pure states, can be written in terms of these states in the form of a density operator. For example, the most general state of a single-mode field can be written in the Fock basis as the following density operator:

$$\hat{\rho} = \sum_{n,n'} p_{n,n'}|n\rangle\langle n'|, \ \mathrm{Tr}(\rho) = 1, \ \rho \geq 0. \tag{2.4.3}$$

Alternatively, a quantized mode can be described in terms of quasi-probability distributions in the phase space of eigenvalues x and p of the quadrature operators of the mode $\hat{x}$

and $\hat{p}$. These operators are defined in terms of the creation and annihilation operators of the mode as $\hat{x} = \hat{a}^\dagger + \hat{a}$ and $\hat{p} = i(\hat{a}^\dagger - \hat{a})$, respectively. The Wigner distribution of a single-mode state can be obtained from its density operator of the form in (2.4.3) as:

$$W(\alpha) = \frac{1}{2\pi^2} \int d^2\tilde{\alpha}\, \mathrm{Tr}\left\{\hat{\rho}\hat{D}(\tilde{\alpha})\right\} e^{-\tilde{\alpha}\alpha^* - \tilde{\alpha}^*\alpha}, \tag{2.4.4}$$

where $\tilde{\alpha} = \tilde{x} + i\tilde{p}$ and $\alpha = x + ip$.

Squeezed light [69] refers to minimum uncertainty states of light whose fluctuations with respect to one of any two orthogonal quadratures in phase space has been reduced at the expense of increased fluctuations in the other. They are described mathematically using the squeezing operator. The single-mode squeezing operator acting on a mode $\hat{a}$ is given by:

$$\hat{S}(\xi) = \exp\left(\frac{1}{2}(\xi\hat{a}^{\dagger 2} - \xi^*\hat{a}^2)\right), \tag{2.4.5}$$

where $\xi = re^{i\theta}$, r and θ being the squeezing parameter and squeezing angle, respectively. The squeezed vacuum state, which is the state corresponding to the action of the squeezing operator in (2.4.5) on the vacuum state is given by

$$\begin{aligned} |\xi\rangle &= \hat{S}(\xi)|0\rangle \\ &= \sum_{m=0}^{\infty} \frac{(2m)!}{2^{2m}(m!)^2} \frac{\tanh^{2m} r}{\cosh r} |2m\rangle. \end{aligned} \tag{2.4.6}$$

It has a mean photon number of $\overline{n} = \sinh^2 r$. There are numerous ways to generate squeezed light. The most common method is based on degenerate parametric down conversion using nonlinear crystals that contain second order ($\chi^{(2)}$) susceptibility. When a $\chi^{(2)}$ nonlinear crystal is pumped with photons of frequency ω_p, some of these pump photons get converted into a pair of photons—of frequencies $\omega_p/2$, which are in the single-mode squeezed vacuum state of (2.4.6). The value of the squeezing parameter r is directly related to the power of the pump beam used in the parametric down conversion process.

2.5 Quantum Parameter Estimation Theory

There exist two main paradigms in parameter estimation, (i) where an unknown parameter is assumed to hold a deterministic value, (ii) where an unknown parameter is assumed to be intrinsically random. In this thesis, we focus on the first one.

Consider N identical copies of a quantum state that has acquired information about an unknown parameter of interest. Since the state carries the information about the parameter of interest, say φ, let us denote it as $\hat{\rho}_\varphi$. Now, consider a set of data points $\mathrm{x} = \{x_1, x_2, \ldots, x_\nu\}$ that are obtained from the N copies of $\hat{\rho}_\varphi$ as outcomes of a generalized quantum measurement. Recall that a generalized quantum measurement is a positive operator-valued measure (POVM), which is a collection of positive operators Λ^x, with the index $x \in \{1, 2, \ldots, M\}$ denoting the outcome of the measurement, whose probability of occurrence for a state ρ, is given by $p(x) = \mathrm{Tr}\{\rho\Lambda^x\}$. The elements of a POVM add up to the identity $\sum_x \Lambda^x = I$, which ensures that $p(x)$ is a valid probability distribution. Since the data points are obtained by measuring identical copies of the quantum state , the X_is $\forall i \in \{1, 2, \ldots, \nu\}$ are independent and identically distributed random variables that are distributed according to some probability distribution function $p_\varphi(x)$. The goal is to apply a suitable estimation rule $\widehat{\varphi}_\nu$ to the data points, to obtain a good estimate for the unknown parameter φ.

2.5.1 Classical and quantum Cramér-Rao bounds

When estimation rule $\widehat{\varphi}_\nu$ is applied to a set of data points x, a good measure of precision for the resulting estimate $\widehat{\varphi}_\nu(\mathrm{x})$ is its mean-square error, given by:

$$\Delta^2\widehat{\varphi}_\nu = \mathrm{E}[(\widehat{\varphi}_\nu(\mathrm{x}) - \varphi)^2], \tag{2.5.1}$$

where E denotes expectation value. For any estimation rule $\widehat{\varphi}_\nu$, which is unbiased, i.e.,

$$\mathrm{E}[\widehat{\varphi}_\nu(\mathrm{x})] = \varphi, \tag{2.5.2}$$

the Cramér-Rao theorem of classical estimation theory lower bounds the mean-square error as

$$\Delta^2\widehat{\varphi}_\nu \geq \frac{1}{\nu F(p_\varphi)}, \tag{2.5.3}$$

where $F(p_\varphi)$ is known as the Fisher information of the probability distribution given by

$$F(p_\varphi) = F_{\mathrm{Cl}}(\hat{\rho}_\varphi, \Lambda^x) = \mathrm{E}\left[-\frac{d^2}{d\varphi^2}\log p_\varphi\right]. \tag{2.5.4}$$

The above lower bound is called the *classical Cramér-Rao bound*. It gives the optimal precision of estimation that is possible when both the parameter-dependent quantum state and the measurement scheme are specified. Estimation rules that attain the classical Cramér-Rao bound are called efficient estimators. The maximum-likelihood estimator is an example of an efficient estimator that attains the lower bound in the asymptotic limit.

The quantum theory of parameter estimation further provides an ultimate lower bound on precision of estimation when the quantum state alone is specified. It goes by the name of *quantum Cramér-Rao bound*, and is given by

$$\Delta^2\widehat{\varphi}_\nu \geq \frac{1}{\nu F_Q(\hat{\rho}_\varphi)}, \tag{2.5.5}$$

where $F_Q(\hat{\rho}_\varphi)$ is known as the quantum Fisher information, which is defined as the optimum of the classical Fisher information over all possible generalized measurements:

$$F_Q(\hat{\rho}_\varphi) = \max_{\Lambda^x} F_{\mathrm{Cl}}(\hat{\rho}_\varphi, \Lambda^x). \tag{2.5.6}$$

A measurement scheme that attains this lower bound is called an optimal measurement scheme. The symmetric logarithmic derivative operation is one such measurement, which is known to be optimal for all quantum states [27].

In the case of entangled pure states, the quantum Fisher information takes the simplified expression given by

$$F_Q = 4\Delta^2 H, \tag{2.5.7}$$

where $\hat{H}$ is the generator of parameter evolution. This gives rise to a generalized uncertainty relation between the generating Hamiltonian of parameter evolution and the estimator that is used for estimating the unknown value of the parameter, given by

$$\Delta^2\widehat{\varphi}_\nu \Delta^2 H \geq \frac{1}{4\nu} \tag{2.5.8}$$

for a generating Hamiltonian $\hat{H}$, and where ν is the number of data points gathered from measuring identical copies of the state.

2.5.2 Shot-noise and Heisenberg limits

Consider linear interferometry, i.e., where $\hat{H}$ is linear in the number of probe particles used. Then, for an N-particle probe state, where the probes are uncorrelated, and ν independent and identical probe states, the quantum Cramér-Rao bound scales as

$$\Delta\widehat{\varphi}_\nu \geq \frac{1}{\sqrt{\nu N}}, \tag{2.5.9}$$

referred to as the *shot-noise limit*. It is called so, because the scaling is identical to that of a Poisson-distributed probe state of mean photon number $\bar{n}$, which is given by

$$\Delta\widehat{\varphi}_\nu = \frac{1}{\sqrt{\bar{n}}}, \tag{2.5.10}$$

known in the classical literature as shot noise. On the other hand, when the N probes are prepared in a maximally entangled state, e.g., in the $N00N$ state in two-mode interferometry given by

$$|\Psi\rangle_{N00N} \equiv \frac{1}{\sqrt{2}} \left(|N\rangle_a \otimes |0\rangle_b + |0\rangle_a \otimes |N\rangle_b \right), \tag{2.5.11}$$

then the quantum Cramér-Rao bound at best scales as

$$\Delta\widehat{\varphi}_\nu \geq \frac{1}{\sqrt{\nu}N}, \tag{2.5.12}$$

for ν independent and identical copies of the state. The above lower bound is known as the *Heisenberg limit*.

Part I
Rényi Quantum Conditional Mutual Information and Applications

Chapter 3
Rényi Squashed Entanglement and Rényi Quantum Discord

3.1 Introduction

Quantum information theory is immensely useful in quantifying quantum correlations. Information quantities such as the quantum entropy, conditional entropy, mutual information, and quantum conditional mutual information (QCMI) underlie various measures of quantum correlations. For example, the squashed entanglement and the quantum discord are based upon the QCMI. Also, the operational meanings that the entropic quantities take in information-theoretic protocols aid in understanding the correlation measures defined based on them. The entropy finds operational meaning in the context of quantum data compression, the conditional entropy in quantum state merging, the mutual information in erasure of total correlations and the conditional mutual information in quantum state redistribution.

In this chapter, we study two new quantifiers of quantum correlation defined based on a Rényi QCMI (see Appendix B), namely, a Rényi squashed entanglement and a Rényi quantum discord. We explore various properties of these measures, and some potential applications.

3.2 Rényi Squashed Entanglement

Squashed entanglement: A brief review. The squashed entanglement mentioned above in Section 3.1 is an entanglement measure defined based on the QCMI. We recall the formal definition of the squashed entanglement below.

Definition 3.1. *The squashed entanglement of a bipartite state $\rho_{AB} \in S(\mathcal{H}_{AB})$ is defined as*

$$E^{\mathrm{sq}}(A;B)_\rho \equiv \frac{1}{2} \inf_{\omega_{ABE}} \left\{ I(A;B|E)_\omega : \rho_{AB} = \mathrm{Tr}_E \{\omega_{ABE}\} \right\}, \tag{3.2.1}$$

where the infimum is over all possible extensions ω_{ABE} of the state ρ_{AB} and $I(A;B|E)_\omega$ is the quantum conditional mutual information from (A.2.1).

The squashed entanglement can also be equivalently defined as

$$E^{\mathrm{sq}}(A;B)_\rho \equiv \frac{1}{2} \inf_{\mathcal{S}_{E' \to E}} \left\{ I(A;B|E)_{\mathcal{S}_{E' \to E}(\psi_{ABE'})} \right\}, \tag{3.2.2}$$

where $\psi_{ABE'}$ is any purification of the state ρ_{AB} and $\mathcal{S}_{E' \to E}$ is a quantum channel called the "squashing channel". Conceptually speaking, the squashed entanglement of a state ρ_{AB} shared between Alice and Bob captures how much quantum correlations between Alice and Bob survive despite the attempts of a third party Eve, who has access to an extension of the state, to try and squash down the correlations.

The squashed entanglement is known to hold many of the properties that are desired of an entanglement measure in the axiomatic approach to such measures. For example, it is monotone non-increasing under LOCC, it is additive on tensor product states and subadditive in general [40]. It is faithful in the sense that the measure equals zero if and only if the state is separable [25, 120] and is asymptotically continuous [4]. The squashed entanglement is normalized on maximally entangled states and private states: for a maximally entangled state of Schmidt rank d, the squashed entanglement equals $\log d$ [40], and is at least $\log d$ for a private state of (2.1.4) containing $\log d$ private bits [36, Proposition 4.19]. Further, the squashed entanglement of a state ρ_{AB} is an upper bound on the rate at which Bell states can be distilled per copy of ρ_{AB} using LOCC in the independent and identically distributed (i.i.d.) limit of a large number of copies of the state [40]. Similarly, it is also an upper bound on the rate at which private states can be distilled using LOCC in the i.i.d. limit [37].

A Rényi squashed entanglement. Likewise, a Rényi squashed entanglement can be defined based on a Rényi QCMI. We now formally define the quantity.

Definition 3.2. *The Rényi squashed entanglement of a bipartite state $\rho_{AB} \in S(\mathcal{H}_{AB})$ is defined for $\alpha \in (0,1) \cup (1,\infty)$ as*

$$E^{\mathrm{sq}}_\alpha(A;B)_\rho \equiv \frac{1}{2} \inf_{\omega_{ABE}} \left\{ I_\alpha(A;B|E)_\omega : \rho_{AB} = \mathrm{Tr}_E \{\omega_{ABE}\} \right\}, \tag{3.2.3}$$

where the infimum is over all extensions ω_{ABE} of the state ρ_{AB} and $I_\alpha(A;B|E)_\omega$ is the Rényi quantum conditional mutual information from Definition B.1.

We will now prove some of the afore-mentioned axioms for the Rényi squashed entanglement. However, before we do so, it is important to emphasize that many of the results we prove in this section rely on the following conjecture:

Conjecture 3.3. *The Rényi quantum conditional mutual information of Definition B.1 obeys monotonicity under CPTP maps on system A, i.e., for* $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_{ABE})$ *and* $\alpha \in (0,1) \cup (1,2]$,

$$I_\alpha(A;B|E)_\rho \geq I_\alpha(A';B|E)_\tau\,, \tag{3.2.4}$$

where $\tau_{A'BE} \equiv \mathcal{M}_{A\to A'}(\rho_{ABE})$ *and* $\mathcal{M}_{A\to A'}$ *is a CPTP map acting on system A alone.*

3.2.1 An entanglement monotone

Assuming Conjecture 3.3, we now prove that the Rényi squashed entanglement defined in Definition 3.2 is an entanglement monotone for $\alpha \in (0,1)\cup(1,2]$. In order to do so, we show that under the said assumption, the Rényi squashed entanglement $E_\alpha^{\mathrm{sq}}(A;B)_\rho$ is monotone under local operations and classical communication (LOCC) and convex.

Consequence 3.4. *Assuming Conjecture 3.3, the Rényi squashed entanglement* $E_\alpha^{\mathrm{sq}}(A;B)_\rho$ *is monotone under local operations for* $\alpha \in (0,1)\cup(1,2]$

$$E_\alpha^{\mathrm{sq}}(A;B)_\rho \geq E_\alpha^{\mathrm{sq}}(A';B')_\sigma \tag{3.2.5}$$

where $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$, $\sigma_{A'B'} \equiv (\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{AB})$, *and* $\mathcal{N}_{A\to A'}$ *and* $\mathcal{M}_{B\to B'}$ *are CPTP maps.*

Proof. This follows directly from monotonicity under local operations of the Rényi QCMI $I_\alpha(A;B|E)_\rho$. ■

Consequence 3.5. *Assuming Conjecture 3.3, the Rényi squashed entanglement* $E_\alpha^{\mathrm{sq}}(A;B)_\rho$ *is invariant under classical communication between A and B for* $\alpha \in (0,1)\cup(1,2]$, *i.e.,*

$$E_\alpha^{\mathrm{sq}}(X_A A;B)_\rho = E_\alpha^{\mathrm{sq}}(X_A A;X_B B)_\rho = E_\alpha^{\mathrm{sq}}(A;X_B B)_\rho\,, \tag{3.2.6}$$

where $\rho_{X_A A X_B B} \equiv \sum_x p_X(x)\,|x\rangle\langle x|_{X_A} \otimes |x\rangle\langle x|_{X_B} \otimes \rho^x_{AB}$.

Proof. Let ρ^x_{ABE} be any extension of ρ^x_{AB}, and $|\varphi^{\rho_X}\rangle_{ABER}$ be a purification of ρ^x_{ABE}. Then,

$$\rho_{X_A ABE} \equiv \sum_x p_X(x)\,|x\rangle\langle x|_{X_A} \otimes \rho^x_{ABE}$$

is an extension of $\rho_{X_A AB}$, and

$$|\varphi^\rho\rangle_{X_A X_R ABER} \equiv \sum_x \sqrt{p_X(x)}\,|x\rangle_{X_A} \otimes |x\rangle_{X_R} \otimes |\varphi^{\rho_X}\rangle_{ABER}\,,$$

a purification of $\rho_{X_A ABE}$. Further, consider the state $\overline{\varphi}^\rho_{X_A X_B X_R ABER}$ defined as

$$\overline{\varphi}^\rho_{X_A X_B X_R ABER} \equiv \sum_x p_X(x)\,|x\rangle\langle x|_{X_A} \otimes |x\rangle\langle x|_{X_B} \otimes |x\rangle\langle x|_{X_R} \otimes \varphi^{\rho_x}_{ABER},$$

where the state of X_A has been copied to X_B, and let $\theta_{X_A X_B X_R ABERF}$be a purification of $\overline{\varphi}^{\rho}_{X_A X_B X_R ABER}$. We then have that $I_\alpha\left(X_A A; B\,|E\right)_\rho$

$$
\begin{aligned}
&= I_\alpha\left(B; X_A A\,|X_R R\right)_{\varphi^\rho} && (3.2.7)\\
&\geq I_\alpha\left(B; X_A A\,|X_R R\right)_{\overline{\varphi}^\rho} && (3.2.8)\\
&= \frac{\alpha}{\alpha-1}\log\sum_x p_X\left(x\right)\exp\left\{\left(\frac{\alpha-1}{\alpha}\right) I_\alpha\left(X_A A; B\,|R\right)_{|x\rangle\langle x|_{X_A}\otimes\varphi^{\rho_x}}\right\} && (3.2.9)\\
&= \frac{\alpha}{\alpha-1}\log\sum_x p_X\left(x\right)\exp\left\{\left(\frac{\alpha-1}{\alpha}\right) I_\alpha\left(X_A A; X_B B\,|R\right)_{|x\rangle\langle x|_{X_A}\otimes|x\rangle\langle x|_{X_B}\otimes\varphi^{\rho_x}}\right\} && (3.2.10)\\
&= I_\alpha\left(X_B B; X_A A\,|X_R R\right)_{\overline{\varphi}^\rho} && (3.2.11)\\
&= I_\alpha\left(X_A A; X_B B\,|EF\right)_\theta && (3.2.12)\\
&\geq 2E^{\text{sq}}_\alpha\left(X_A A; X_B B\right)_\rho. && (3.2.13)
\end{aligned}
$$

The first equality follows from duality of the Rényi QCMI. The first inequality is a result of monotonicity under a local dephasing operation

$$\sum |x\rangle\langle x|_{X_A}(\cdot)\,|x\rangle\langle x|_{X_A}, \tag{3.2.14}$$

which relies on Conjecture 3.3. The second equality follows from Lemma D.6 given in Appendix D.2.4. The third equality is an application of Lemma D.7 given in Appendix D.2.5. The fourth equality is from another application of Lemma D.6. The fifth equality is from another application of duality. The final inequality is a result of Definition 3.2. Since the inequality holds for any extension of $\rho_{X_A AB}$, it follows that

$$E^{\text{sq}}_\alpha\left(X_A A; B\right)_\rho \geq E^{\text{sq}}_\alpha\left(X_A A; X_B B\right)_\rho. \tag{3.2.15}$$

By a similar line of reasoning, but without having to rely on Conjecture 3.3, it follows that

$$E^{\text{sq}}_\alpha\left(A; X_B B\right)_\rho \geq E^{\text{sq}}_\alpha\left(X_A A; X_B B\right)_\rho. \tag{3.2.16}$$

However, from monotonicity of E^{sq}_α under local operations, we already know that

$$
\begin{aligned}
E^{\text{sq}}_\alpha\left(X_A A; B\right)_\rho &\leq E^{\text{sq}}_\alpha\left(X_A A; X_B B\right)_\rho, && (3.2.17)\\
E^{\text{sq}}_\alpha\left(A; X_B B\right)_\rho &\leq E^{\text{sq}}_\alpha\left(X_A A; X_B B\right)_\rho. && (3.2.18)
\end{aligned}
$$

Therefore, (3.2.15)-(3.2.18) give the statement of the proposition. ■

Consequence 3.6. *Assuming Conjecture 3.3, Propositions 3.4 and 3.5 together imply that the Rényi squashed entanglement* $E^{\text{sq}}_\alpha\left(A; B\right)_\rho$ *is an LOCC monotone for* $\alpha \in (0,1)\cup(1,2]$.

Proposition 3.7. *The Rényi squashed entanglement* $E^{\text{sq}}_\alpha\left(A; B\right)_\rho$ *is convex for* $\alpha \in (0,1)$, *i.e., for a state* $\bar{\rho}_{AB} \equiv \sum_x p_X\left(x\right)\rho^x_{AB}$,

$$E^{\text{sq}}_\alpha\left(A; B\right)_{\bar{\rho}} \leq \sum_x p_X\left(x\right) E^{\text{sq}}_\alpha\left(A; B\right)_{\rho^x}. \tag{3.2.19}$$

Proof. Let ρ^x_{ABE} be any extension of ρ^x_{AB}. Then

$$\rho_{ABEX} \equiv \sum_x p_X(x) |x\rangle\langle x|_X \otimes \rho^x_{ABE} \tag{3.2.20}$$

is an extension of $\bar{\rho}_{AB}$. Therefore, we have that

$$\begin{aligned} 2E^{\mathrm{sq}}_\alpha(A;B)_{\bar{\rho}} &\leq I_\alpha(A;B|EX)_\rho & (3.2.21)\\ &= \frac{\alpha}{\alpha-1}\log\sum_x p_X(x)\exp\left\{\left(\frac{\alpha-1}{\alpha}\right)I_\alpha(A;B|E)_{\rho^x}\right\} & (3.2.22)\\ &\leq \sum_x p_X(x)\left[\frac{\alpha}{\alpha-1}\log\exp\left\{\left(\frac{\alpha-1}{\alpha}\right)I_\alpha(A;B|E)_{\rho^x}\right\}\right] & (3.2.23)\\ &= \sum_x p_X(x) I_\alpha(A;B|E)_{\rho^x}. & (3.2.24)\end{aligned}$$

The first inequality follows from Definition 3.2. The second inequality follows from the convexity of $-\log$. Of course this step is applicable only for $\alpha \in (0,1)$, which forms the bottleneck of this proof. Since the inequality holds for any extension of each ρ^x_{AB}, we can conclude the statement of the proposition. ■

Consequence 3.8. *Assuming Conjecture 3.3, Remark 3.6 and Proposition 3.7 together imply that the Rényi squashed entanglement $E^{\mathrm{sq}}_\alpha(A;B)_\rho$ is an entanglement monotone for $\alpha \in (0,1)$.*

3.2.2 More properties

Proposition 3.9. *For separable state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$, the Rényi squashed entanglement $E^{\mathrm{sq}}_\alpha(A;B)_\rho$ vanishes for $\alpha \in (0,1)\cup(1,\infty)$.*

Proof. Consider any separable state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$. We can write it as a convex sum of tensor product of pure states as follows:

$$\rho_{AB} = \sum_x p_X(x) |\psi_x\rangle\langle\psi_x|_A \otimes |\phi_x\rangle\langle\phi_x|_B. \tag{3.2.25}$$

Let $\rho_{ABX} = \sum_x p_X(x) |\psi_x\rangle\langle\psi_x|_A \otimes |\phi_x\rangle\langle\phi_x|_B$ be an extension of ρ_{AB}. Then, by applying Lemma D.6, we find that

$$I_\alpha(A;B|X) = \frac{\alpha}{\alpha-1}\log\sum_x p_X(x)\exp^{\left(\frac{\alpha-1}{\alpha}\right)I_\alpha(A;B)_{\psi_x\otimes\phi_x}}. \tag{3.2.26}$$

However, the Rényi mutual information is equal to zero for any product state. This implies that

$$I_\alpha(A;B|X) = \frac{\alpha}{\alpha-1}\log\sum_x p_X(x) = 0. \tag{3.2.27}$$

■

Proposition 3.10. *For tensor product states* $\rho_{A_1A_2B_1B_2} \equiv \sigma_{A_1B_1} \otimes \tau_{A_2B_2} \in \mathcal{S}\left(\mathcal{H}_{A_1A_2B_1B_2}\right)$, *the Rényi squashed entanglement* $E_\alpha^{\mathrm{sq}}\left(A;B\right)_\rho$ *is subadditive for* $\alpha \in (0,1) \cup (1,\infty)$, *i.e.,*

$$E_\alpha^{\mathrm{sq}}\left(A_1A_2;B_1B_2\right)_\rho \leq E_\alpha^{\mathrm{sq}}\left(A_1;B_1\right)_\sigma + E_\alpha^{\mathrm{sq}}\left(A_2;B_2\right)_\tau . \tag{3.2.28}$$

Proof. Let $\sigma_{A_1B_1E_1}$ and $\tau_{A_2B_2E_2}$ be extensions of $\sigma_{A_1B_1}$ and $\tau_{A_2B_2}$. Then, we have that

$$\omega_{A_1B_1E_1A_2B_2E_2} \equiv \sigma_{A_1B_1E_1} \otimes \tau_{A_2B_2E_2} \tag{3.2.29}$$

is an extension of $\rho_{A_1A_2B_1B_2}$. Therefore, we have that

$$\begin{aligned} 2E_\alpha^{\mathrm{sq}}\left(A_1A_2;B_1B_2\right)_\rho &\leq I_\alpha\left(A_1A_2;B_1B_2\left|E_1E_2\right.\right)_\omega &(3.2.30)\\ &= I_\alpha\left(A_1;B_1\left|E_1\right.\right)_\sigma + I_\alpha\left(A_2;B_2\left|E_2\right.\right)_\tau . &(3.2.31)\end{aligned}$$

The inequality follows from Definition 3.2, and equality follows by direct substitution of the state ω into (B.4.11). Since the inequality is independent of the particular extensions $\sigma_{A_1B_1E_1}$ and $\tau_{A_2B_2E_2}$, the statement of the proposition follows. ■

3.2.3 Relations to Rényi entropy of entanglement and Rényi entanglement of formation

The entropy of entanglement [13] and the entanglement of formation [15] are among the earliest proposed measures of entanglement for bipartite pure and mixed states, respectively. The entropy of entanglement of a bipartite pure state $\psi_{AB} \in \mathcal{S}\left(\mathcal{H}_{AB}\right)$ is defined as the von Neumann entropy of either reduced density operators, i.e.,

$$E\left(A;B\right)_\psi \equiv H\left(A\right)_\psi = H\left(B\right)_\psi . \tag{3.2.32}$$

The entanglement of formation of a bipartite mixed state is based upon the entropy of entanglement via an extended convex roof construction. For a state $\rho_{AB} \in \mathcal{S}\left(\mathcal{H}_{AB}\right)$, the entanglement of formation is defined as

$$E^{\mathrm{F}}\left(A;B\right) \equiv \min_{\left\{p_X(x),\,|\psi^x\rangle_{AB}\right\}} \left\{ \sum_x p_X\left(x\right) E\left(A;B\right)_{\psi^x} : \rho_{AB} = \sum_x p_X\left(x\right) \left|\psi^x\right\rangle \left\langle\psi^x\right|_{AB} \right\} \tag{3.2.33}$$

$$= \min_{\left\{p_X(x),\,|\psi^x\rangle_{AB}\right\}} \left\{ H\left(A\left|X\right.\right)_\sigma : \sigma_{ABX} = \sum_x p_X\left(x\right) \left|x\right\rangle\left\langle x\right|_X \otimes \left|\psi^x\right\rangle\left\langle\psi^x\right|_{AB} \right\}, \tag{3.2.34}$$

where the state ρ_{AB} has been decomposed into a mixture of pure states, and the state σ_{ABX} is a classical-quantum state constructed based on the decomposition.

Likewise, a Rényi entropy of entanglement and entanglement of formation can be defined with the Rényi entropies in place of the von Neumann entropies. We now formally define these quantities.

Definition 3.11. *The Rényi entropy of entanglement of a bipartite pure state* $\psi_{AB} \in S(\mathcal{H}_{AB})$ *is defined for* $\alpha \in (0,1) \cup (1,\infty)$ *as* $H_\alpha(A)_\psi$. *Further, the Rényi entanglement of formation of a bipartite state* $\rho_{AB} \in S(\mathcal{H}_{AB})$ *is defined for* $\alpha \in (0,1) \cup (1,\infty)$ *as*

$$E_\alpha^{\mathrm{F}}(A;B)_\rho \equiv \inf_{\{p_X(x), |\psi^x\rangle_{AB}\}} \left\{ H_\alpha(A|X)_\sigma : \sigma_{ABX} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes |\psi^x\rangle\langle\psi^x|_{AB} \right\}, \tag{3.2.35}$$

where $H_\alpha(A|X)_\sigma$ *is the Rényi conditional entropy of* (2.2.47), σ_{ABX} *is the classical extension of* ρ_{AB} *based on its decomposition into a mixture of pure states.*

Proposition 3.12. *For a pure state* $\psi_{AB} \in S(\mathcal{H}_{AB})$ *and for* $\alpha \in (0,1) \cup (1,2]$ *, the Rényi squashed entanglement is related to the Rényi entropy of entanglement as*

$$E_\alpha^{\mathrm{sq}}(A;B)_\psi = H_{(2-\alpha)/\alpha}(A)_\psi .$$

Proof. Consider that any extension of a pure state ψ_{AB} is of the form $\psi_{AB} \otimes \omega_E$. So applying Lemma D.7, we find that

$$I_\alpha(A;B|E)_{\psi\otimes\omega} = I_\alpha(A;B)_\psi . \tag{3.2.36}$$

The Rényi mutual information of a pure state can then be evaluated as

$$I_\alpha(A;B)_\psi = \frac{\alpha}{\alpha-1} \log \mathrm{Tr}\left\{ \left(\mathrm{Tr}_A\left\{ \psi_A^{1-\alpha} \psi_{AB}^\alpha \right\} \right)^{1/\alpha} \right\} \tag{3.2.37}$$

$$= \frac{\alpha}{\alpha-1} \log \mathrm{Tr}\left\{ \left(\mathrm{Tr}_A\left\{ \psi_A^{1-\alpha} \psi_{AB} \right\} \right)^{1/\alpha} \right\} \tag{3.2.38}$$

$$= \frac{\alpha}{\alpha-1} \log \mathrm{Tr}\left\{ \left(\mathrm{Tr}_A\left\{ \psi_B^{1-\alpha} \psi_{AB} \right\} \right)^{1/\alpha} \right\} \tag{3.2.39}$$

$$= \frac{\alpha}{\alpha-1} \log \mathrm{Tr}\left\{ \left(\psi_B^{1-\alpha} \psi_B \right)^{1/\alpha} \right\} \tag{3.2.40}$$

$$= \frac{\alpha}{\alpha-1} \log \mathrm{Tr}\left\{ \psi_B^{(2-\alpha)/\alpha} \right\} \tag{3.2.41}$$

$$= 2\frac{1}{1-(2-\alpha)/\alpha} \log \mathrm{Tr}\left\{ \psi_B^{(2-\alpha)/\alpha} \right\} \tag{3.2.42}$$

$$= 2H_{(2-\alpha)/\alpha}(B)_\psi \tag{3.2.43}$$

$$= 2H_{(2-\alpha)/\alpha}(A)_\psi . \tag{3.2.44}$$

The first equality follows from (2.2.50). The second equality follows because $\psi_{AB}^\alpha = \psi_{AB}$ for a pure state ψ. The third equality follows because $\psi_A^{1-\alpha}|\psi\rangle_{AB} = \psi_B^{1-\alpha}|\psi\rangle_{AB}$ for a pure bipartite state ψ. The fourth equality follows by taking the partial trace over system A. The rest of the equalities are straightforward, by applying the definition of the Rényi entropy. ■

Corollary 3.13. *The Rényi squashed entanglement is normalized on maximally entangled states, in the sense that for* $\alpha \in (0,1) \cup (1,2]$

$$E_\alpha^{\mathrm{sq}}(A;B)_\Psi = \log d, \tag{3.2.45}$$

where d *is the Schmidt rank of the maximally entangled state* Ψ_{AB}.

Proof. This follows from Proposition 3.12 and from the fact that the Rényi entropy of a maximally mixed state of dimension d is equal to $\log d$. ■

Proposition 3.14. *The Rényi entanglement of formation of $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ can be written as*

$$E_\alpha^{\mathrm{F}}(A;B)_\rho = \min_{\{p_X(x),|\psi^x\rangle_{AB}\}} \left\{ \frac{\alpha}{1-\alpha} \log \sum_x p_X(x) \left[\mathrm{Tr}\{(\psi_A^x)^\alpha\}^{1/\alpha} \right] : \rho_{AB} = \sum_x p_X(x) |\psi^x\rangle\langle\psi^x|_{AB} \right\}. \tag{3.2.46}$$

Proof. By applying the Sibson identity mentioned in [169] to $H_\alpha(A|X)_\sigma$ in (3.2.35), we find that

$$H_\alpha(A|X)_\sigma = \frac{\alpha}{1-\alpha} \log \mathrm{Tr}\left\{ (\mathrm{Tr}_A\{\sigma_{AX}^\alpha\})^{1/\alpha} \right\} \tag{3.2.47}$$

$$= \frac{\alpha}{1-\alpha} \log \mathrm{Tr}\left\{ \left(\mathrm{Tr}_A \left\{ \sum_x p_X^\alpha(x) |x\rangle\langle x|_X \otimes (\psi_A^x)^\alpha \right\} \right)^{1/\alpha} \right\} \tag{3.2.48}$$

$$= \frac{\alpha}{1-\alpha} \log \mathrm{Tr}\left\{ \left(\left\{ \sum_x p_X^\alpha(x) |x\rangle\langle x|_X \mathrm{Tr}\{(\psi_A^x)^\alpha\} \right\} \right)^{1/\alpha} \right\} \tag{3.2.49}$$

$$= \frac{\alpha}{1-\alpha} \log \sum_x p_X(x) \left[\mathrm{Tr}\{(\psi_A^x)^\alpha\}^{1/\alpha} \right]. \tag{3.2.50}$$

Finally, by an application of the Carathodory theorem, we know that the infimum can be replaced by a minimum because $2^{\frac{1-\alpha}{\alpha} H_\alpha(A|X)_\sigma}$ can be written as a convex combination of $\mathrm{Tr}\{(\psi_A^x)^\alpha\}^{1/\alpha}$, which is a continuous function of the marginals of the elements of a convex decomposition of the state ρ_{AB} and these marginals are elements of a compact set. ■

Proposition 3.15. *For $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$, the Rényi squashed entanglement is upper bounded by the Rényi entanglement of formation for $\alpha \in (0,1) \cup (1,2)$ as*

$$E_{(2-\alpha)/\alpha}^{\mathrm{F}}(A;B)_\rho \geq E_\alpha^{\mathrm{sq}}(A;B)_\rho. \tag{3.2.51}$$

Proof. Consider a spectral decomposition of ρ_{AB} in terms of an ensemble$\{p_X(x), |\psi^x\rangle_{AB}\}$

$$\rho_{AB} = \sum_x p_X(x) |\psi^x\rangle\langle\psi^x|_{AB}. \tag{3.2.52}$$

Let σ_{XAB} be a classical extension of ρ_{AB}, given by

$$\sigma_{XAB} = \sum_x p_X(x) |x\rangle\langle x|_X \otimes |\psi^x\rangle\langle\psi^x|_{AB}. \tag{3.2.53}$$

Consider that

$$H_\beta(A|X) = \frac{\beta}{1-\beta} \log \sum_x p_X(x) \left[\mathrm{Tr}\left\{ (\psi_A^x)^\beta \right\}^{1/\beta} \right] \tag{3.2.54}$$

$$= \frac{1}{1-\beta} \log \left[\sum_x p_X(x) \left[\mathrm{Tr}\left\{ (\psi_A^x)^\beta \right\}^{1/\beta} \right] \right]^\beta. \tag{3.2.55}$$

For $\beta \in (0,1) \cup (1,\infty)$, we have from concavity / convexity of the function x^β that

$$H_\beta(A|X) \geq \frac{1}{1-\beta} \log \sum_x p_X(x) \operatorname{Tr}\left\{ (\psi_A^x)^\beta \right\}. \tag{3.2.56}$$

Let $\beta = (2-\alpha)/\alpha$. Then, from (3.2.56), for $\alpha \in (0,1) \cup (1,2)$, we have that

$$H_{(2-\alpha)/\alpha}(A|X) \geq \frac{1}{1-(2-\alpha)/\alpha} \log \sum_x p_X(x) \operatorname{Tr}\left\{ (\psi_A^x)^{(2-\alpha)/\alpha} \right\}. \tag{3.2.57}$$

Now consider that

$$\frac{1}{2} I_\alpha(A;B|X)_\sigma = \frac{1}{2}\frac{\alpha}{\alpha-1} \log \sum_x p_X(x) \exp^{\left(\frac{\alpha-1}{\alpha}\right) I_\alpha(A;B)_{\psi^x}} \tag{3.2.58}$$

$$= \frac{1}{2}\frac{\alpha}{\alpha-1} \log \sum_x p_X(x) \exp^{\left(\frac{\alpha-1}{\alpha}\right)\frac{\alpha}{\alpha-1} \log \operatorname{Tr}\left\{ (\psi_A^x)^{(2-\alpha)/\alpha} \right\}} \tag{3.2.59}$$

$$= \frac{1}{2}\frac{\alpha}{\alpha-1} \log \sum_x p_X(x) \operatorname{Tr}\left\{ (\psi_A^x)^{(2-\alpha)/\alpha} \right\} \tag{3.2.60}$$

$$= \frac{1}{1-(2-\alpha)/\alpha} \log \sum_x p_X(x) \operatorname{Tr}\left\{ (\psi_A^x)^{(2-\alpha)/\alpha} \right\}. \tag{3.2.61}$$

The first equality follows by applying Lemma D.6. The second equality follows from some steps given in the proof of Proposition 3.12. The last two equalities are straightforward.

From (3.2.57) and (3.2.61), we have that

$$H_{(2-\alpha)/\alpha}(A|X) \geq \frac{1}{2} I_\alpha(A;B|X). \tag{3.2.62}$$

The statement of the proposition follows from (3.2.62), because

$$\frac{1}{2} I_\alpha(A;B|X) \geq E_\alpha^{\mathrm{sq}}(A;B)_\rho, \tag{3.2.63}$$

which in turn follows because the state in (3.2.53) is a particular extension of the state ρ_{AB} and by definition, the Rényi squashed entanglement is equal to the infimum over all such extensions. So putting together (3.2.62) and (3.2.63) gives the statement of the proposition. ■

We end this section with Table 3.1, which summarizes the properties of the Rényi squashed entanglement and draws a comparison with those of the von Neumann entropy based squashed entanglement.

3.3 Rényi Quantum Discord

Quantum discord: A brief review. The quantum discord of a bipartite state ρ_{AB} is defined as the gap between the quantum mutual information $I(A;B)_\rho \equiv H(A)_\rho + H(B)_\rho - H(AB)_\rho$ and the mutual information after one of the systems A or B has been measured,

Table 3.1: Properties of the Rényi squashed entanglement in comparison to those of the original von Neumann entropy based squashed entanglement. question marks indicate properties that remain open for the Rényi squashed entanglement of Definition 3.2. Two of the properties for the Rényi squashed entanglement rely on conjectures. Conj. 3.3 is the statement that the Rényi conditional quantum mutual information obeys monotonicity under quantum operations on system A, i.e., for $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_{ABE})$ and $\alpha \in (0,1) \cup (1,2]$, $I_\alpha(A;B|E)_\rho \geq I_\alpha(A';B|E)_\tau$, where $\tau_{A'BE} \equiv \mathcal{M}_{A\to A'}(\rho_{ABE})$ and $\mathcal{M}_{A\to A'}$ is a CPTP map acting on system A alone. Conjecture B.25 is the statement that the Rényi conditional quantum mutual information is monotone non-decreasing in the Rényi parameter, i.e., $I_\alpha(A;B|C) \leq I_\beta(A;B|C)$ for $0 \leq \alpha \leq \beta$.

Property	Squashed Ent. of (3.2.1)	Rényi Squashed Ent. of (3.2.3)
Normalized	✓	✓ for $\alpha \in (0,1) \cup (1,2]$
LOCC Monotonicity	✓	if Conj. 3.3 true, then true for $\alpha \in (0,1) \cup (1,2]$
Convexity	✓	✓ for $\alpha \in (0,1)$
Faithfulness	✓	vanishing on sep. states for $\alpha \in (0,1) \cup (1,\infty)$; if Conj. B.25 true, then true for $\alpha \in (1,\infty)$
Additivity	✓	subadditive for $\alpha \in (0,1) \cup (1,\infty)$
Monogamy	✓	?
Non-lockability	✓	?
Asymptotic Continuity	✓	?

where the latter is maximized over all measurements [136, 207]. That is, if the measurement occurs on system A, then the quantum discord is defined as

$$D(\overline{A};B)_\rho \equiv I\left(A;B\right)_\rho - \max_{\{\Lambda^x\}} I(X;B)_\omega, \tag{3.3.1}$$

with the overbar denoting the system being measured, and

$$\omega_{XB} \equiv \sum_x |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\{(\Lambda_A^x \otimes I_B)\rho_{AB}\}, \tag{3.3.2}$$

$\Lambda^x \geq 0\;\forall x$, and $\sum_x \Lambda^x = I$. (It is well known to be sufficient to optimize the quantum discord over rank-one POVMs [129].) The quantum discord characterizes quantum correlations that are different from those due to entanglement. It is non-negative, invariant under local unitary operations, and equal to zero if and only if the state is classical on the system being measured.

We think that it is an important conceptual realization that the quantum discord can be re-expressed in terms of the QCMI [145]. To see how this comes about, consider the following. Let $\mathcal{M}_{A\to X}$ denote the following measurement map on a state σ_A:

$$\mathcal{M}_{A\to X}\left(\sigma_A\right) \equiv \sum_x \mathrm{Tr}\left\{\Lambda_A^x \sigma_A\right\} |x\rangle\left\langle x\right|_X . \tag{3.3.3}$$

Using this, we can write (3.3.2) as $\omega_{XB} = \mathcal{M}_{A\to X}\left(\rho_{AB}\right)$. Now, to every measurement map $\mathcal{M}_{A\to X}$, we can find an isometric extension of it, having the following form:

$$U_{A\to XE}^{\mathcal{M}} \left|\psi\right\rangle_A \equiv \sum_x \left|x\right\rangle_X \left|x,y\right\rangle_E \left\langle \varphi_{x,y}\right|_A \left|\psi\right\rangle_A , \tag{3.3.4}$$

where the vectors $\left\{\left|\varphi_{x,y}\right\rangle_A\right\}$ are part of a rank-one refinement of the POVM $\{\Lambda_A^x\}$:

$$\Lambda_A^x = \sum_y \left|\varphi_{x,y}\right\rangle\left\langle \varphi_{x,y}\right| . \tag{3.3.5}$$

Thus,

$$\mathcal{M}_{A\to X}\left(\sigma_A\right) = \mathrm{Tr}_E\left\{\mathcal{U}_{A\to XE}^{\mathcal{M}}\left(\sigma_A\right)\right\}, \tag{3.3.6}$$

where

$$\mathcal{U}_{A\to XE}^{\mathcal{M}}\left(\sigma_A\right) \equiv U_{A\to XE}^{\mathcal{M}}\left(\sigma_A\right)\left(U_{A\to XE}^{\mathcal{M}}\right)^\dagger . \tag{3.3.7}$$

Figure 3.1 illustrates this equivalence between the action of a measurement map and its isometric extension.

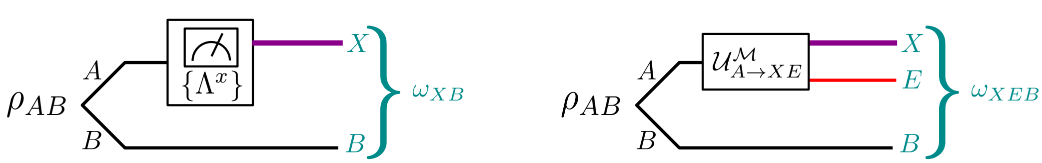

Figure 3.1: A measurement map $\mathcal{M}$ described by $\{\Lambda^x\}$, and its isometric extension $\mathcal{U}^{\mathcal{M}}$.

Let ω_{XEB} denote the following state:

$$\omega_{XEB} = \mathcal{U}_{A\to XE}^{\mathcal{M}}\left(\rho_{AB}\right). \tag{3.3.8}$$

We can use the above development to rewrite the objective function of the quantum discord in (3.3.1) as follows:

$$I(A;B)_\rho - I(X;B)_\omega = I(XE;B)_\omega - I(X;B)_\omega \tag{3.3.9}$$
$$= I(E;B|X)_\omega . \tag{3.3.10}$$

Thus, the quantum discord can be defined in terms of the QCMI as follows.

Definition 3.16. *The quantum discord of a state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$is defined as*

$$D\left(\overline{A};B\right)_\rho \equiv \min_{\{\Lambda_x\}} I(E;B|X)_\omega , \tag{3.3.11}$$

where the optimization is over all possible POVMs acting on system A, with X being the classical output and E being an environment for the measurement map, so that

$$\omega_{XEB} \equiv U_{A\to XE}\rho_{AB}U^\dagger_{A\to XE}, \tag{3.3.12}$$
$$U_{A\to XE}|\psi\rangle_A \equiv \sum_x |x\rangle_X \otimes \left(\sqrt{\Lambda^x}|\psi\rangle_A \otimes |x\rangle\right)_E . \tag{3.3.13}$$

Here $U_{A\to XE}(\cdot)\,U^\dagger_{A\to XE}$ is an isometric extension of a generalized rank-one POVM-based measurement map $\mathcal{M}_{A\to X}(\cdot) = \sum_x Tr\{\Lambda_x \cdot\}\,|x\rangle\langle x|_X$ acting on system A. Thus, the quantum discord captures how much correlations are lost to the environment in the act of a quantum measurement. This interpretation is made concrete in [197, Section 6.3].

A Rényi quantum discord. Similarly to Definition 3.16, a Rényi quantum discord can be defined with a Rényi QCMI in place of the QCMI. We now formally define the quantity.

Definition 3.17. *The Rényi quantum discord of a state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ is defined for $\alpha \in (0,1)\cup(1,2]$ as*

$$D\left(\bar{A};B\right)_\rho \equiv \inf_{\{\Lambda_x\}} I_\alpha(E;B|X)_\rho , \tag{3.3.14}$$

where $\rho_{EXB} = \mathcal{U}_{A\to EX}(\rho_{AB})$, $\mathcal{U}_{A\to EX}(\cdot) \equiv U_{A\to EX}(\cdot)\,U^\dagger_{A\to EX}$ is an isometric extension map of a generalized rank-one POVM-based measurement map $\mathcal{M}_{A\to X}(\cdot) = \sum_x Tr\{\Lambda_x \cdot\}\,|x\rangle\langle x|_X$ acting on system A.

3.3.1 Properties

We now prove that the Rényi quantum discord for $\alpha \in (0,1)\cup(1,2]$ is non-negative, invariant under local unitaries, vanishes on the set of classical-quantum states, and is optimized by a rank-one POVM.

Proposition 3.18. *The Rényi quantum discord $D^\alpha(\overline{A};B)_\rho$ is non-negative for $\alpha \in (0,1)\cup(1,2]$.*

Proof. This follows easily from the fact that the Rényi conditional mutual information is non-negative for $\alpha \in (0,1)\cup(1,2]$ [18, Corollary 16]. ■

Proposition 3.19. *For a classical-quantum state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ the Rényi quantum discord is equal to zero for $\alpha \in (0,1)\cup(1,\infty)$.*

Proof. Consider a classical-quantum state ρ_{AB}:

$$\rho_{AB} = \sum_x p_X(x) |x\rangle \langle x|_A \otimes \rho_B^x. \tag{3.3.15}$$

Let the dilation of a von Neumann measurement of system A be $|x\rangle_A \rightarrow |x\rangle_X |x\rangle_E$, so that it produces

$$\rho_{XEB} \equiv \sum_x p(x) |x\rangle \langle x|_X \otimes |x\rangle \langle x|_E \otimes \rho_B^x. \tag{3.3.16}$$

So the conditioning system X is classical. Applying Lemma D.6, we find that

$$I_\alpha(E;B|X) = \frac{\alpha}{\alpha-1} \log \sum_x p_X(x) \exp^{\left(\frac{\alpha-1}{\alpha}\right) I_\alpha(E;B)_{|x\rangle\langle x| \otimes \rho^x}} = \frac{\alpha}{\alpha-1} \log \sum_x p_X(x) = 0. \tag{3.3.17}$$

Combining this with the previous proposition, we see that it is equal to zero for classical-quantum states. ■

Proposition 3.20. *The Rényi quantum discord $D^\alpha(\overline{A};B)_\rho$ is invariant under local unitaries for $\alpha \in (0,1) \cup (1,\infty)$.*

Proof. First, from the definition of $I_\alpha(A;B|E)$, we can see that this quantity is invariant under local unitaries. It then immediately follows that the Rényi discord is invariant under local unitaries $U_A \otimes V_B$. That is, if the optimal measurement is given by $\{\Lambda_A^x\}$, then the optimal measurement under a local unitary U_A can be taken as $\left\{U_A^\dagger \Lambda_A^x U_A\right\}$. ■

Proposition 3.21. *The infimum in the definition of Rényi quantum discord (Definition 3.17) is optimized by a rank-one POVM for $\alpha \in (0,1) \cup (1,2]$.*

Proof. Consider an arbitrary measurement map

$$\mathcal{M}(\sigma) \equiv \sum_x \text{Tr}\{\Lambda_x \sigma\} |x\rangle \langle x|_X, \tag{3.3.18}$$

and a spectral decomposition of each Λ_x:

$$\Lambda_x = \sum_y \mu_y |\phi_{x,y}\rangle \langle \phi_{x,y}|. \tag{3.3.19}$$

For a fixed x, the set $\{|\phi_{x,y}\rangle\}_y$ is orthonormal. Furthermore, the set $\{\mu_y |\phi_{x,y}\rangle \langle \phi_{x,y}|\}_{x,y}$ forms a POVM (a rank-one refinement of the original POVM). We can then rewrite the measurement map as

$$\mathcal{M}(\sigma) = \sum_{x,y} \text{Tr}\{\mu_y |\phi_{x,y}\rangle \langle \phi_{x,y}| \sigma\} |x\rangle \langle x|_X. \tag{3.3.20}$$

In this way, we can already see that there is some loss of information when discarding the outcome y. An isometric extension of the original measurement map is specified by

$$U^{\mathcal{M}}_{A \rightarrow E X_E Y X} |\psi\rangle_A \equiv \sum_{x,y} \sqrt{\mu_y} \left(|\phi_{x,y}\rangle_E \langle \phi_{x,y}|_A\right) |\psi\rangle_A \otimes |x\rangle_{X_E} |y\rangle_Y \otimes |x\rangle_X. \tag{3.3.21}$$

This is because the original map is recovered by tracing over the environmental systems EX_EY:

$$\begin{aligned}
&\operatorname{Tr}_{EX_EY}\left\{U^{\mathcal{M}}_{A\to EX_EYX}\sigma\left(U^{\mathcal{M}}_{A\to EX_EYX}\right)^\dagger\right\}\\
&=\operatorname{Tr}_{EX_EY}\Bigg\{\sum_{x,y,x',y'}\sqrt{\mu_y}\sqrt{\mu_{y'}}\left(\left|\phi_{x,y}\right\rangle_E\left\langle\phi_{x,y}\right|_A\right)\sigma\left|\phi_{x',y'}\right\rangle_A\left\langle\phi_{x',y'}\right|_E\otimes|x\rangle\langle x'|_{X_E}\otimes|y\rangle\langle y'|_Y\\
&\otimes|x\rangle\langle x'|_X\Bigg\} \qquad (3.3.22)\\
&=\sum_{x,y}\mu_y\left(\left\langle\phi_{x,y}\right|_E\left|\phi_{x,y}\right\rangle_E\left\langle\phi_{x,y}\right|_A\right)\sigma\left|\phi_{x,y}\right\rangle_A\otimes|x\rangle\langle x|_X \qquad (3.3.23)\\
&=\sum_{x,y}\operatorname{Tr}\left\{\mu_y\left|\phi_{x,y}\right\rangle\left\langle\phi_{x,y}\right|\sigma\right\}|x\rangle\langle x|_X \qquad (3.3.24)\\
&=\mathcal{M}\left(\sigma\right). \qquad (3.3.25)
\end{aligned}$$

Let ψ^ρ_{RAB} be a purification of the state ρ_{AB} on which we are evaluating the Rényi discord. Then let ω_{REX_EYXB} be the following pure state:

$$\omega_{REX_EYXB}\equiv U^{\mathcal{M}}_{A\to EX_EYX}\psi^\rho_{RAB}\left(U^{\mathcal{M}}_{A\to EX_EYX}\right)^\dagger. \qquad (3.3.26)$$

Consider the following chain of inequalities:

$$I_\alpha\left(EX_EY;B|X\right)_\omega=I_\alpha\left(B;EX_EY|R\right)_\omega\geq I_\alpha\left(B;EX_E|R\right)_\omega=I_\alpha\left(EX_E;B|XY\right)_\omega. \qquad (3.3.27)$$

The first equality is by duality of the Rényi QCMI. The second inequality is from monotonicity under local quantum operation. The last equality is again from duality. But now consider that the last quantity corresponds to the quantum discord for the following refined rank-one measurement map:

$$\sigma\to\sum_{x,y}\operatorname{Tr}\left\{\mu_y\left|\phi_{x,y}\right\rangle\left\langle\phi_{x,y}\right|\sigma\right\}|x\rangle\langle x|_X\otimes|y\rangle\langle y|_Y. \qquad (3.3.28)$$

Furthermore, the systems EX_E above play the role of the environment of the refined rank-one measurement map from A to X and Y. This is because

$$\begin{aligned}
&\operatorname{Tr}_{EX_E}\left\{U^{\mathcal{M}}_{A\to EX_EYX}\sigma\left(U^{\mathcal{M}}_{A\to EX_EYX}\right)^\dagger\right\}\\
&=\operatorname{Tr}_{EX_E}\Bigg\{\sum_{x,y,x',y'}\sqrt{\mu_y}\sqrt{\mu_{y'}}\left(\left|\phi_{x,y}\right\rangle_E\left\langle\phi_{x,y}\right|_A\right)\sigma\left|\phi_{x',y'}\right\rangle_A\left\langle\phi_{x',y'}\right|_E\otimes|x\rangle\langle x'|_{X_E}\\
&\otimes|y\rangle\langle y'|_Y\otimes|x\rangle\langle x'|_X\Bigg\} \qquad (3.3.29)\\
&=\sum_{x,y,y'}\mu_y\left(\left\langle\phi_{x,y'}\right|_E\left|\phi_{x,y}\right\rangle_E\left\langle\phi_{x,y}\right|_A\right)\sigma\left|\phi_{x,y'}\right\rangle_A\otimes|y\rangle\langle y'|_Y\otimes|x\rangle\langle x|_X \qquad (3.3.30)\\
&=\sum_{x,y,y'}\mu_y\left\langle\phi_{x,y}\right|_A\sigma\left|\phi_{x,y}\right\rangle_A\otimes|y\rangle\langle y|_Y\otimes|x\rangle\langle x|_X \qquad (3.3.31)\\
&=\sum_{x,y}\operatorname{Tr}\left\{\mu_y\left|\phi_{x,y}\right\rangle\left\langle\phi_{x,y}\right|\sigma\right\}|x\rangle\langle x|_X\otimes|y\rangle\langle y|_Y. \qquad (3.3.32)
\end{aligned}$$

Since a rank-one POVM always achieves a lower value of the Rényi quantum discord, it suffices to optimize over only these kinds of POVMs when calculating it. ■

A different Rényi quantum discord. At this point we would like to note that a different Rényi generalization of the quantum discord $\mathcal{D}^\alpha(\overline{A}; B)_\rho$, proposed in [128], is optimized by a rank-one POVM as well. This quantity was defined based upon an optimization over rank-one projective measurements, but can be extended to an optimization over all POVMs. Consider the definition for the Rényi discord of a bipartite state ρ_{AB} proposed in [128, Eq. (26)] (with projective measurements replaced by POVMs $\{\Lambda^x\}$):

$$\mathfrak{D}^\alpha(\overline{A}; B)_\rho \equiv \min_{\sigma_A, \sigma_B} D_\alpha(\rho_{AB} \| \sigma_A \otimes \sigma_B) - \max_{\{\Lambda^x\}} \min_{\sigma_X, \sigma_B} D_\alpha(\rho_{XB} \| \sigma_X \otimes \sigma_B). \tag{3.3.33}$$

The sufficiency of rank-one POVMs $\{\Lambda^x\}$ in the above definition can be proven along the following lines. Similar to the proof of Proposition 3.21, consider a spectral decomposition of the POVM elements $\{\Lambda^x\}$:

$$\Lambda_x = \sum_y \mu_{xy} |\phi_{x,y}\rangle \langle \phi_{x,y}| . \tag{3.3.34}$$

Once again, for a fixed x, the set $\{|\phi_{x,y}\rangle\}_y$ is orthonormal, and the set $\{\mu_{xy} |\phi_{x,y}\rangle \langle \phi_{x,y}|\}_{x,y}$ forms a rank-one refinement of the original POVM. The output state corresponding to the measurement consisting of these above rank-one refinements can be written as

$$\rho_{XYB} = \sum_{x,y} |x\rangle \langle x|_X \otimes |y\rangle \langle y|_Y \otimes \mu_{xy} \langle \phi_{x,y}|_A \rho_{AB} |\phi_{x,y}\rangle_A . \tag{3.3.35}$$

Due to the monotonicity of the Rényi relative entropy under local quantum operations, we have that

$$\min_{\sigma_{XY}, \sigma_B} D_\alpha(\rho_{XYB} \| \sigma_{XY} \otimes \sigma_B) \geq \min_{\sigma_X, \sigma_B} D_\alpha(\rho_{XB} \| \sigma_X \otimes \sigma_B). \tag{3.3.36}$$

This implies

$$\max_{\{\mu_y |\phi_{x,y}\rangle \langle \phi_{x,y}|\}_{x,y}} \min_{\sigma_{XY}, \sigma_B} D_\alpha(\rho_{XYB} \| \sigma_{XY} \otimes \sigma_B) \geq \max_{\{\mu_y |\phi_{x,y}\rangle \langle \phi_{x,y}|\}_{x,y}} \min_{\sigma_X, \sigma_B} D_\alpha(\rho_{XB} \| \sigma_X \otimes \sigma_B). \tag{3.3.37}$$

Hence, the second term in (3.3.33) can be replaced with

$$\max_{\{\mu_y |\phi_{x,y}\rangle \langle \phi_{x,y}|\}_{x,y}} \min_{\sigma_{XY}, \sigma_B} D_\alpha(\rho_{XYB} \| \sigma_{XY} \otimes \sigma_B). \tag{3.3.38}$$

Therefore, it suffices to optimize the Rényi quantum discord defined in [128, Eq. (26)] over only rank-one POVMs.

We summarize the above discussed properties in the Table 3.2.

Table 3.2: Properties of the Rényi quantum discord of (3.3.11) in comparison to those of the original von Neumann entropy based quantum discord and the Rényi quantum discord proposed in [128, Eq. (26)]. In the first column, cq-states refers to classical-quantum states. The property of monotonicity in α for the Rényi quantum discord of (3.3.14) relies on Conjecture B.25, which is the statement that the Rényi QCMI is monotone non-decreasing in the Rényi parameter, i.e., $I_\alpha(A;B|C) \leq I_\beta(A;B|C)$ for $0 \leq \alpha \leq \beta$. Rényi discord of [128] is not monotone in α because it is equal to a difference of two Rényi relative entropies.

Property	Discord of (3.3.11)	Rényi Discord of (3.3.14)	Rényi Discord of (3.3.33) as in [128]
Non-negative	✓	✓ for $\alpha \in (0,1) \cup (1,2]$	✓ for $\alpha \in [1/2,1) \cup (1,\infty)$
Vanishing on cq-states	✓	✓ for $\alpha \in (0,1) \cup (1,\infty)$	✓ for $\alpha \in (0,1) \cup (1,\infty)$
Unitary invariance	✓	✓ for $\alpha \in (0,1) \cup (1,\infty)$	✓ for $\alpha \in (0,1) \cup (1,\infty)$
Rank-1 POVM optimal	✓	✓ for $\alpha \in (0,1) \cup (1,2]$	✓ for $\alpha \in [1/2,1) \cup (1,\infty)$
Monotone in α	N/A	if [18, Conj. 34] true, then true	x

3.3.2 Rényi quantum discord for pure bipartite states

We now give an expression for the Rényi discord of pure bipartite states.

Proposition 3.22. *The Rényi quantum discord of a pure bipartite state $\psi_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ for $\alpha \in (0,1) \cup (1,2]$ is given by*

$$D^\alpha \left(\overline{A};B\right)_\psi = \inf_{\{|\varphi_x\rangle : \sum_x |\varphi_x\rangle\langle\varphi_x| = I\}} \frac{\alpha}{\alpha-1} \log \sum_x p\left(x\right) \langle \xi_x|_B \, \psi_B^{1-\alpha} \, |\xi_x\rangle^{1/\alpha}, \tag{3.3.39}$$

where

$$|\xi_x\rangle_B = \frac{\langle\varphi_x|_A|\psi\rangle_{AB}}{\sqrt{p(x)}}, \quad p(x) = \|\langle\varphi_x|_A|\psi\rangle_{AB}\|_2^2, \tag{3.3.40}$$

and $\{|\varphi_x\rangle : \sum_x |\varphi_x\rangle\langle\varphi_x| = I\}$ denotes a rank-one POVM acting on system A.

Proof. We begin by recalling Proposition 3.21, i.e., that it suffices to optimize the Rényi quantum discord over rank-one POVMs. Let $\{|\varphi_x\rangle\langle\varphi_x|_A\}_x$ denote such a POVM, so that $\sum_x |\varphi_x\rangle\langle\varphi_x|_A = I_A$. Consider a bipartite pure state

$$|\psi\rangle_{AB} = \sum_{y=0}^{d-1} \sqrt{\lambda(y)} \left|\tilde{\psi}_y\right\rangle_A |\psi_y\rangle_B , \tag{3.3.41}$$

where $\left|\tilde{\psi}_y\right\rangle$ and $|\psi_y\rangle$ are orthonormal bases in $\mathcal{H}_A$ and $\mathcal{H}_B$. The post measurement tripartite state is given by

$$\omega_{BEX} \equiv U_{A\to EX}\psi_{AB}U_{A\to EX}^\dagger, \tag{3.3.42}$$

where $U_{A\to EX}$ an isometric extension of the aforementioned rank-one measurement:

$$U_{A\to EX} \equiv \sum_x |x\rangle_E |x\rangle_X \langle\varphi_x|_A . \tag{3.3.43}$$

The above state, and the reduced states on systems BE and B can thus be equivalently written as

$$\omega_{BEX} \equiv \sum_{x,y} \sqrt{p(x)\, p(y)}\, |x\rangle\langle y|_X \otimes |x\rangle\langle y|_E \otimes |\xi_x\rangle\langle\xi_y|_B , \tag{3.3.44}$$

$$\omega_{BE} \equiv \sum_x p(x)\, |x\rangle\langle x|_E \otimes |\xi_x\rangle\langle\xi_x|_B , \tag{3.3.45}$$

where $p(x) = \operatorname{Tr}\{|\varphi_x\rangle\langle\varphi_x|_A|\psi\rangle\langle\psi|_{AB}\}$ and $|\xi_x\rangle\langle\xi_x|_B = \operatorname{Tr}_A\{|\varphi_x\rangle\langle\varphi_x|_A|\psi\rangle\langle\psi|_{AB}\}/p(x)$. The Rényi conditional quantum mutual information of ω_{BEX} is thereby given by

$$\begin{aligned}
I_\alpha(E;B|X)_\omega &= I_\alpha(B;E)_\omega && (3.3.46)\\
&= \frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\operatorname{Tr}_B\left\{\omega_{BE}^{\alpha}\omega_B^{1-\alpha}\right\}^{1/\alpha}\right\} && (3.3.47)\\
&= \frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\operatorname{Tr}_B\left\{\left(\sum_x p(x)^\alpha |x\rangle\langle x|_E \otimes |\xi_x\rangle\langle\xi_x|_B\right)\omega_B^{1-\alpha}\right\}^{1/\alpha}\right\} && (3.3.48)\\
&= \frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\sum_x p(x)\, |x\rangle\langle x|_E \operatorname{Tr}_B\left\{|\xi_x\rangle\langle\xi_x|_B\,\omega_B^{1-\alpha}\right\}^{1/\alpha}\right\} && (3.3.49)\\
&= \frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\sum_x p(x) \operatorname{Tr}_B\left\{|\xi_x\rangle\langle\xi_x|_B\,\omega_B^{1-\alpha}\right\}^{1/\alpha}\right\} && (3.3.50)\\
&= \frac{\alpha}{\alpha-1}\log\sum_x p(x)\,\langle\xi_x|_B\,\omega_B^{1-\alpha}\,|\xi_x\rangle^{1/\alpha} . && (3.3.51)
\end{aligned}$$

The first equality follows from application of duality of Rényi QCMI along with the fact that ω_{BEX} is a pure state. The second and third equalities follow from the definition of Rényi QCMI, the fact that the system E is classical, and the fact that the post-measurement states on system B are pure whenever a rank-one POVM is performed on system A. The fourth one follows from tracing over the E system. The fifth and sixth equalities are straightforward. ■

Corollary 3.23. *The Rényi quantum discord of a maximally entangled state $\Phi_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ simplifies to*

$$D^\alpha\left(\overline{A};B\right)_\Phi = \log|A|. \tag{3.3.52}$$

Proof. For a maximally entangled state, $p(x)$ in (3.3.44) is equal to $1/|A|$, and the reduced state on system B is maximally mixed. The result then follows from (3.3.51). ■

3.3.3 Conjectured remainder terms for quantum discord

Conjecture B.25 predicts that a Rényi QCMI defined based upon the sandwiched Rényi relative entropy of (B.4.24) is also monotone in the Rényi parameter. That is, for a positive definite tripartite state ρ_{ABC} and $0 \leq \alpha \leq \beta$, it was conjectured that

$$\widetilde{I}_{\alpha}\left(A;B|C\right)_{\rho} \leq \widetilde{I}_{\beta}\left(A;B|C\right)_{\rho}, \tag{3.3.53}$$

where the "sandwiched" Rényi conditional mutual information is defined as [18, Section 6]

$$\widetilde{I}_{\alpha}\left(A;B|C\right)_{\rho} \equiv \frac{1}{\alpha-1}\log\left\|\rho_{ABC}^{1/2}\rho_{AC}^{(1-\alpha)/2\alpha}\rho_{C}^{(\alpha-1)/2\alpha}\rho_{BC}^{(1-\alpha)/2\alpha}\right\|_{2\alpha}^{2\alpha}. \tag{3.3.54}$$

Proofs were given for this conjectured inequality in Section B.6.3 in some special cases.

Since the quantum discord is based upon the QCMI, we now examine the implications of this conjecture for the quantum discord, by writing down a corresponding lower bound on it. This lower bound if true would provide a characterization for states with small quantum discord (the von Neumann entropy based quantity that is). It has the interpretation as quantifying how far a quantum state is from being a fixed point of an entanglement-breaking map. In case the discord is equal to zero we can conclude that the state is a fixed point of an entanglement-breaking map. In this case, we can apply [67, Theorem 5.3] to conclude the known result that any zero-discord state is in fact a classical-quantum state.

Consequence 3.24. *Assuming Conjecture B.25, the following lower bounds hold for the quantum discord of* $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$*:*

$$D(\overline{A};B)_{\rho} \geq \min_{\left\{|\phi_x\rangle:\sum_x|\phi_x\rangle\langle\phi_x|=I\right\}} -\log F\left(\rho_{AB},\mathcal{E}_A(\rho_{AB})\right), \tag{3.3.55}$$

where

$$\rho_B^x \equiv \frac{1}{\operatorname{Tr}\left\{|\phi_x\rangle\langle\phi_x|_A\,\rho_{AB}\right\}}\langle\phi_x|_A\,\rho_{AB}\,|\phi_x\rangle_A, \tag{3.3.56}$$

and $\mathcal{E}_A$ *is the following entanglement-breaking map:*

$$\mathcal{E}_A(\sigma_A) \equiv \sum_x \langle\phi_x|_A\,\sigma_A\,|\phi_x\rangle_A\,\frac{\rho_A^{1/2}\,|\phi_x\rangle\langle\phi_x|_A\,\rho_A^{1/2}}{\operatorname{Tr}\left\{|\phi_x\rangle\langle\phi_x|_A\,\rho_A\right\}}. \tag{3.3.57}$$

Consider a rank-one measurement $\{|\phi_x\rangle\langle\phi_x|\}$, and its isometric extension

$$U_{A\to XE} = \sum_x |x\rangle_X\,|x\rangle_E\,\langle\phi_x|_A\,. \tag{3.3.58}$$

For a given state ρ_{AB}, the state relevant for discord becomes

$$\begin{aligned} U_{A\to XE}\rho_{AB}U_{A\to XE}^{\dagger} &= \sum_{x,y}|x\rangle_X\,|x\rangle_E\,\langle\phi_x|_A\,\rho_{AB}\,|\phi_y\rangle_A\,\langle y|_X\,\langle y|_E & (3.3.59)\\ &= \sum_{x,y}\langle\phi_x|_A\,\rho_{AB}\,|\phi_y\rangle_A\otimes|x\rangle\langle y|_X\otimes|x\rangle\langle y|_E\,. & (3.3.60)\end{aligned}$$

The lower bound in (B.6.40) for this state takes the form:

$$I\left(E;B|X\right) \geq -\log F\left(\rho_{BEX},\rho_{EX}^{1/2}\rho_X^{-1/2}\rho_{BX}\rho_X^{-1/2}\rho_{EX}^{1/2}\right). \tag{3.3.61}$$

So, we need to calculate ρ_{BX}, ρ_X, and ρ_{EX}:

$$\rho_{BX} = \sum_x \langle\phi_x|_A \rho_{AB} |\phi_x\rangle_A \otimes |x\rangle \langle x|_X , \tag{3.3.62}$$

$$\rho_X = \sum_x \text{Tr}\{|\phi_x\rangle \langle\phi_x|_A \rho_{AB}\} |x\rangle \langle x|_X , \tag{3.3.63}$$

$$\rho_{EX} = \sum_{x,y} \text{Tr}\{|\phi_y\rangle \langle\phi_x|_A \rho_{AB}\} |x\rangle \langle y|_X \otimes |x\rangle \langle y|_E . \tag{3.3.64}$$

Let

$$\rho_B^x \equiv \frac{1}{\text{Tr}\{|\phi_x\rangle \langle\phi_x|_A \rho_{AB}\}} \langle\phi_x|_A \rho_{AB} |\phi_x\rangle_A . \tag{3.3.65}$$

Then we have that

$$\begin{aligned}
&\rho_{EX}^{1/2}\rho_X^{-1/2}\rho_{BX}\rho_X^{-1/2}\rho_{EX}^{1/2} \\
&= \rho_{EX}^{1/2}\left(\sum_x |x\rangle \langle x|_X \otimes \rho_B^x\right)\rho_{EX}^{1/2} &(3.3.66)\\
&= \left(U_{A\to XE}\rho_A U_{A\to XE}^\dagger\right)^{1/2}\left(\sum_x |x\rangle \langle x|_X \otimes \rho_B^x\right)\left(U_{A\to XE}\rho_A U_{A\to XE}^\dagger\right)^{1/2} &(3.3.67)\\
&= U_{A\to XE}\rho_A^{1/2}U_{A\to XE}^\dagger\left(\sum_x |x\rangle \langle x|_X \otimes \rho_B^x\right)U_{A\to XE}\rho_A^{1/2}U_{A\to XE}^\dagger. &(3.3.68)
\end{aligned}$$

Sandwiching by $U_{A\to XE}^\dagger (\cdot) U_{A\to XE}$ then gives

$$\begin{aligned}
&\rho_A^{1/2}U_{A\to XE}^\dagger\left(\sum_x |x\rangle \langle x|_X \otimes \rho_B^x\right)U_{A\to XE}\rho_A^{1/2} \\
&= \rho_A^{1/2}\left(\sum_z |\phi_z\rangle_A \langle z|_X \langle z|_E\right)\left(\sum_x |x\rangle \langle x|_X \otimes \rho_B^x\right)\left(\sum_{z'} |z'\rangle_X |z'\rangle_E \langle\phi_{z'}|_A\right)\rho_A^{1/2} &(3.3.69)\\
&= \rho_A^{1/2}\left(\sum_{z,x,z'} |\phi_z\rangle_A \langle\phi_{z'}|_A \langle z| |z'\rangle_E \langle z| |x\rangle \langle x| |z'\rangle_X \otimes \rho_B^x\right)\rho_A^{1/2} &(3.3.70)\\
&= \rho_A^{1/2}\left(\sum_x |\phi_x\rangle \langle\phi_x|_A \otimes \rho_B^x\right)\rho_A^{1/2} &(3.3.71)\\
&= \sum_x \rho_A^{1/2} |\phi_x\rangle \langle\phi_x|_A \rho_A^{1/2} \otimes \rho_B^x, &(3.3.72)
\end{aligned}$$

which we can see is a density operator on systems A and B. This establishes that $\rho_{EX}^{1/2}\rho_X^{-1/2}\rho_{BX}$ $\rho_X^{-1/2}\rho_{EX}^{1/2}$ is in the subspace onto which $U_{A\to XE}U_{A\to XE}^\dagger$ projects, and since this is true also for the state ρ_{BXE}, we find that

$$F\left(\rho_{BEX}, \rho_{EX}^{1/2}\rho_X^{-1/2}\rho_{BX}\rho_X^{-1/2}\rho_{EX}^{1/2}\right) = F\left(\rho_{AB}, \sum_x \rho_A^{1/2} |\phi_x\rangle \langle\phi_x|_A \rho_A^{1/2} \otimes \rho_B^x\right) \tag{3.3.73}$$

which is the bound in (3.3.55).

3.4 Discussion

To summarize, in this chapter, we defined a Rényi squashed entanglement and a Rényi quantum discord, and examined various properties of the quantities. We took as a conjecture that the Rényi conditional mutual information of a tripartite state ρ_{ABC} is monotone under local CPTP maps on both systems A and B. Assuming the conjecture, we showed that these quantities retain most of the properties of the original von Neumann entropy based quantities. For example, we showed that the Rényi squashed entanglement is convex, monotone under LOCC, that it vanishes on separable states and is subadditive on tensor-product states. Similarly, we showed that the Rényi quantum discord is non-negative, invariant under the action of local unitaries, vanishes on the set of classical-quantum states, and is optimized by a rank-one POVM. Further, we proved relations of the Rényi squashed entanglement to a Rényi entropy of entanglement and a Rényi entanglement of formation. We gave an expression for the Rényi discord of pure bipartite states. Also, assuming the truth of a conjecture on the monotonicity of the Rényi QCMI with respect to the Rényi parameter, we derived a remainder term for von Neumann entropy based quantum discord via the Rényi quantum discord.

The following are some future directions that could be considered based on the results presented in this chapter. One could also try to prove more properties of the Rényi squashed entanglement and discord. For example, we have left open the converse part of faithfulness for both the Rényi squashed entanglement as well as the Rényi discord. The von Neumann entropy based squashed entanglement is known to be superadditive in general and additive on tensor-product states. However, we have only been able to show that the Rényi squashed entanglement is subadditive on tensor-product states; super-additivity of the Rényi squashed entanglement in general has been left open. As far as applications are concerned, it is an open question if the von Neumann entropy based squashed entanglement is a strong converse rate for entanglement distillation; the Rényi squashed entanglement may be a useful tool in investigating this question. Also, using the Rényi squashed entanglement, one could try to prove that the von Neumann entropy based squashed entanglement is a strong converse rate for the two-way assisted quantum capacity of any channel (the weak converse bound being shown in [178, 177]). It might also be interesting to determine if a Koashi-Winter type [112] relation holds for the proposed Rényi discord.

Chapter 4
Fidelity of Recovery, Geometric Squashed Entanglement and Measurement Recoverability

4.1 Introduction

While defining the Rényi squashed entanglement and discord quantities in Chapter 3, we had left the Rényi parameter to be any arbitrary real value $\alpha \in (0,1) \cup (1,2]$. Also, subsequently in proving some of the properties of these quantities, we had to assume the monotonicity of the Rényi quantum conditional mutual information (QCMI) $I_\alpha(A;B|C)_\rho$ with respect to quantum operations on system A to be true. In this chapter, we define a new squashed entanglement and quantum discord that are inspired from a particular Rényi QCMI, and these quantities do not rely on such an assumption about monotonicity under quantum operations.

Before defining the new Rényi squashed entanglement and discord quantities, we give some background that led to the development of the core quantity behind these new quantities. Consider the Rényi QCMI $\widetilde{I}_\alpha(A;B|C)_\rho$ of $(B.4.24)$. It can be written as the following norm:

$$\widetilde{I}_\alpha(A;B|C)_\rho \equiv \frac{1}{\alpha-1} \log \left\| \rho_{ABC}^{1/2} \rho_{AC}^{(1-\alpha)/2\alpha} \rho_C^{(\alpha-1)/2\alpha} \rho_{BC}^{(1-\alpha)/2\alpha} \right\|_{2\alpha}^{2\alpha}. \tag{4.1.1}$$

In particular, consider the quantity corresponding to $\alpha = 1/2$

$$\tilde{I}_{1/2}(A;B|C)_\rho = -2\log \left\| \rho_{ABC}^{1/2} \rho_{AC}^{1/2} \rho_C^{-1/2} \rho_{BC}^{1/2} \right\|_1 \tag{4.1.2}$$

$$= -\log \operatorname{Tr}\left\{ \left(\rho_{ABC}^{1/2} \rho_{AC}^{1/2} \rho_C^{-1/2} \rho_{BC} \rho_C^{-1/2} \rho_{AC}^{1/2} \rho_{ABC}^{1/2} \right)^{1/2} \right\}^2 \tag{4.1.3}$$

$$= -\log F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}^{\mathcal{P}}(\rho_{BC})\right), \tag{4.1.4}$$

where

$$\mathcal{R}_{C\to AC}^{\mathcal{P}}(\cdot) \equiv \rho_{AC}^{1/2} \rho_C^{-1/2} (\cdot)\, \rho_C^{-1/2} \rho_{AC}^{1/2} \tag{4.1.5}$$

is a quantum channel called the Petz recovery map [80], and

$$F(\rho,\sigma) \equiv \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1^2 \tag{4.1.6}$$

is the fidelity between two positive semidefinite operators ρ and σ. The Conjecture B.25, if proven to be true, would imply the following lower bound for the QCMI in terms of $\tilde{I}_{1/2}(A;B|C)_\rho$

$$I(A;B|C)_\rho \geq -\log F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}^{\mathcal{P}}(\rho_{BC})\right). \tag{4.1.7}$$

The above statement would then in turn imply that it is possible to understand tripartite states with small QCMI in the following sense: *If one loses system A of a tripartite state ρ_{ABC} and is allowed to perform the Petz recovery map on system C alone, then the fidelity of recovery in doing so will be high.* The converse statement was already discussed in Proposition B.26 and independently in [62, Eq. (8)]. It has also been explicitly proven in [62, Eq. (8)] that the following lower bound on the QCMI holds

$$I\left(A;B\left|C\right.\right)_{\rho} \geq I_F\left(A;B\left|C\right.\right)_{\rho} \equiv -\inf_{\mathcal{R}_{C\to AC}} \log F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right), \tag{4.1.8}$$

where $\mathcal{R}_{C\to AC}\left(\cdot\right)$ is now any recovery quantum channel acting on system C that attempts to recover system A.

We show that the $I_F\left(A;B\left|C\right.\right)_{\rho}$ quantity serves as a proxy for the QCMI in the sense that it obeys many of the same properties as the QCMI. Unlike the Rényi QCMI for arbitrary α, $I_F\left(A;B\left|C\right.\right)_{\rho}$ is a well behaved quantity for which we can prove monotonicity under local quantum operations on both systems A and B. Consequently, we define a new squashed entanglement and discord based on $I_F\left(A;B\left|C\right.\right)_{\rho}$ and prove that they are valid correlation measures without having to rely on any conjectures.

This chapter is organized as follows. We introduce the fidelity of recovery of state ρ_{ABC}, $F\left(A;B|C\right)_{\rho}$, which is a quantity that underlies $I_F\left(A;B\left|C\right.\right)_{\rho}$ of (4.1.8) as $-\log F\left(A;B|C\right)_{\rho}$. (In other words, $I_F\left(A;B\left|C\right.\right)_{\rho}$ is the surprisal of the fidelity of recovery.) We explain the essence of this quantity, and prove the properties that place $I_F\left(A;B\left|C\right.\right)_{\rho}$ on an almost equal footing as the QCMI. We then define and study our new correlation measures based on $I_F\left(A;B\left|C\right.\right)_{\rho}$, namely the geometric squashed entanglement and the surprisal of measurement recoverability. We show that the geometric squashed entanglement is a 1-LOCC monotone, which is also faithful and continuous. Likewise, we show that the surprisal of measurement recoverability satisfies all the same properties as the von Neumann entropy-based quantum discord.

4.2 Fidelity of Recovery

Consider a tripartite state $\rho_{ABC} \in \mathcal{S}\left(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C\right)$ on systems A, B, and C. Suppose that system A is lost, and a recovery operation is performed on system C alone in an attempt to recover the full state on all three systems. The fidelity of recovery is a measure that quantifies how well one can recover the full state when the optimal recovery operation is performed. Figure 4.1 illustrates the essence of the quantity. We now formally define the fidelity of recovery, and prove some properties.

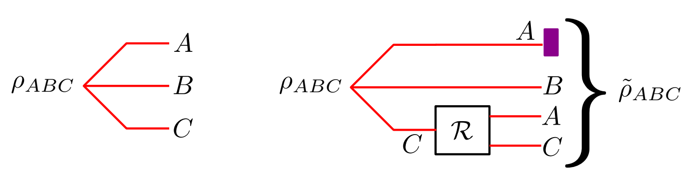

Figure 4.1: The fidelity of recovery of a tripartite state ρ_{ABC} captures how closely the state $\tilde{\rho}_{ABC}$ approximates ρ_{ABC}.

Definition 4.1. *Let ρ_{ABC} be a tripartite state. The fidelity of recovery of ρ_{ABC} with respect to system A is defined as follows:*

$$F(A;B|C)_{\rho} \equiv \sup_{\mathcal{R}_{C\to AC}} F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right). \tag{4.2.1}$$

Proposition 4.2. *Let ρ_{ABC} be a tripartite state. Then $I_F(A;B|C)_{\rho} \geq 0$ and for finite-dimensional ρ_{ABC}, $I_F(A;B|C)_{\rho} = 0$ if and only if ρ_{ABC} is a short quantum Markov chain, as defined in [80].*

Proof. The inequality $I_F(A;B|C)_{\rho} \geq 0$ is a consequence of the fidelity always being less than or equal to one. Suppose that ρ_{ABC} is a short quantum Markov chain as defined in [80]. As discussed in that paper, this is equivalent to the equality

$$\rho_{ABC} = \mathcal{R}^{P}_{C\to AC}\left(\rho_{BC}\right), \tag{4.2.2}$$

where $\mathcal{R}^{P}_{C\to AC}$ is the Petz recovery channel. So this implies that

$$F\left(\rho_{ABC}, \mathcal{R}^{P}_{C\to AC}\left(\rho_{BC}\right)\right) = 1, \tag{4.2.3}$$

which in turn implies that $F(A;B|C)_{\rho} = 1$ and hence $I_F(A;B|C)_{\rho} = 0$. Now suppose that $I_F(A;B|C)_{\rho} = 0$. This implies that

$$\sup_{\mathcal{R}_{C\to AC}} F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right) = 1. \tag{4.2.4}$$

Due to the finite-dimensional assumption, the space of channels over which we are optimizing is compact. Furthermore, the fidelity is continuous in its arguments. This is sufficient for us to conclude that the supremum is achieved and that there exists a channel $\mathcal{R}_{C\to AC}$ for which $F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right) = 1$, implying that

$$\rho_{ABC} = \mathcal{R}_{C\to AC}\left(\rho_{BC}\right). \tag{4.2.5}$$

From a result of Petz [141], this implies that the Petz recovery channel recovers ρ_{ABC} perfectly, i.e.,

$$\rho_{ABC} = \mathcal{R}^{P}_{C\to AC}\left(\rho_{BC}\right), \tag{4.2.6}$$

and this is equivalent to ρ_{ABC} being a short quantum Markov chain [80]. ■

Proposition 4.3. *Let ϕ_{ABCD} denote a four-party pure state. Then*

$$F(A;B|C)_{\phi} = F(A;B|D)_{\phi}, \tag{4.2.7}$$

which is equivalent to

$$I_F(A;B|C)_{\phi} = I_F(A;B|D)_{\phi}. \tag{4.2.8}$$

Proof. The proof of this proposition uses Uhlmann's theorem given in . By definition,

$$F(A;B|C)_{\phi} = \sup_{\mathcal{R}^{1}_{C\to AC}} F\left(\phi_{ABC}, \mathcal{R}^{1}_{C\to AC}\left(\phi_{BC}\right)\right). \tag{4.2.9}$$

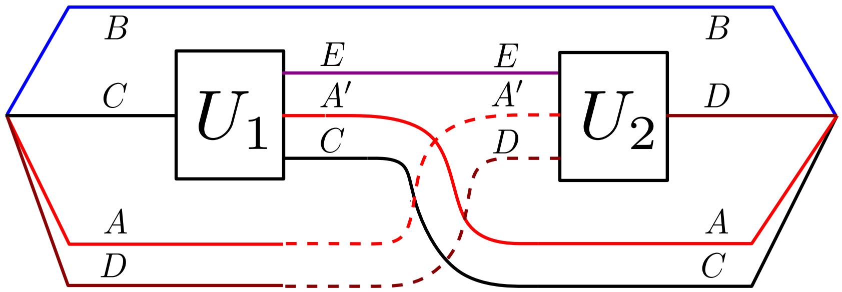

Figure 4.2: This figure helps to illustrate the main idea behind the proof of Proposition 4.3 and furthermore highlights the dual role played by an isometric extension of the recovery map on C and an Uhlmann isometry acting on system D (and vice versa).

Let $\mathcal{U}^{\mathcal{R}^1}_{C\to ACE}$ be an isometric map which extends $\mathcal{R}^1_{C\to AC}$. Since ϕ_{ABCD} is a purification of ϕ_{ABC} and $\mathcal{U}^{\mathcal{R}^1}_{C\to ACE}(\phi_{BCA'D})$ is a purification of $\mathcal{R}^1_{C\to AC}(\phi_{BC})$, we can apply Uhlmann's theorem for fidelity to conclude that

$$\sup_{\mathcal{R}^1_{C\to AC}} F\left(\phi_{ABC}, \mathcal{R}^1_{C\to AC}(\phi_{BC})\right) = \sup_{\mathcal{U}_{D\to A'DE}} \sup_{\mathcal{U}^{\mathcal{R}^1}_{C\to ACE}} F\left(\mathcal{U}_{D\to A'DE}(\phi_{ABCD}), \mathcal{U}^{\mathcal{R}^1}_{C\to ACE}(\phi_{BCA'D})\right). \tag{4.2.10}$$

Now consider that

$$F(A;B|D)_\phi = \sup_{\mathcal{R}^2_{D\to AD}} F\left(\phi_{ABD}, \mathcal{R}^2_{D\to AD}(\phi_{BD})\right). \tag{4.2.11}$$

Let $\mathcal{U}^{\mathcal{R}^2}_{D\to ADE}$ be an isometric map which extends $\mathcal{R}^2_{D\to AD}$. Since ϕ_{ABCD} is a purification of ϕ_{ABD} and $\mathcal{U}^{\mathcal{R}^2}_{D\to ADE}(\phi_{BDA'C})$ is a purification of $\mathcal{R}^2_{D\to AD}(\phi_{BD})$, we can apply Uhlmann's theorem for fidelity to conclude that

$$\begin{aligned}&\sup_{\mathcal{R}^2_{D\to AD}} F\left(\phi_{ABD}, \mathcal{R}^2_{D\to AD}(\phi_{BD})\right)\\ &= \sup_{\mathcal{U}_{C\to A'CE}} \sup_{\mathcal{U}^{\mathcal{R}^2}_{D\to ADE}} F\left(\mathcal{U}_{C\to A'CE}(\phi_{ABCD}), \mathcal{U}^{\mathcal{R}^2}_{D\to ADE}(\phi_{BDA'C})\right).\end{aligned} \tag{4.2.12}$$

By inspecting the RHS of (4.2.10) and the RHS of (4.2.12), we see that the two expressions are equivalent so that the statement of the proposition holds. Figure 4.2 gives a graphical depiction of this proof which should help in determining which systems are "connected together" and furthermore highlights how the duality between the recovery map and the map from Uhlmann's theorem is reflected in the duality for the fidelity of recovery. ■

Remark 4.4. *The physical interpretation of the above duality is as follows: beginning with a four-party pure state ϕ_{ABCD}, suppose that system A is lost. Then one can recover the state on systems ABC from system C alone just as well as one can recover the state on systems ABD from system D alone.*

Proposition 4.5. *The fidelity of recovery is monotone under local operations on systems A and B, i.e.*

$$F(A;B|C)_\rho \leq F(A';B'|C)_\tau, \tag{4.2.13}$$

where $\tau_{A'B'C} \equiv (\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{ABC})$. *The above inequality is equivalent to*

$$I_F(A;B|C)_\rho \geq I_F(A';B'|C)_\tau . \tag{4.2.14}$$

Proof. Consider any recovery map $\mathcal{R}_{C\to AC}$. We have that

$$F(\rho_{ABC}, \mathcal{R}_{C\to AC}(\rho_{BC})) \tag{4.2.15}$$
$$\leq F((\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{ABC}), (\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\mathcal{R}_{C\to AC}(\rho_{BC}))) \tag{4.2.16}$$
$$= F((\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{ABC}), (\mathcal{N}_{A\to A'} \circ \mathcal{R}_{C\to AC})(\mathcal{M}_{B\to B'}(\rho_{BC}))) \tag{4.2.17}$$
$$\leq \sup_{\mathcal{R}_{C\to A'C}} F((\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{ABC}), \mathcal{R}_{C\to A'C}(\mathcal{M}_{B\to B'}(\rho_{BC}))) \tag{4.2.18}$$
$$= F(A';B'|C)_{(\mathcal{N}\otimes\mathcal{M})(\rho)} . \tag{4.2.19}$$

The first inequality is due to monotonicity of the fidelity under quantum operations. The first equality follows from the fact that the recovery map $\mathcal{R}$ and the noisy map $\mathcal{M}$ commute since the former does not act on system B. The second inequality follows from the fact that the supremum of the fidelity with respect to an optimization over recovery maps can only be greater than or equal to the fidelity corresponding to an arbitrary recovery map. The second equality follows from Definition 4.1. Finally, since the above chain of reasoning holds for all $\mathcal{R}_{C\to AC}$, it follows that

$$F(A;B|C)_\rho = \sup_{\mathcal{R}_{C\to AC}} F(\rho_{ABC}, \mathcal{R}_{C\to AC}(\rho_{BC})) \leq F(A';B'|C)_{(\mathcal{N}\otimes\mathcal{M})(\rho)} . \tag{4.2.20}$$

■

Remark 4.6. *The physical interpretation of the above monotonicity under local operations is as follows: for a tripartite state* ρ_{ABC}*, suppose that system* A *is lost. Then it is easier to recover the state on systems* ABC *from* C *alone if there is local noise applied to systems* A *or* B *or both, before system* A *is lost (and thus before attempting the recovery). The only property of the fidelity used to prove the above proposition is that it is monotone under quantum operations. This suggests that we can construct a fidelity-of-recovery-like measure from any "generalized divergence" (a function that is monotone under quantum operations).*

Proposition 4.7. *Let* ρ_{ABC} *be a tripartite quantum state and let*

$$\sigma_{A'B'C'} \equiv (\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'} \otimes \mathcal{W}_{C\to C'})(\rho_{ABC}), \tag{4.2.21}$$

where $\mathcal{U}_{A\to A'}$, $\mathcal{V}_{B\to B'}$*, and* $\mathcal{W}_{C\to C'}$ *are isometric quantum channels. Then*

$$F(A;B|C)_\rho = F(A';B'|C')_\sigma , \tag{4.2.22}$$
$$I_F(A;B|C)_\rho = I_F(A';B'|C')_\sigma . \tag{4.2.23}$$

Proof. We prove the statement for fidelity of recovery. We first need to define some CPTP maps that invert the isometric channels $\mathcal{U}_{A\to A'}$, $\mathcal{V}_{B\to B'}$, and $\mathcal{W}_{C\to C'}$, given that $\mathcal{U}^\dagger_{A\to A'}$, $\mathcal{V}^\dagger_{B\to B'}$, and $\mathcal{W}^\dagger_{C\to C'}$ are not necessarily quantum channels. So we define the CPTP linear map $\mathcal{T}^{\mathcal{U}}_{A'\to A}$ as follows:

$$\mathcal{T}^{\mathcal{U}}_{A'\to A}(\omega_{A'}) \equiv \mathcal{U}^\dagger_{A\to A'}(\omega_{A'}) + \mathrm{Tr}\left\{\left(\mathrm{id}_{A'} - \mathcal{U}^\dagger_{A\to A'}\right)(\omega_{A'})\right\}\tau_A, \tag{4.2.24}$$

where τ_A is some state on system A. We define the maps $\mathcal{T}^{\mathcal{V}}_{B'\to B}$ and $\mathcal{T}^{\mathcal{W}}_{C'\to C}$ similarly. All three maps have the property that

$$\mathcal{T}^{\mathcal{U}}_{A'\to A} \circ \mathcal{U}_{A\to A'} = \mathrm{id}_A, \tag{4.2.25}$$
$$\mathcal{T}^{\mathcal{V}}_{B'\to B} \circ \mathcal{V}_{B\to B'} = \mathrm{id}_B, \tag{4.2.26}$$
$$\mathcal{T}^{\mathcal{W}}_{C'\to C} \circ \mathcal{W}_{C\to C'} = \mathrm{id}_C. \tag{4.2.27}$$

Let $\mathcal{R}_{C\to AC}$ be an arbitrary recovery map. Then

$$F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right)$$
$$= F\left(\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'} \otimes \mathcal{W}_{C\to C'}\right)\left(\rho_{ABC}\right), \left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'} \otimes \mathcal{W}_{C\to C'}\right)\left(\mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right)\right) \tag{4.2.28}$$
$$= F\left(\sigma_{A'B'C'}, \left(\mathcal{U}_{A\to A'} \otimes \mathcal{W}_{C\to C'}\right)\left(\mathcal{R}_{C\to AC}\left(\mathcal{V}_{B\to B'}\left(\rho_{BC}\right)\right)\right)\right) \tag{4.2.29}$$

$$= F\left(\sigma_{A'B'C'}, \left(\mathcal{U}_{A\to A'} \otimes \mathcal{W}_{C\to C'}\right)\left(\mathcal{R}_{C\to AC}\left(\mathcal{T}^{\mathcal{W}}_{C'\to C}\left(\mathcal{V}_{B\to B'} \otimes \mathcal{W}_{C\to C'}\right)\left(\rho_{BC}\right)\right)\right)\right)$$
$$\leq \sup_{\mathcal{R}_{C'\to A'C'}} F\left(\sigma_{A'B'C'}, \mathcal{R}_{C'\to A'C'}\left(\left(\mathcal{V}_{B\to B'} \otimes \mathcal{W}_{C\to C'}\right)\left(\rho_{BC}\right)\right)\right)$$
$$= F\left(A'; B'|C'\right)_\sigma.$$

The first equality follows from invariance of fidelity with respect to isometries. The second equality follows because $\mathcal{R}_{C\to AC}$ and $\mathcal{V}_{B\to B'}$ commute. The third equality follows from (4.2.27). The inequality follows because

$$\left(\mathcal{U}_{A\to A'} \otimes \mathcal{W}_{C\to C'}\right) \circ \mathcal{R}_{C\to AC} \circ \mathcal{T}^{\mathcal{W}}_{C'\to C} \tag{4.2.30}$$

is a particular CPTP recovery map from C' to $A'C'$. The last equality is from the definition of fidelity of recovery. Given that the inequality

$$F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right) \leq F\left(A'; B'|C'\right)_\sigma \tag{4.2.31}$$

holds for an arbitrary recovery map $\mathcal{R}_{C\to AC}$, we can conclude that

$$F\left(A; B|C\right)_\rho \leq F\left(A'; B'|C'\right)_\sigma. \tag{4.2.32}$$

For the other inequality, let $\mathcal{R}_{C'\to A'C'}$ be an arbitrary recovery map. Then

$$F\left(\sigma_{A'B'C'}, \mathcal{R}_{C'\to A'C'}\left(\sigma_{B'C'}\right)\right)$$
$$\leq F\left(\left(\mathcal{T}^{\mathcal{U}}_{A'\to A} \otimes \mathcal{T}^{\mathcal{V}}_{B'\to B} \otimes \mathcal{T}^{\mathcal{W}}_{C'\to C}\right)\left(\sigma_{A'B'C'}\right), \left(\mathcal{T}^{\mathcal{U}}_{A'\to A} \otimes \mathcal{T}^{\mathcal{V}}_{B'\to B} \otimes \mathcal{T}^{\mathcal{W}}_{C'\to C}\right)\left(\mathcal{R}_{C'\to A'C'}\left(\sigma_{B'C'}\right)\right)\right) \tag{4.2.33}$$
$$= F\left(\rho_{ABC}, \left(\mathcal{T}^{\mathcal{U}}_{A'\to A} \otimes \mathcal{T}^{\mathcal{W}}_{C'\to C}\right)\left(\mathcal{R}_{C'\to A'C'}\left(\mathcal{T}^{\mathcal{V}}_{B'\to B}\left(\sigma_{B'C'}\right)\right)\right)\right) \tag{4.2.34}$$
$$= F\left(\rho_{ABC}, \left(\mathcal{T}^{\mathcal{U}}_{A'\to A} \otimes \mathcal{T}^{\mathcal{W}}_{C'\to C}\right)\left(\mathcal{R}_{C'\to A'C'}\left(\left(\mathcal{T}^{\mathcal{V}}_{B'\to B} \circ \mathcal{V}_{B\to B'} \otimes \mathcal{W}_{C\to C'}\right)\left(\rho_{BC}\right)\right)\right)\right) \tag{4.2.35}$$
$$= F\left(\rho_{ABC}, \left(\mathcal{T}^{\mathcal{U}}_{A'\to A} \otimes \mathcal{T}^{\mathcal{W}}_{C'\to C}\right)\left(\mathcal{R}_{C'\to A'C'}\left(\mathcal{W}_{C\to C'}\left(\rho_{BC}\right)\right)\right)\right) \tag{4.2.36}$$
$$\leq \sup_{\mathcal{R}_{C\to AC}} F\left(\rho_{ABC}, \mathcal{R}_{C\to AC}\left(\rho_{BC}\right)\right) \tag{4.2.37}$$
$$= F\left(A; B|C\right)_\rho. \tag{4.2.38}$$

The first inequality is from monotonicity of the fidelity with respect to quantum channels. The first equality is a consequence of (4.2.25)-(4.2.27). The second equality is from the definition of $\sigma_{B'C'}$. The third equality follows from (4.2.27). The last inequality follows because $\left(\mathcal{T}^{\mathcal{U}}_{A'\to A}\otimes\mathcal{T}^{\mathcal{W}}_{C'\to C}\right)\circ\mathcal{R}_{C'\to A'C'}\circ\mathcal{W}_{C\to C'}$ is a particular recovery map from C to AC. Given that the inequality

$$F\left(\sigma_{A'B'C'},\mathcal{R}_{C'\to A'C'}\left(\sigma_{B'C'}\right)\right)\leq F\left(A;B|C\right)_{\rho} \tag{4.2.39}$$

holds for an arbitrary recovery map $\mathcal{R}_{C'\to A'C'}$, we can conclude that

$$F\left(A';B'|C'\right)_{\sigma}\leq F\left(A;B|C\right)_{\rho}. \tag{4.2.40}$$

■

Remark 4.8. *The only property of the fidelity used to prove Propositions 4.5 and 4.7 is that it is monotone with respect to quantum operations. This suggests that we can construct a fidelity-of-recovery-like measure from any "generalized divergence" (a function that is monotone with respect to quantum operations).*

Proposition 4.9. *The fidelity of recovery obeys the following dimension bound:*

$$F\left(A;B|C\right)_{\rho}\geq\frac{1}{|A|^{2}}, \tag{4.2.41}$$

which is equivalent to

$$I_{F}\left(A;B|C\right)_{\rho}\leq 2\log|A|. \tag{4.2.42}$$

If the system A is classical, so that we relabel it as X, then the following hold

$$F\left(X;B|C\right)_{\rho}\geq\frac{1}{|X|}, \tag{4.2.43}$$

$$I_{F}\left(X;B|C\right)_{\rho}\leq\log|X|. \tag{4.2.44}$$

Examples of states achieving these bounds are $\Phi_{AB}\otimes\sigma_{C}$ for (4.2.41)-(4.2.42) and $\overline{\Phi}_{XB}\otimes\sigma_{C}$ for (4.2.43)-(4.2.44), where

$$\overline{\Phi}_{XB}\equiv\frac{1}{|X|}\sum_{x}|x\rangle\langle x|_{X}\otimes|x\rangle\langle x|_{B}. \tag{4.2.45}$$

Proof. Consider that the following inequality holds, simply by choosing the recovery map to be one in which we do not do anything to system C and prepare the maximally mixed state $\pi_{A}\equiv I_{A}/|A|$ on system A:

$$F\left(A;B|C\right)_{\rho}\geq F\left(\rho_{ABC},\pi_{A}\otimes\rho_{BC}\right) \tag{4.2.46}$$

$$=\frac{1}{|A|}F\left(\rho_{ABC},I_{A}\otimes\rho_{BC}\right) \tag{4.2.47}$$

$$\geq\frac{1}{|A|}\left[\operatorname{Tr}\left\{\sqrt{\rho_{ABC}}\sqrt{I_{A}\otimes\rho_{BC}}\right\}\right]^{2}. \tag{4.2.48}$$

Taking a negative logarithm and letting ϕ_{ABCD} be a purification of ρ_{ABC}, we find that

$$I_F(A;B|C)_\rho \leq \log|A| - 2\log \operatorname{Tr}\left\{\sqrt{\rho_{ABC}}\sqrt{I_A \otimes \rho_{BC}}\right\} \tag{4.2.49}$$

$$= \log|A| - H_{1/2}(A|BC)_\rho \tag{4.2.50}$$

$$= \log|A| + H_{3/2}(A|D)_\rho \tag{4.2.51}$$

$$\leq \log|A| + H_{3/2}(A)_\rho \tag{4.2.52}$$

$$\leq 2\log|A|. \tag{4.2.53}$$

The first equality follows by recognizing that the second term is a conditional Rényi entropy of order 1/2 [183, Definition 3]. The second equality follows from a duality relation for this conditional Rényi entropy [183, Lemma 6]. The second inequality is a consequence of the quantum data processing inequality for conditional Rényi entropies [183, Lemma 5] (with the map taken to be a partial trace over system D). The last inequality follows from a dimension bound which holds for any Rényi entropy.

To see that $\Phi_{AB} \otimes \sigma_C$ has $I_F(A;B|C) = 2\log|A|$, we can apply Propositions 4.24 and 4.23.

For classical A system, we follow the same steps up to (4.2.50), but then apply Lemma D.8 to conclude that $H_{1/2}(A|BC) \geq 0$ for a classical A. This gives (4.2.43)-(4.2.44). To see that $\overline{\Phi}_{XB} \otimes \sigma_C$ has $I_F(X;B|C) = \log|X|$, we apply Proposition 4.12 and then evaluate

$$F\left(\overline{\Phi}_{XB}, \tau_X \otimes \overline{\Phi}_B\right) = \left\| \left(\sum_x \frac{1}{\sqrt{|X|}} |x\rangle\langle x|_X \otimes |x\rangle\langle x|_B \right) \left(\sqrt{\tau_X} \otimes \frac{1}{\sqrt{|X|}} I_B \right) \right\|_1^2 \tag{4.2.54}$$

$$= \left[\frac{1}{|X|} \left\| \left(\sum_x |x\rangle\langle x|_X \otimes |x\rangle\langle x|_B \right) (\sqrt{\tau_X} \otimes I_B) \right\|_1 \right]^2 \tag{4.2.55}$$

$$= \left[\frac{1}{|X|} \sum_x \left\| |x\rangle\langle x|_X \sqrt{\tau_X} \right\|_1 \right]^2 \tag{4.2.56}$$

$$= \left[\frac{1}{|X|} \sum_x \sqrt{\langle x|\tau|x\rangle} \right]^2$$

$$\leq \frac{1}{|X|} \sum_x \langle x|\tau|x\rangle$$

$$= \frac{1}{|X|}$$

Choosing τ_X maximally mixed then achieves the upper bound, i.e.,

$$\sup_{\tau_X} F\left(\overline{\Phi}_{XB}, \tau_X \otimes \overline{\Phi}_B\right) = F\left(\overline{\Phi}_{XB}, \pi_X \otimes \overline{\Phi}_B\right) = \frac{1}{|X|}. \tag{4.2.57}$$

■

Proposition 4.10. *Given a four-party state ρ_{ABCD}, the following inequality holds*

$$I_F(AC;B|D)_\rho \geq I_F(A;B|CD)_\rho . \tag{4.2.58}$$

Proof. The inequality is equivalent to

$$F(AC;B|D)_\rho \leq F(A;B|CD)_\rho , \tag{4.2.59}$$

which is the statement that it is easier to recover A from CD than it is to recover both A and C from D alone. Indeed, let $\mathcal{R}_{D\to ACD}$ be any recovery map. Then

$$\begin{aligned} F(\rho_{ABCD}, \mathcal{R}_{D\to ACD}(\rho_{BD})) &= F(\rho_{ABCD}, (\mathcal{R}_{D\to ACD}\circ \mathrm{Tr}_C)(\rho_{BCD})) & (4.2.60)\\ &\leq \sup_{\mathcal{R}_{CD\to ACD}} F(\rho_{ABCD}, (\mathcal{R}_{CD\to ACD})(\rho_{BCD})) & (4.2.61)\\ &= F(A;B|CD)_\rho . & (4.2.62)\end{aligned}$$

Since the chain of inequalities holds for any recovery map $\mathcal{R}_{D\to ACD}$, we can conclude (4.2.59) from the definition of $F(AC;B|D)_\rho$. ■

Proposition 4.11. *Let ω_{ABCX} be a state for which system X is classical:*

$$\omega_{ABCX} = \sum_x p_X(x)\, \omega^x_{ABC} \otimes |x\rangle\langle x|_X , \tag{4.2.63}$$

where $\{|x\rangle_X\}$ is an orthonormal basis, $p_X(x)$ is a probability distribution, and each ω^x_{ABC} is a state. Then the following equalities hold

$$F(A;B|CX)_\omega \geq \left[\sum_x p_X(x)\sqrt{F(A;B|C)_{\omega^x}}\right]^2 , \tag{4.2.64}$$

$$I_F(A;B|CX)_\omega \leq -2\log\left[\sum_x p_X(x)\exp\left\{-\frac{1}{2}I_F(A;B|C)_{\omega^x}\right\}\right] . \tag{4.2.65}$$

Proof. For any set of recovery maps $\mathcal{R}^x_{C\to CA}$, we define $\mathcal{R}_{CX\to CXA}$ as follows:

$$\mathcal{R}_{CX\to CXA}(\tau_{CX}) \equiv \sum_x \mathcal{R}^x_{C\to CA}(\langle x|_X(\tau_{CX})|x\rangle_X)\ |x\rangle\langle x|_X , \tag{4.2.66}$$

so that it first measures the system X in the basis $\{|x\rangle\langle x|_X\}$, places the outcome in the same classical register, and then acts with the particular recovery map $\mathcal{R}^x_{C\to CA}$. Then

$$\begin{aligned} &\left[\sum_x p_X(x)\sqrt{F(\omega^x_{ABC}, \mathcal{R}^x_{C\to CA}(\omega^x_{BC}))}\right]^2 \\ &= F\left(\sum_x p_X(x)\,\omega^x_{ABC}\otimes|x\rangle\langle x|_X , \sum_x p_X(x)\,\mathcal{R}^x_{C\to CA}(\omega^x_{BC})\otimes|x\rangle\langle x|_X\right) & (4.2.67)\\ &= F\left(\sum_x p_X(x)\,\omega^x_{ABC}\otimes|x\rangle\langle x|_X , \mathcal{R}_{CX\to CXA}\left(\sum_x p_X(x)\,\omega^x_{BC}\otimes|x\rangle\langle x|_X\right)\right) & (4.2.68)\\ &\leq F(A;B|CX)_\omega . & (4.2.69)\end{aligned}$$

Since the inequality holds for any set of individual recovery maps $\{\mathcal{R}^x_{C\to CA}\}$, we obtain (4.2.64).

Finally, we recover (4.2.65) by applying a negative logarithm to the inequality in (4.2.64) and convexity of $-\log$. ■

Proposition 4.12. *Let $\rho_{ABC} = \sigma_{AB} \otimes \omega_C$. Then*

$$F(A;B|C)_\rho = F(A;B)_\sigma \equiv \sup_{\tau_A} F(\sigma_{AB}, \tau_A \otimes \sigma_B), \tag{4.2.70}$$

$$I_F(A;B|C)_\rho = I_F(A;B)_\sigma \equiv -\log F(A;B)_\sigma. \tag{4.2.71}$$

Proof. Consider that, for any recovery map $\mathcal{R}_{C\to AC}$

$$F(\sigma_{AB} \otimes \omega_C, \mathcal{R}_{C\to AC}(\sigma_B \otimes \omega_C)) = F(\sigma_{AB} \otimes \omega_C, \sigma_B \otimes \mathcal{R}_{C\to AC}(\omega_C)) \tag{4.2.72}$$

$$\leq F(\sigma_{AB}, \sigma_B \otimes \mathcal{R}_{C\to A}(\omega_C)) \tag{4.2.73}$$

$$\leq \sup_{\tau_A} F(\sigma_{AB}, \sigma_B \otimes \tau_A). \tag{4.2.74}$$

The first inequality follows because fidelity is monotone under partial trace over the C system. The second inequality follows by optimizing the second argument to the fidelity over all states on the A system. Since the inequality holds independent of the recovery map $\mathcal{R}_{C\to AC}$, this proves that

$$F(A;B|C)_\rho \leq F(A;B)_\sigma. \tag{4.2.75}$$

To prove the other inequality $F(A;B)_\sigma \leq F(A;B|C)_\rho$, consider for any state τ_A that

$$F(\sigma_{AB}, \sigma_B \otimes \tau_A) = F(\sigma_{AB} \otimes \omega_C, \sigma_B \otimes \tau_A \otimes \omega_C) \tag{4.2.76}$$

$$= F(\sigma_{AB} \otimes \omega_C, (\mathrm{id}_C \otimes \mathcal{P}^\tau_A)(\sigma_B \otimes \omega_C)) \tag{4.2.77}$$

$$\leq \sup_{\mathcal{R}_{C\to AC}} F(\sigma_{AB} \otimes \omega_C, \mathcal{R}_{C\to AC}(\sigma_B \otimes \omega_C)). \tag{4.2.78}$$

The first equality follows because fidelity is multiplicative under tensor-product states. The second equality follows by taking $(\mathrm{id}_C \otimes \mathcal{P}^\tau_A)$ to be the recovery map that does nothing to system C and prepares τ_A on system A. The inequality follows by optimizing over all recovery maps. Since the inequality is independent of the prepared state, we obtain the other inequality

$$F(A;B)_\sigma \leq F(A;B|C)_\rho. \tag{4.2.79}$$

The equality $I_F(A;B|C)_\rho = I_F(A;B)_\sigma$ follows by applying a negative logarithm to

$$F(A;B|C)_\rho = F(A;B)_\sigma. \tag{4.2.80}$$

We note in passing that the quantity on the RHS in (4.2.71) is closely related to the sandwiched Rényi mutual information of order 1/2 [132, 198, 11, 76]. ■

The following proposition gives a simple proof of the main result of [62] when the tripartite state of interest is pure:

Proposition 4.13. *The QCMI $I(A;B|C)_\psi$ of a pure tripartite state ψ_{ABC} has the following lower bound:*

$$I(A;B|C)_\psi \geq -\log F(A;B|C)_\psi. \tag{4.2.81}$$

Proof. Let φ_D be a pure state on an auxiliary system D, so that $|\psi\rangle_{ABC} \otimes |\varphi\rangle_D$ is a purification of $|\psi\rangle_{ABC}$. Consider the following chain of inequalities:

$$
\begin{aligned}
I(A;B|C)_\psi &= I(A;B|D)_{\psi\otimes\varphi} && (4.2.82)\\
&= I(A;B)_\psi && (4.2.83)\\
&\geq -\log F(\psi_{AB}, \psi_A \otimes \psi_B) && (4.2.84)\\
&\geq -\log F(A;B)_\psi && (4.2.85)\\
&= -\log F(A;B|D)_{\psi\otimes\varphi} && (4.2.86)\\
&= -\log F(A;B|C)_\psi . && (4.2.87)
\end{aligned}
$$

The first equality follows from duality of QCMI. The second follows because system D is product with systems A and B. The first inequality follows from monotonicity of the sandwiched Rényi relative entropies [132, Theorem 7]:

$$\widetilde{D}_\alpha(\rho\|\sigma) \leq \widetilde{D}_\beta(\rho\|\sigma), \tag{4.2.88}$$

for states ρ and σ and Rényi parameters α and β such that $0 \leq \alpha \leq \beta$. We apply this with the choices $\alpha = 1/2$, $\beta = 1$, $\rho = \psi_{AB}$, and $\sigma = \psi_A \otimes \psi_B$. The second inequality follows by optimizing over states on system A and applying the definition in (4.2.71). The second-to-last equality follows from Proposition 4.12 and the last from Proposition 4.3. ■

4.3 Geometric Squashed Entanglement

In this section, we formally define the geometric squashed entanglement of a bipartite state ρ_{AB}, and we prove its properties.

Definition 4.14. *The geometric squashed entanglement of a bipartite state ρ_{AB} is defined as follows:*

$$E_F^{\mathrm{sq}}(A;B)_\rho \equiv -\frac{1}{2}\log F^{\mathrm{sq}}(A;B)_\rho, \tag{4.3.1}$$

where

$$
\begin{aligned}
F^{\mathrm{sq}}(A;B)_\rho &\equiv \sup_{\omega_{ABE}} \left\{ F(A;B|E)_\rho : \rho_{AB} = \mathrm{Tr}_E\{\omega_{ABE}\} \right\} && (4.3.2)\\
&= \sup_{\omega_{ABE}} \sup_{\mathcal{R}_{E\to AE}} \{ F(\omega_{ABE}, \mathcal{R}_{E\to AE}(\omega_{BE})) : \rho_{AB} = \mathrm{Tr}_E\{\omega_{ABE}\}\} . && (4.3.3)
\end{aligned}
$$

The geometric squashed entanglement can equivalently be written in terms of an optimization over "squashing channels" acting on a purifying system of the original state (cf. [40, Eq. (3)]):

Proposition 4.15. *Let ρ_{AB} be a bipartite state and let $|\psi\rangle_{ABE'}$ be a fixed purification of it. Then*

$$F^{\mathrm{sq}}(A;B)_\rho = \sup_{\mathcal{S}_{E'\to E}} F(A;B|E)_{\mathcal{S}(\psi)}, \tag{4.3.4}$$

where the optimization is over squashing channels $\mathcal{S}_{E'\to E}$.

Proof. We first prove the inequality $F^{\text{sq}}(A;B)_\rho \geq \sup_{\mathcal{S}_{E'\to E}} F(A;B|E)_{\mathcal{S}(\psi)}$. Indeed, for a given squashing channel $\mathcal{S}_{E'\to E}$ and purification $\psi_{ABE'}$, the state $\mathcal{S}_{E'\to E}(\psi_{ABE'})$ is an extension of ρ_{AB}. So it follows by definition that

$$F(A;B|E)_{\mathcal{S}(\psi)} \leq F^{\text{sq}}(A;B)_\rho . \tag{4.3.5}$$

Since the choice of squashing channel was arbitrary, the first inequality follows.

We now prove the other inequality

$$F^{\text{sq}}(A;B)_\rho \leq \sup_{\mathcal{S}_{E'\to E}} F(A;B|E)_{\mathcal{S}(\psi)} . \tag{4.3.6}$$

Let ω_{ABE} be an extension of ρ_{AB}. Let φ_{ABEE_1} be a purification of ω_{ABE}, which is in turn also a purification of ρ_{AB}. Since all purifications are related by isometries acting on the purifying system, we know that there exists an isometry $U^\omega_{E'\to EE_1}$ (depending on ω) such that

$$|\varphi\rangle_{ABEE_1} = U^\omega_{E'\to EE_1} |\psi\rangle_{ABE'} . \tag{4.3.7}$$

Furthermore, we know that

$$\omega_{ABE} = \text{Tr}_{E_1}\left\{U^\omega_{E'\to EE_1}\psi_{ABE'}\left(U^\omega_{E'\to EE_1}\right)^\dagger\right\} \tag{4.3.8}$$

$$\equiv \mathcal{S}^\omega_{E'\to E}(\psi_{ABE'}) , \tag{4.3.9}$$

where we define the squashing channel $\mathcal{S}^\omega_{E'\to E}$ from the isometry $U^\omega_{E'\to EE_1}$. So this implies that

$$F(A;B|E)_\omega = F(A;B|E)_{\mathcal{S}^\omega(\psi)} \leq \sup_{\mathcal{S}_{E'\to E}} F(A;B|E)_{\mathcal{S}(\psi)} . \tag{4.3.10}$$

Since the inequality above holds for all extensions, the inequality in (4.3.6) follows. ■

The following statement is a direct consequence of Proposition 4.5:

Corollary 4.16. *The geometric squashed entanglement is monotone under local operations on both systems A and B:*

$$E_F^{\text{sq}}(A;B)_\rho \geq E_F^{\text{sq}}(A';B')_\tau , \tag{4.3.11}$$

where $\tau_{A'B'} \equiv (\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{AB})$. This is equivalent to

$$F^{\text{sq}}(A;B)_\rho \leq F^{\text{sq}}(A';B')_\tau . \tag{4.3.12}$$

Proof. Let ω_{ABE} be an arbitrary extension of ρ_{AB} and let

$$\theta_{A'B'E} \equiv (\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\omega_{ABE}) . \tag{4.3.13}$$

Then by the monotonicity of fidelity of recovery with respect to local quantum operations, we find that

$$F(A;B|E)_\omega \leq F(A';B'|E)_\theta \leq F^{\text{sq}}(A';B')_\tau . \tag{4.3.14}$$

Since the inequality holds for an arbitrary extension ω_{ABE} of ρ_{AB}, we can conclude that (4.3.12) holds and (4.3.11) follows by definition. ■

Proposition 4.17. *The geometric squashed entanglement is invariant with respect to local isometries, in the sense that*

$$E_F^{\rm sq}\left(A;B\right)_\rho = E_F^{\rm sq}(A';B')_\sigma, \tag{4.3.15}$$

where

$$\sigma_{A'B'} \equiv \left(\mathcal{U}_{A\to A'}\otimes\mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right) \tag{4.3.16}$$

and $\mathcal{U}_{A\to A'}$ *and* $\mathcal{V}_{B\to B'}$ *are isometric quantum channels.*

Proof. From Corollary 4.16, we can conclude that

$$E_F^{\rm sq}\left(A;B\right)_\rho \geq E_F^{\rm sq}(A';B')_\sigma. \tag{4.3.17}$$

Now let $\mathcal{T}^{\mathcal{U}}_{A'\to A}$ and $\mathcal{T}^{\mathcal{V}}_{B'\to B}$ be the quantum channels defined in (4.2.24). Again using Corollary 4.16, we find that

$$E_F^{\rm sq}(A';B')_\sigma \geq E_F^{\rm sq}(A;B)_{(\mathcal{T}^{\mathcal{U}}\otimes\mathcal{T}^{\mathcal{V}})(\sigma)} = E_F^{\rm sq}\left(A;B\right)_\rho, \tag{4.3.18}$$

where the equality follows from (4.2.25)-(4.2.26). ■

Proposition 4.18. *The geometric squashed entanglement obeys the following classical communication relations:*

$$E_F^{\rm sq}\left(AX_A;B\right)_\rho \leq E_F^{\rm sq}\left(AX_A;BX_B\right)_\rho = E_F^{\rm sq}\left(A;BX_B\right)_\rho, \tag{4.3.19}$$

for a state $\rho_{X_AX_BAB}$ *defined as*

$$\rho_{X_AX_BAB} \equiv \sum_x p_X\left(x\right)\left|x\right\rangle\left\langle x\right|_{X_A}\otimes\left|x\right\rangle\left\langle x\right|_{X_B}\otimes\rho^x_{AB}. \tag{4.3.20}$$

These are equivalent to

$$F^{\rm sq}\left(AX_A;B\right)_\rho \geq F^{\rm sq}\left(AX_A;BX_B\right)_\rho = F^{\rm sq}\left(A;BX_B\right)_\rho. \tag{4.3.21}$$

Proof. From monotonicity with respect to local operations, we find that

$$F^{\rm sq}\left(AX_A;BX_B\right)_\rho \leq F^{\rm sq}\left(AX_A;B\right)_\rho, \tag{4.3.22}$$

$$F^{\rm sq}\left(AX_A;BX_B\right)_\rho \leq F^{\rm sq}\left(A;BX_B\right)_\rho. \tag{4.3.23}$$

We now give a proof of the following inequality:

$$F^{\rm sq}\left(A;BX_B\right)_\rho \leq F^{\rm sq}\left(AX_A;BX_B\right)_\rho. \tag{4.3.24}$$

Let

$$\rho_{X_AX_BX_EABE} = \sum_x p_X\left(x\right)\left|x\right\rangle\left\langle x\right|_{X_A}\otimes\left|x\right\rangle\left\langle x\right|_{X_B}\otimes\left|x\right\rangle\left\langle x\right|_{X_E}\otimes\rho^x_{ABE}, \tag{4.3.25}$$

where ρ^x_{ABE} extends ρ^x_{AB}. Observe that $\rho_{X_AX_BX_EABE}$ is an extension of $\rho_{X_AX_BAB}$ and ρ_{X_BABE} is an arbitrary extension of ρ_{X_BAB}. Let $\mathcal{R}_{E\to AE}$ be an arbitrary recovery channel and let

$\mathcal{R}_{EX_E\to AX_AEX_E}$ be a channel that copies the value in X_E to X_A and applies $\mathcal{R}_{E\to AE}$ to system E. Consider that

$$F\left(\rho_{ABX_BE}, \mathcal{R}_{E\to AE}\left(\rho_{BX_BE}\right)\right) \tag{4.3.26}$$

$$= \left[\sum_x p_X(x)\sqrt{F}\left(\rho^x_{ABE}, \mathcal{R}_{E\to AE}\left(\rho^x_{BE}\right)\right)\right]^2 \tag{4.3.27}$$

$$= F\Bigg(\sum_x p_X(x)\left|xxx\right\rangle\left\langle xxx\right|_{X_AX_BX_E}\otimes\rho^x_{ABE}, \sum_x p_X(x)\left|xxx\right\rangle\left\langle xxx\right|_{X_AX_BX_E} \otimes\mathcal{R}_{E\to AE}\left(\rho^x_{BE}\right)\Bigg) \tag{4.3.28}$$

$$= F\left(\rho_{AX_ABX_BEX_E}, \mathcal{R}_{EX_E\to AX_AEX_E}\left(\rho_{BX_BEX_E}\right)\right) \tag{4.3.29}$$

$$\leq F^{\text{sq}}\left(AX_A; BX_B\right)_\rho. \tag{4.3.30}$$

The first two equalities are a consequence of the following property of fidelity:

$$\sqrt{F}\left(\tau_{ZS}, \omega_{ZS}\right) = \sum_z p_Z(z)\sqrt{F}\left(\tau^z_S, \omega^z_S\right), \tag{4.3.31}$$

where

$$\tau_{ZS} \equiv \sum_z p_Z(z)\left|z\right\rangle\left\langle z\right|_Z\otimes\tau^z_S, \qquad \omega_{ZS} \equiv \sum_z p_Z(z)\left|z\right\rangle\left\langle z\right|_Z\otimes\omega^z_S. \tag{4.3.32}$$

The third equality follows from the description of the map $\mathcal{R}_{EX_E\to AX_AEX_E}$ given above. The last inequality is a consequence of the definition of F^{sq} because $\rho_{AX_ABX_BEX_E}$ is a particular extension of ρ_{ABX_BE} and $\mathcal{R}_{EX_E\to AX_AEX_E}$ is a particular recovery map. Given that the chain of inequalities holds for all recovery maps $\mathcal{R}_{E\to AE}$ and extensions ρ_{ABX_BE} of ρ_{ABX_B}, we can conclude that

$$F^{\text{sq}}\left(A; BX_B\right)_\rho \leq F^{\text{sq}}\left(AX_A; BX_B\right)_\rho. \tag{4.3.33}$$

■

Remark 4.19. *The inequalities in Proposition 4.18 demonstrate that the geometric squashed entanglement is monotone non-increasing with respect to classical communication from Bob to Alice, but not necessarily the other way around. The essential idea in establishing the inequality $F^{\text{sq}}(A; BX_B)_\rho \leq F^{\text{sq}}(AX_A; BX_B)_\rho$ is to give a copy of the classical data to the party possessing the extension system and to have the recovery map give a copy to Alice. It is unclear to us whether the other inequality $F^{\text{sq}}(AX_A; B)_\rho \leq F^{\text{sq}}(AX_A; BX_B)_\rho$ could be established, given that the recovery operation only goes from an extension system to Alice, and so it appears that we have no way of giving a copy of this classical data to Bob.*

The following theorem is a direct consequence of Corollary 4.16 and Proposition 4.18:

Theorem 4.20. *The geometric squashed entanglement is a 1-LOCC monotone, in the sense that it is monotone non-increasing with respect to local operations and classical communication from Bob to Alice.*

Theorem 4.21. *The geometric squashed entanglement is convex, i.e.,*

$$\sum_x p_X(x)\, E_F^{\mathrm{sq}}(A;B)_{\rho^x} \geq E_F^{\mathrm{sq}}(A;B)_{\overline{\rho}}, \tag{4.3.34}$$

where

$$\overline{\rho}_{AB} \equiv \sum_x p_X(x)\, \rho_{AB}^x. \tag{4.3.35}$$

Proof. Let ρ_{ABE}^x be an extension of each ρ_{AB}^x, so that

$$\omega_{XABE} \equiv \sum_x p_X(x)\, |x\rangle \langle x|_X \otimes \rho_{ABE}^x \tag{4.3.36}$$

is some extension of $\overline{\rho}_{AB}$. Then the definition of $E_F^{\mathrm{sq}}(A;B)_{\overline{\rho}}$ and Proposition 4.11 give that

$$2E_F^{\mathrm{sq}}(A;B)_{\overline{\rho}} \leq I_F(A;B|EX)_\omega \leq \sum_x p_X(x)\, I_F(A;B|E)_{\rho^x}. \tag{4.3.37}$$

Since the inequality holds independent of each particular extension of ρ_{AB}^x, we can conclude (4.3.34). ■

Theorems 4.20 and 4.21 immediately lead to the following corollary:

Theorem 4.22. *The geometric squashed entanglement is faithful, in the sense that*

$$E_F^{\mathrm{sq}}(A;B)_\rho = 0 \textit{ if and only if } \rho_{AB} \textit{ is separable.} \tag{4.3.38}$$

This is equivalent to

$$F^{\mathrm{sq}}(A;B)_\rho = 1 \textit{ if and only if } \rho_{AB} \textit{ is separable.} \tag{4.3.39}$$

Furthermore, we have the following bound holding for all states:

$$E_F^{\mathrm{sq}}(A;B)_\rho \geq \frac{1}{512\,|A|^4} \left\|\rho_{AB} - \mathrm{SEP}(A:B)\right\|_1^4. \tag{4.3.40}$$

Proof. We first prove the if-part of the theorem. So, given by assumption that ρ_{AB} is separable, it has a decomposition of the following form:

$$\rho_{AB} = \sum_x p_X(x)\, |\psi_x\rangle \langle\psi_x|_A \otimes |\phi_x\rangle \langle\phi_x|_B. \tag{4.3.41}$$

Then an extension of the state is of the form

$$\rho_{ABE} = \sum_x p_X(x)\, |\psi_x\rangle \langle\psi_x|_A \otimes |\phi_x\rangle \langle\phi_x|_B \otimes |x\rangle \langle x|_E. \tag{4.3.42}$$

Clearly, if the system A becomes lost, someone who possesses system E could measure it and prepare the state $|\psi_x\rangle_A$ conditioned on the measurement outcome. That is, the recovery map $\mathcal{R}_{E\to AE}$ is as follows:

$$\mathcal{R}_{E\to AE}(\sigma_E) = \sum_x \langle x|\, \sigma_E\, |x\rangle \;\; |\psi_x\rangle \langle\psi_x|_A \otimes |x\rangle \langle x|_E. \tag{4.3.43}$$

So this implies that

$$F\left(\rho_{ABE}, \mathcal{R}_{E\to AE}\left(\rho_{BE}\right)\right) = 1, \tag{4.3.44}$$

and thus $F^{\mathrm{sq}}\left(A;B\right)_\rho = 1$.

The only-if-part of the theorem is a direct consequence of the reasoning in [199]. We repeat the argument from [199] here for the convenience of the reader. The reasoning from [199] establishes that the trace distance between ρ_{AB} and the set $\mathrm{SEP}(A:B)$ of separable states on systems A and B is bounded from above by a function of $-1/2\log F^{\mathrm{sq}}\left(A;B\right)_\rho$ and $|A|$. This will then allow us to conclude the only-if-part of the theorem.

Let

$$\varepsilon \equiv -1/2\log F^{\mathrm{sq}}\left(A;B\right)_\rho \tag{4.3.45}$$

for some bipartite state ρ_{AB} and let

$$\varepsilon_{\omega,\mathcal{R}} \equiv -1/2\log F(\omega_{ABE}, \mathcal{R}_{E\to AE}\left(\omega_{BE}\right)), \tag{4.3.46}$$

for some extension ω_{ABE} and a recovery map $\mathcal{R}_{E\to AE}$. By definition, we have that

$$\varepsilon = \inf_{\omega,\mathcal{R}_{E\to AE}} \varepsilon_{\omega,\mathcal{R}}. \tag{4.3.47}$$

Then consider that

$$\varepsilon_{\omega,\mathcal{R}} \geq \frac{1}{8}\left\|\omega_{ABE} - \mathcal{R}_{E\to AE}\left(\omega_{BE}\right)\right\|_1^2, \tag{4.3.48}$$

where the inequality follows from a well known relation between the fidelity and trace distance [66]. Therefore, by defining $\delta_{\omega,\mathcal{R}} = \sqrt{8\varepsilon_{\omega,\mathcal{R}}}$ we have that

$$\delta_{\omega,\mathcal{R}} \geq \left\|\omega_{ABE} - \mathcal{R}_{E\to AE}\left(\omega_{BE}\right)\right\|_1 \tag{4.3.49}$$

$$= \left\|\omega_{ABE} - \left(\mathcal{R}_{E\to A_2E}\circ \mathrm{Tr}_{A_1}\right)\left(\omega_{A_1BE}\right)\right\|_1, \tag{4.3.50}$$

where the systems A_1 and A_2 are defined to be isomorphic to system A. Now consider applying the same recovery map again. We then have that

$$\delta_{\omega,\mathcal{R}} \geq \left\|\left(\mathcal{R}_{E\to A_3E}\circ \mathrm{Tr}_{A_2}\right)\left(\omega_{A_2BE}\right) - \bigcirc_{i=2}^{3}\left(\mathcal{R}_{E\to A_iE}\circ \mathrm{Tr}_{A_{i-1}}\right)\left(\omega_{A_1BE}\right)\right\|_1, \tag{4.3.51}$$

which follows from the inequality above and monotonicity of the trace distance under the quantum operation $\mathcal{R}_{E\to A_3E}\circ\mathrm{Tr}_{A_2}$. Combining via the triangle inequality, we find for $k\geq 2$ that

$$\left\|\omega_{ABE} - \bigcirc_{i=2}^{3}\left(\mathcal{R}_{E\to A_iE}\circ \mathrm{Tr}_{A_{i-1}}\right)\left(\omega_{A_1BE}\right)\right\|_1 \leq 2\delta_{\omega,\mathcal{R}} \tag{4.3.52}$$

$$\leq k\delta_{\omega,\mathcal{R}}. \tag{4.3.53}$$

We can iterate this reasoning in the following way: For $j\in\{4,\ldots,k\}$ (assuming now $k\geq 4$), apply the maps $\mathcal{R}_{E\to A_jE}\circ\mathrm{Tr}_{A_{j-1}}$ along with monotonicity of trace distance to establish the following inequalities:

$$\left\|\left[\bigcirc_{i=3}^{j}\left(\mathcal{R}_{E\to A_iE}\circ \mathrm{Tr}_{A_{i-1}}\right)\left(\omega_{A_2BE}\right)\right] - \left[\bigcirc_{i=2}^{j}\left(\mathcal{R}_{E\to A_iE}\circ \mathrm{Tr}_{A_{i-1}}\right)\left(\omega_{A_1BE}\right)\right]\right\|_1 \leq \delta_{\omega,\mathcal{R}} \tag{4.3.54}$$

Apply the triangle inequality to all of these to establish the following inequalities for $j \in \{1, \ldots, k\}$:

$$\left\| \omega_{ABE} - \bigcirc_{i=2}^{j} \left(\mathcal{R}_{E \to A_i E} \circ \operatorname{Tr}_{A_{i-1}} \right) (\omega_{A_1 BE}) \right\|_1 \leq k\delta_{\omega,\mathcal{R}}, \tag{4.3.55}$$

with the interpretation for $j = 1$ that there is no map applied. From monotonicity of trace distance under quantum operations, we can then conclude the following inequalities for $j \in \{1, \ldots, k\}$:

$$\left\| \rho_{AB} - \operatorname{Tr}_E \left\{ \bigcirc_{i=2}^{j} \left(\mathcal{R}_{E \to A_i E} \circ \operatorname{Tr}_{A_{i-1}} \right) (\omega_{A_1 BE}) \right\} \right\|_1 \leq k\delta_{\omega,\mathcal{R}}. \tag{4.3.56}$$

Let $\gamma_{A_1 A_2 \cdots A_k BE}$ denote the following state:

$$\gamma_{A_1 A_2 \cdots A_k BE} \equiv \mathcal{R}_{E \to A_k E} \left(\cdots \left(\mathcal{R}_{E \to A_2 E} \left(\omega_{A_1 BE} \right) \right) \right). \tag{4.3.57}$$

(See Figure 4.3 for a graphical depiction of this state.) Then the inequalities in (4.3.56) are equivalent to the following inequalities for $j \in \{1 \ldots, k\}$:

$$\left\| \rho_{AB} - \gamma_{A_j B} \right\|_1 \leq k\delta_{\omega,\mathcal{R}}, \tag{4.3.58}$$

which are in turn equivalent to the following ones for any permutation $\pi \in S_k$:

$$\left\| \rho_{AB} - \operatorname{Tr}_{A_2 \cdots A_k} \left\{ W^{\pi}_{A_1 A_2 \cdots A_k} \gamma_{A_1 A_2 \cdots A_k B} \left(W^{\pi}_{A_1 A_2 \cdots A_k} \right)^{\dagger} \right\} \right\|_1 \leq k\delta_{\omega,\mathcal{R}}, \tag{4.3.59}$$

with $W^{\pi}_{A_1 A_2 \cdots A_k}$ a unitary representation of the permutation π. We can then define $\overline{\gamma}_{A_1 \cdots A_k B}$ as a symmetrized version of $\gamma_{A_1 \cdots A_k B}$:

$$\overline{\gamma}_{A_1 \cdots A_k B} \equiv \frac{1}{k!} \sum_{\pi \in S_k} W^{\pi}_{A_1 A_2 \cdots A_k} \gamma_{A_1 \cdots A_k B} \left(W^{\pi}_{A_1 A_2 \cdots A_k} \right)^{\dagger}. \tag{4.3.60}$$

The inequalities in (4.3.59) allow us to conclude that

$$k\delta_{\omega,\mathcal{R}} \geq \frac{1}{k!} \sum_{\pi \in S_k} \left\| \rho_{AB} - \operatorname{Tr}_{A_2 \cdots A_k} \left\{ W^{\pi}_{A_1 A_2 \cdots A_k} \gamma_{A_1 A_2 \cdots A_k B} \left(W^{\pi}_{A_1 A_2 \cdots A_k} \right)^{\dagger} \right\} \right\|_1 \tag{4.3.61}$$

$$\geq \left\| \rho_{AB} - \operatorname{Tr}_{A_2 \cdots A_k} \left\{ \frac{1}{k!} \sum_{\pi \in S_k} W^{\pi}_{A_1 A_2 \cdots A_k} \gamma_{A_1 A_2 \cdots A_k B} \left(W^{\pi}_{A_1 A_2 \cdots A_k} \right)^{\dagger} \right\} \right\|_1 \tag{4.3.62}$$

$$= \left\| \rho_{AB} - \overline{\gamma}_{A_1 B} \right\|_1, \tag{4.3.63}$$

where the second inequality is a consequence of the convexity of trace distance. So what the reasoning in [199] accomplishes is to construct a k-extendible state $\overline{\gamma}_{A_1 B}$ that is $k\delta_{\omega,\mathcal{R}}$-close to ρ_{AB} in trace distance.

Following [199], we now recall a particular quantum de Finetti result in [38, Theorem II.7']. Consider a state $\omega_{A_1 \cdots A_k B}$ which is permutation invariant with respect to systems $A_1 \cdots A_k$. Let $\omega_{A_1 \cdots A_n B}$ denote the reduced state on n of the k A systems where $n \leq k$. Then, for large k, $\omega_{A_1 \cdots A_n B}$ is close in trace distance to a convex combination of product states of the form $\int \sigma_A^{\otimes n} \otimes \tau(\sigma)_B \; d\mu(\sigma)$, where μ is a probability measure on the set of

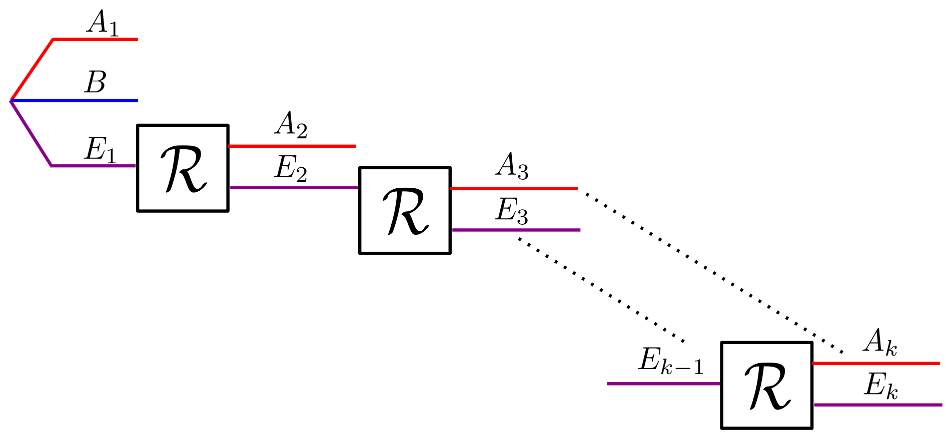

Figure 4.3: This figure illustrates the global state after performing a recovery map k times on system E.

mixed states on a single A system and $\{\tau(\sigma)\}_\sigma$ is a family of states parametrized by σ, with the approximation given by

$$\frac{2\,|A|^2\,n}{k} \geq \left\| \omega_{A_1\cdots A_n B} - \int \sigma_A^{\otimes n} \otimes \tau(\sigma)_B \;\, d\mu(\sigma) \right\|_1. \tag{4.3.64}$$

Applying this theorem in our context (choosing $n = 1$) leads to the following conclusion:

$$\frac{2\,|A|^2}{k} \geq \left\| \overline{\gamma}_{A_1 B} - \int \sigma_{A_1} \otimes \tau(\sigma)_B \;\, d\mu(\sigma) \right\|_1 \tag{4.3.65}$$

$$\geq \left\| \overline{\gamma}_{A_1 B} - \mathrm{SEP}(A_1 : B) \right\|_1, \tag{4.3.66}$$

because the state $\int \sigma_{A_1} \otimes \tau(\sigma)_B \;\, d\mu(\sigma)$ is a particular separable state.

We can now combine (4.3.63) and (4.3.66) with the triangle inequality to conclude the following bound

$$\|\rho_{AB} - \mathrm{SEP}(A : B)\|_1 \leq \frac{2|A|^2}{k} + k\delta_{\omega,\mathcal{R}}. \tag{4.3.67}$$

By choosing k to diverge slower than $\delta_{\omega,\mathcal{R}}^{-1}$, say as $k = |A|\sqrt{2/\delta_{\omega,\mathcal{R}}}$, we obtain the following bound:

$$\|\rho_{AB} - \mathrm{SEP}(A : B)\|_1 \leq |A|\,\sqrt{8\delta_{\omega,\mathcal{R}}} \tag{4.3.68}$$

$$= (512)^{1/4}\,|A|\,\varepsilon_{\omega,\mathcal{R}}^{1/4}. \tag{4.3.69}$$

Since the above bound holds for all extensions and recovery maps, we can obtain the tightest bound by taking an infimum over all of them. By substituting with (4.3.45) and (4.3.46), we find that

$$\|\rho_{AB} - \mathrm{SEP}(A : B)\|_1 \leq (512)^{1/4}\,|A|\left(-1/2\log F^{\mathrm{sq}}(A;B)_\rho\right)^{1/4}, \tag{4.3.70}$$

or equivalently

$$E_F^{\mathrm{sq}}(A;B)_\rho = -1/2\log F^{\mathrm{sq}}(A;B)_\rho \geq \frac{1}{512\,|A|^4}\,\|\rho_{AB} - \mathrm{SEP}(A : B)\|_1^4. \tag{4.3.71}$$

This proves the converse part of the faithfulness of the geometric squashed entanglement. ■

Proposition 4.23. *Let ϕ_{AB} be a bipartite pure state. Then*

$$E_F^{\mathrm{sq}}(A;B)_\phi = -\frac{1}{2}\log\sup_{|\varphi\rangle_A}\langle\phi|_{AB}(\varphi_A\otimes\phi_B)|\phi\rangle_{AB} \tag{4.3.72}$$

$$= -\frac{1}{2}\log\left\|\phi_A^2\right\|_\infty . \tag{4.3.73}$$

Any extension of a pure bipartite state is of the form $\phi_{AB}\otimes\omega_E$. Applying Proposition 4.12, we find that

$$F(A;B|E)_{\phi\otimes\omega} = F(A;B)_\phi \tag{4.3.74}$$

$$= \sup_{\sigma_A} F(\phi_{AB},\phi_B\otimes\sigma_A) \tag{4.3.75}$$

$$= \sup_{|\varphi\rangle_A}\langle\phi|_{AB}(\varphi_A\otimes\phi_B)|\phi\rangle_{AB} . \tag{4.3.76}$$

The last equality follows due to a convexity argument applied to

$$F(\phi_{AB},\phi_B\otimes\sigma_A) = \langle\phi|_{AB}\,\phi_B\otimes\sigma_A\,|\phi\rangle_{AB} . \tag{4.3.77}$$

Since the equality holds independent of any particular extension of ϕ_{AB}, we obtain (4.3.72) upon applying a negative logarithm and dividing by two. The other equality (4.3.73) follows because

$$\langle\phi|_{AB}(\varphi_A\otimes\phi_B)|\phi\rangle_{AB} = \langle\phi|_{AB}(\varphi_A\phi_A\otimes I_B)|\phi\rangle_{AB} \tag{4.3.78}$$

$$= \mathrm{Tr}\left\{|\phi\rangle\langle\phi|_{AB}(\varphi_A\phi_A\otimes I_B)\right\} \tag{4.3.79}$$

$$= \mathrm{Tr}\left\{\phi_A\varphi_A\phi_A\right\} \tag{4.3.80}$$

$$= \langle\varphi|_A\,\phi_A^2\,|\varphi\rangle_A . \tag{4.3.81}$$

Taking a supremum over all unit vectors $|\varphi\rangle_A$ then gives (4.3.73).

Proposition 4.24. *For a maximally entangled state Φ_{AB} of Schmidt rank d,*

$$E_F^{\mathrm{sq}}(A;B)_\Phi = \log d. \tag{4.3.82}$$

Proof. This follows directly from (4.3.73) of Proposition 4.23 because $\Phi_A = I_A/d$. ■

Proposition 4.25. *For a private state $\gamma_{ABA'B'}$ of $\log d$ private bits, the geometric squashed entanglement obeys the following bound:*

$$E_F^{\mathrm{sq}}(AA';BB')_\gamma \geq \log d. \tag{4.3.83}$$

Proof. The proof is in a similar spirit to the proof of [36, Proposition 4.19], but tailored to the fidelity of recovery quantity. Recall (2.1.4)-(2.1.7). Any extension $\gamma_{ABA'B'E}$ of a private state $\gamma_{ABA'B'}$ takes the form:

$$\gamma_{ABA'B'E} = U_{ABA'B'}(\Phi_{AB}\otimes\rho_{A'B'E})\,U_{ABA'B'}^\dagger, \tag{4.3.84}$$

where $\rho_{A'B'E}$ is an extension of $\rho_{A'B'}$. This is because the state Φ_{AB} is not extendible. Then consider that

$$F\left(AA';BB'|E\right)_{\gamma}=\sup_{\mathcal{R}}F\left(\gamma_{ABA'B'E},\mathcal{R}_{E\to AA'E}\left(\gamma_{BB'E}\right)\right), \tag{4.3.85}$$

where $\mathcal{R}_{E\to AA'E}$ is a recovery map. From (2.1.4)-(2.1.7), we can write

$$\gamma_{ABA'B'E}=\frac{1}{d}\sum_{i,j}|i\rangle\langle j|_{A}\otimes|i\rangle\langle j|_{B}\otimes V^{i}_{A'B'}\rho_{A'B'E}\left(V^{j}_{A'B'}\right)^{\dagger}, \tag{4.3.86}$$

which implies that

$$\gamma_{BB'E}=\frac{1}{d}\sum_{i}|i\rangle\langle i|_{B}\otimes\mathrm{Tr}_{\hat{A}'}\left\{V^{i}_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^{i}_{\hat{A}'B'}\right)^{\dagger}\right\}. \tag{4.3.87}$$

So then consider the fidelity of recovery for a particular recovery map $\mathcal{R}_{E\to AA'E}$:

$$\begin{aligned}
&F\left(\gamma_{ABA'B'E},\mathcal{R}_{E\to AA'E}\left(\gamma_{BB'E}\right)\right)\\
&=F\Bigg(U_{ABA'B'}\left(\Phi_{AB}\otimes\rho_{A'B'E}\right)U^{\dagger}_{ABA'B'},\\
&\frac{1}{d}\sum_{i}|i\rangle\langle i|_{B}\otimes\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^{i}_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^{i}_{\hat{A}'B'}\right)^{\dagger}\right\}\right)\Bigg) &(4.3.88)\\
&=F\Bigg(\left(\Phi_{AB}\otimes\rho_{A'B'E}\right),\\
&U^{\dagger}_{ABA'B'}\left[\frac{1}{d}\sum_{i}|i\rangle\langle i|_{B}\otimes\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^{i}_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^{i}_{\hat{A}'B'}\right)^{\dagger}\right\}\right)\right]U_{ABA'B'}\Bigg), &(4.3.89)
\end{aligned}$$

where the second equality follows from invariance of the fidelity under unitaries. Then consider that

$$\begin{aligned}
&U^{\dagger}_{ABA'B'}\left[\frac{1}{d}\sum_{i}|i\rangle\langle i|_{B}\otimes\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^{i}_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^{i}_{\hat{A}'B'}\right)^{\dagger}\right\}\right)\right]U_{ABA'B'}\\
&=\left(I_{A}\otimes\sum_{j}|j\rangle\langle j|_{B}\otimes\left(V^{j}_{A'B'}\right)^{\dagger}\right)\left[\frac{1}{d}\sum_{i}|i\rangle\langle i|_{B}\otimes\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^{i}_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^{i}_{\hat{A}'B'}\right)^{\dagger}\right\}\right)\right]\\
&\times\left(I_{A}\otimes\sum_{j'}|j'\rangle\langle j'|_{B}\otimes V^{j'}_{A'B'}\right) &(4.3.90)\\
&=\frac{1}{d}\sum_{i}|i\rangle\langle i|_{B}\otimes\left(V^{i}_{A'B'}\right)^{\dagger}\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^{i}_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^{i}_{\hat{A}'B'}\right)^{\dagger}\right\}\right)V^{i}_{A'B'}. &(4.3.91)
\end{aligned}$$

If we trace over systems $A'B'$, the fidelity only goes up, so consider that the state above becomes as follows under this partial trace:

$$\frac{1}{d}\sum_i |i\rangle\langle i|_B \otimes \mathrm{Tr}_{A'B'}\left\{\left(V^i_{A'B'}\right)^\dagger \mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^i_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^i_{\hat{A}'B'}\right)^\dagger\right\}\right)V^i_{A'B'}\right\}$$

$$= \frac{1}{d}\sum_i |i\rangle\langle i|_B \otimes \mathrm{Tr}_{A'B'}\left\{\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'}\left\{V^i_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^i_{\hat{A}'B'}\right)^\dagger\right\}\right)\right\} \tag{4.3.92}$$

$$= \frac{1}{d}\sum_i |i\rangle\langle i|_B \otimes \mathrm{Tr}_{A'}\left\{\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'B'}\left\{V^i_{\hat{A}'B'}\rho_{\hat{A}'B'E}\left(V^i_{\hat{A}'B'}\right)^\dagger\right\}\right)\right\} \tag{4.3.93}$$

$$= \frac{1}{d}\sum_i |i\rangle\langle i|_B \otimes \mathrm{Tr}_{A'}\left\{\mathcal{R}_{E\to AA'E}\left(\mathrm{Tr}_{\hat{A}'B'}\left\{\rho_{\hat{A}'B'E}\right\}\right)\right\} \tag{4.3.94}$$

$$= \frac{1}{d}\sum_i |i\rangle\langle i|_B \otimes \mathrm{Tr}_{A'}\left\{\mathcal{R}_{E\to AA'E}\left(\rho_E\right)\right\} \tag{4.3.95}$$

$$= \pi_B \otimes \mathcal{R}_{E\to AE}\left(\rho_E\right), \tag{4.3.96}$$

where π_B is a maximally mixed state on system B. So an upper bound on (4.3.89) is given by

$$F\left(\Phi_{AB}\otimes\rho_E, \pi_B\otimes\mathcal{R}_{E\to AE}\left(\rho_E\right)\right) \leq F\left(\Phi_{AB}, \pi_B\otimes\mathcal{R}_{E\to A}\left(\rho_E\right)\right) \tag{4.3.97}$$

$$= 1/d^2. \tag{4.3.98}$$

Since this upper bound is universal for any recovery map and any extension of the original state, we obtain the following inequality:

$$\sup_{\substack{\gamma_{ABA'B'E}:\\ \gamma_{ABA'B'}=\mathrm{Tr}_E\{\gamma_{ABA'B'E}\}}} F\left(AA';BB'|E\right)_\gamma \leq 1/d^2. \tag{4.3.99}$$

After taking a negative logarithm, we recover the statement of the proposition. ■

Proposition 4.26. *Let* $\omega_{A_1B_1A_2B_2} \equiv \rho_{A_1B_1}\otimes\sigma_{A_2B_2}$. *Then*

$$E_F^{\mathrm{sq}}\left(A_1A_2;B_1B_2\right)_\omega \leq E_F^{\mathrm{sq}}\left(A_1;B_1\right)_\rho + E_F^{\mathrm{sq}}\left(A_2;B_2\right)_\sigma, \tag{4.3.100}$$

which is equivalent to

$$F^{\mathrm{sq}}\left(A_1;B_1\right)_\rho \cdot F^{\mathrm{sq}}\left(A_2;B_2\right)_\tau \leq F^{\mathrm{sq}}\left(A_1A_2;B_1B_2\right)_{\rho\otimes\tau}. \tag{4.3.101}$$

Proof. Let $\rho_{A_1B_1E_1}$ be an extension of $\rho_{A_1B_1}$ and let $\tau_{A_2B_2E_2}$ be an extension of $\tau_{A_2B_2}$. Let $\mathcal{R}^1_{E_1\to A_1E_1}$ and $\mathcal{R}^2_{E_2\to A_2E_2}$ be recovery maps. Then

$$F\left(\rho_{A_1B_1E_1}, \mathcal{R}^1_{E_1\to A_1E_1}\left(\rho_{B_1E_1}\right)\right)\cdot F\left(\tau_{A_2B_2E_2}, \mathcal{R}^2_{E_2\to A_2E_2}\left(\tau_{B_2E_2}\right)\right)$$

$$= F\left(\rho_{A_1B_1E_1}\otimes\tau_{A_2B_2E_2}, \mathcal{R}^1_{E_1\to A_1E_1}\left(\rho_{B_1E_1}\right)\otimes\mathcal{R}^2_{E_2\to A_2E_2}\left(\tau_{B_2E_2}\right)\right) \tag{4.3.102}$$

$$\leq \sup_{\omega_{A_1A_2B_1B_2E}} \sup_{\mathcal{R}_{E\to A_1A_2E}}$$

$$\left\{F\left(\omega_{A_1A_2B_1B_2E}, \mathcal{R}_{E\to A_1A_2E}\left(\omega_{B_1B_2E}\right)\right) : \rho_{A_1B_1}\otimes\tau_{A_2B_2} = \mathrm{Tr}_E\left\{\omega_{A_1A_2B_1B_2E}\right\}\right\} \tag{4.3.103}$$

$$= F^{\mathrm{sq}}\left(A_1A_2;B_1B_2\right)_{\rho\otimes\tau} \tag{4.3.104}$$

Since the inequality holds for all extensions $\rho_{A_1B_1E_1}$ and $\tau_{A_2B_2E_2}$ and recovery maps $\mathcal{R}^1_{E_1\to A_1E_1}$ and $\mathcal{R}^2_{E_2\to A_2E_2}$, we can conclude that

$$F^{\text{sq}}\left(A_1;B_1\right)_\rho \cdot F^{\text{sq}}\left(A_2;B_2\right)_\tau \leq F^{\text{sq}}\left(A_1A_2;B_1B_2\right)_{\rho\otimes\tau} \tag{4.3.105}$$

By taking negative logarithms and dividing by 1/2, we arrive at the subadditivity statement for E^{sq}_F. ■

Proposition 4.27. *The geometric squashed entanglement is a continuous function of its input. That is, given two bipartite states ρ_{AB} and σ_{AB} such that $F\left(\rho_{AB},\sigma_{AB}\right)\geq 1-\varepsilon$ where $\varepsilon\in[0,1]$, then the following inequalities hold*

$$\left|F^{\text{sq}}\left(A;B\right)_\rho - F^{\text{sq}}\left(A;B\right)_\sigma\right| \leq 8\sqrt{\varepsilon}, \tag{4.3.106}$$

$$\left|E^{\text{sq}}_F\left(A;B\right)_\rho - E^{\text{sq}}_F\left(A;B\right)_\sigma\right| \leq 4\left|A\right|^2\sqrt{\varepsilon}. \tag{4.3.107}$$

Proof. One of the main tools for our proof is the purified distance [180, Definition 4], defined for two quantum states as

$$P\left(\rho,\sigma\right)\equiv\sqrt{1-F\left(\rho,\sigma\right)}, \tag{4.3.108}$$

and which for our case implies that

$$P\left(\rho_{AB},\sigma_{AB}\right)\leq\sqrt{\varepsilon}. \tag{4.3.109}$$

Letting σ_{ABE} be an arbitrary extension of σ_{AB}, [180, Corollary 9] implies that there exists an extension ρ_{ABE} of ρ_{AB} such that

$$P\left(\rho_{ABE},\sigma_{ABE}\right)=P\left(\rho_{AB},\sigma_{AB}\right)\leq\sqrt{\varepsilon}. \tag{4.3.110}$$

Let $\mathcal{R}_{E\to AE}$ be an arbitrary recovery map. Then the above and monotonicity of the purified distance under quantum operations [180, Lemma 7] imply that

$$P\left(\mathcal{R}_{E\to AE}\left(\rho_{BE}\right),\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right)\right)\leq P\left(\rho_{ABE},\sigma_{ABE}\right)\leq\sqrt{\varepsilon}. \tag{4.3.111}$$

So consider that the triangle inequality for purified distance [180, Lemma 5] implies that

$$\begin{aligned}
P\left(\rho_{ABE},\mathcal{R}_{E\to AE}\left(\rho_{BE}\right)\right) &\leq P\left(\rho_{ABE},\sigma_{ABE}\right)+P\left(\sigma_{ABE},\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right)\right)\\
&\quad + P\left(\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right),\mathcal{R}_{E\to AE}\left(\rho_{BE}\right)\right) && (4.3.112)\\
&\leq\sqrt{\varepsilon}+P\left(\sigma_{ABE},\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right)\right)+\sqrt{\varepsilon} && (4.3.113)\\
&=P\left(\sigma_{ABE},\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right)\right)+2\sqrt{\varepsilon}. && (4.3.114)
\end{aligned}$$

This is equivalent to

$$\sqrt{1-F\left(\rho_{ABE},\mathcal{R}_{E\to AE}\left(\rho_{BE}\right)\right)}\leq\sqrt{1-F\left(\sigma_{ABE},\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right)\right)}+2\sqrt{\varepsilon} \tag{4.3.115}$$

which upon squaring gives

$$1-F\left(\rho_{ABE},\mathcal{R}_{E\to AE}\left(\rho_{BE}\right)\right)\leq 1-F\left(\sigma_{ABE},\mathcal{R}_{E\to AE}\left(\sigma_{BE}\right)\right)+8\sqrt{\varepsilon}, \tag{4.3.116}$$

where we used that $F(\rho,\sigma) \in [0,1]$ and $\varepsilon \leq \sqrt{\varepsilon}$ for $\varepsilon \in [0,1]$. This in turn implies the following inequality

$$F(\rho_{ABE}, \mathcal{R}_{E\to AE}(\rho_{BE})) + 8\sqrt{\varepsilon} \geq F(\sigma_{ABE}, \mathcal{R}_{E\to AE}(\sigma_{BE})). \tag{4.3.117}$$

By taking a supremum, we find that

$$F^{\text{sq}}(A;B)_\rho + 8\sqrt{\varepsilon} \geq F(\sigma_{ABE}, \mathcal{R}_{E\to AE}(\sigma_{BE})). \tag{4.3.118}$$

Since the extension of σ_{AB} and the recovery map $\mathcal{R}_{E\to AE}$ were arbitrary, it follows that

$$F^{\text{sq}}(A;B)_\rho + 8\sqrt{\varepsilon} \geq F^{\text{sq}}(A;B)_\sigma. \tag{4.3.119}$$

By a similar argument (but tailoring an extension of σ_{ABE} to an arbitrary extension of ρ_{AB}), we can conclude the other inequality

$$F^{\text{sq}}(A;B)_\sigma + 8\sqrt{\varepsilon} \geq F^{\text{sq}}(A;B)_\rho, \tag{4.3.120}$$

which gives us (4.3.106).

By dividing (4.3.119) by $F^{\text{sq}}(A;B)_\rho$ and taking a logarithm, we find that

$$\log\left(\frac{F^{\text{sq}}(A;B)_\sigma}{F^{\text{sq}}(A;B)_\rho}\right) \leq \log\left(1 + \frac{8\sqrt{\varepsilon}}{F^{\text{sq}}(A;B)_\rho}\right) \tag{4.3.121}$$

$$\leq \frac{8\sqrt{\varepsilon}}{F^{\text{sq}}(A;B)_\rho} \tag{4.3.122}$$

$$\leq |A|^2\, 8\sqrt{\varepsilon}. \tag{4.3.123}$$

where we used that $\log(x+1) \leq x$ and the dimension bound from Proposition 4.9. Applying this to the other inequality in (4.3.120) gives that

$$\log\left(\frac{F^{\text{sq}}(A;B)_\rho}{F^{\text{sq}}(A;B)_\sigma}\right) \leq |A|^2\, 8\sqrt{\varepsilon}, \tag{4.3.124}$$

from which we can conclude (4.3.107) upon dividing both sides by 1/2. ■

4.4 Surprisal of Measurement Recoverability

In this section, we propose an alternative measure of quantum correlations, the *surprisal of measurement recoverability*, which follows the original motivation behind the quantum discord [207]. However, our measure has a clear operational meaning in the "one-shot" setting, being based on how well one can recover a bipartite quantum state if one system is measured.

Recall the definition of quantum discord from Definition 3.16. Similarly, we define the surprisal of measurement recoverability as follows.

Definition 4.28. *We define the following information quantity:*

$$D_F\left(\overline{A};B\right)_\rho \equiv \inf_{\{\Lambda^x\}} I_F\left(E;B|X\right)_\sigma, \tag{4.4.1}$$

where we have simply substituted the QCMI in (3.3.11) *with* I_F*. Writing out the right-hand side of* (4.4.1) *carefully, we find that*

$$D_F\left(\overline{A};B\right) = -\log \sup_{\mathcal{U}^{\mathcal{M}}_{A\to XE},\mathcal{R}_{X\to XE}} F\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right), \mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right), \tag{4.4.2}$$

where $\mathcal{M}_{A\to X}$ *is defined in* (3.3.3)*,* $U^{\mathcal{M}}_{A\to XE}$ *is defined in* (3.3.4)*, and* $\mathcal{U}^{\mathcal{M}}_{A\to XE}$ *is defined in* (3.3.7)*.*

This quantity has a similar interpretation as the original discord, as summarized in the following quote from [207]:

> "A vanishing discord can be considered as an indicator of the superselection rule, or — in the case of interest — its value is a measure of the efficiency of einselection. When [the discord] is large for any measurement, a lot of information is missed and destroyed by any measurement on the apparatus alone, but when [the discord] is small almost all the information about [the system] that exists in the [system–apparatus] correlations is locally recoverable from the state of the apparatus."

Indeed, we can rewrite D_F as characterizing how well a bipartite state ρ_{AB} is preserved when an entanglement-breaking channel [95] acts on the A system:

Proposition 4.29. *For a bipartite state* ρ_{AB}*, we have the following equality:*

$$D_F\left(\overline{A};B\right) = -\log \sup_{\mathcal{E}_A} F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right), \tag{4.4.3}$$

where the optimization on the right-hand side is over the convex set of entanglement-breaking channels acting on the system A*.*

Proof. We begin by establishing that

$$\sup_{\mathcal{U}^{\mathcal{M}}_{A\to XE},\mathcal{R}_{X\to XE}} F\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right), \mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right) \leq \sup_{\mathcal{E}_A} F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right). \tag{4.4.4}$$

Let $\mathcal{M}_{A\to X}$ be any measurement map, let $U^{\mathcal{M}}_{A\to XE}$ be an isometric extension for it, and let $\mathcal{R}_{X\to XE}$ be any recovery map. Let $\mathcal{T}_{XE\to A}$ denote the following quantum channel:

$$\mathcal{T}_{XE\to A}\left(\gamma_{XE}\right) \equiv \left(U^{\mathcal{M}}\right)^\dagger \gamma_{XE} U^{\mathcal{M}} + \text{Tr}\left\{\left(I - U^{\mathcal{M}}\left(U^{\mathcal{M}}\right)^\dagger\right)\gamma_{XE}\right\}\sigma_A, \tag{4.4.5}$$

where σ_A is some state on the system A. Observe that

$$\left(\mathcal{T}_{XE\to A}\circ \mathcal{U}^{\mathcal{M}}_{A\to XE}\right)\left(\rho_{AB}\right) = \rho_{AB}. \tag{4.4.6}$$

Then consider that

$$\begin{aligned}
&F\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right),\mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right)\\
&\le F\left(\mathcal{T}_{XE\to A}\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right)\right),\mathcal{T}_{XE\to A}\left(\mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right)\right) &(4.4.7)\\
&= F\left(\rho_{AB},\mathcal{T}_{XE\to A}\left(\mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right)\right) &(4.4.8)\\
&\le \sup_{\mathcal{E}_A} F\left(\rho_{AB},\mathcal{E}_A\left(\rho_{AB}\right)\right). &(4.4.9)
\end{aligned}$$

The first inequality is a consequence of the monotonicity of fidelity under quantum operations and the last follows because any entanglement breaking channel can be written as a concatenation of a measurement followed by a preparation. In the third line, the measurement is $\mathcal{M}_{A\to X}$ and the preparation is $\mathcal{T}_{XE\to A}\circ\mathcal{R}_{X\to XE}$.

We now prove the other inequality:

$$\sup_{U^{\mathcal{M}}_{A\to XE},\mathcal{R}_{X\to XE}} F\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right),\mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right) \ge \sup_{\mathcal{E}_A} F\left(\rho_{AB},\mathcal{E}_A\left(\rho_{AB}\right)\right). \quad (4.4.10)$$

Let $\mathcal{E}_A$ be any entanglement-breaking channel, which consists of a measurement $\mathcal{M}_{A\to X}$ followed by a preparation $\mathcal{P}_{X\to A}$. Let $U^{\mathcal{M}}_{A\to XE}$ be an isometric extension of the measurement map. Then consider that

$$\begin{aligned}
F\left(\rho_{AB},\mathcal{E}_A\left(\rho_{AB}\right)\right) &= F\left(\rho_{AB},\mathcal{P}_{X\to A}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right) &(4.4.11)\\
&= F\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right),\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\mathcal{P}_{X\to A}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right)\right) &(4.4.12)\\
&\le \sup_{U^{\mathcal{M}}_{A\to XE},\mathcal{R}_{X\to XE}} F\left(\mathcal{U}^{\mathcal{M}}_{A\to XE}\left(\rho_{AB}\right),\mathcal{R}_{X\to XE}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right), &(4.4.13)
\end{aligned}$$

where the inequality follows because $\mathcal{U}^{\mathcal{M}}_{A\to XE}\circ\mathcal{P}_{X\to A}$ is a particular recovery map. So (4.4.10) follows and this concludes the proof. ∎

The proof follows the interpretation given in the quote above: the measurement map $\mathcal{M}_{A\to X}$ is performed on the A system of the state ρ_{AB}, which is followed by a recovery map $\mathcal{P}_{X\to A}$ that attempts to recover the A system from the state of the measuring apparatus. Since the measurement map has a classical output, any recovery map acting on such a classical system is equivalent to a preparation map. So the quantity $D_F\left(\overline{A};B\right)$ captures how difficult it is to recover the full bipartite state after some measurement is performed on it, following the original spirit of the quantum discord. However, the quantity $D_F\left(\overline{A};B\right)$ defined above has the advantage of being a "one-shot" measure, given that the fidelity has a clear operational meaning in a "one-shot" setting. If $D_F\left(\overline{A};B\right)$ is near to zero, then $F\left(\rho_{AB},\left(\mathcal{P}_{X\to A}\left(\mathcal{M}_{A\to X}\left(\rho_{AB}\right)\right)\right)\right)$ is close to one, so that it is possible to recover the system A by performing a recovery map on the state of the apparatus. Conversely, if $D_F\left(\overline{A};B\right)$ is far from zero, then the measurement recoverability is far from one, so that it is not possible to recover system A from the state of the measuring apparatus.

The observation in Proposition 4.29 leads to the following proposition, which characterizes quantum states with discord nearly equal to zero.

Proposition 4.30. *A bipartite quantum state ρ_{AB} has quantum discord nearly equal to zero if and only if it is an approximate fixed point of an entanglement breaking channel. More* *precisely, we have the following: If there exists an entanglement breaking channel $\mathcal{E}_A$ and $\varepsilon \in [0,1]$ such that*

$$\left\|\rho_{AB} - \mathcal{E}_A\left(\rho_{AB}\right)\right\|_1 \leq \varepsilon, \tag{4.4.14}$$

then the quantum discord $D\left(\overline{A};B\right)_\rho$ obeys the following bound

$$D\left(\overline{A};B\right)_\rho \leq 4h_2\left(\varepsilon\right) + 8\varepsilon \log\left|A\right|, \tag{4.4.15}$$

where $h_2\left(\varepsilon\right)$ is the binary entropy with the property that $\lim_{\varepsilon \searrow 0} h_2\left(\varepsilon\right) = 0$. Conversely, if the quantum discord $D\left(\overline{A};B\right)_\rho$ obeys the following bound for $\varepsilon \in [0,1]$:

$$D\left(\overline{A};B\right)_\rho \leq \varepsilon, \tag{4.4.16}$$

then there exists an entanglement breaking channel $\mathcal{E}_A$ such that

$$\left\|\rho_{AB} - \mathcal{E}_A\left(\rho_{AB}\right)\right\|_1 \leq 2\sqrt{\varepsilon}. \tag{4.4.17}$$

Proof. We begin by proving (4.4.14)-(4.4.15). Since any entanglement breaking channel $\mathcal{E}_A$ consists of a measurement map $\mathcal{M}_{A\to X}$ followed by a preparation map $\mathcal{P}_{X\to A}$, we can write $\mathcal{E}_A = \mathcal{P}_{X\to A} \circ \mathcal{M}_{A\to X}$. Then consider that

$$D\left(\overline{A};B\right)_\rho = I\left(A;B\right)_\rho - \sup_{\{\Lambda^x\}} I\left(X;B\right)_\sigma \tag{4.4.18}$$

$$\leq I\left(A;B\right)_\rho - I\left(X;B\right)_{\mathcal{M}(\rho)} \tag{4.4.19}$$

$$\leq I\left(A;B\right)_\rho - I\left(A;B\right)_{\mathcal{P}\circ\mathcal{M}(\rho)} \tag{4.4.20}$$

$$= I\left(A;B\right)_\rho - I\left(A;B\right)_{\mathcal{E}(\rho)} \tag{4.4.21}$$

$$\leq 4h_2\left(\varepsilon\right) + 8\varepsilon \log\left|A\right|. \tag{4.4.22}$$

The first inequality follows because the measurement given by $\mathcal{M}_{A\to X}$ is not necessarily optimal. The second inequality is a consequence of the quantum data processing inequality, in which quantum mutual information is non-increasing under the local operation $\mathcal{P}_{X\to A}$. The last equality follows because $\mathcal{E}_A = \mathcal{P}_{X\to A} \circ \mathcal{M}_{A\to X}$. The last inequality is a consequence of the Alicki-Fannes inequality [4].

We now prove (4.4.16)-(4.4.17). The Fawzi-Renner inequality

$$I(A;B|C)_\rho \geq -\log F(A;B|C)_\rho \tag{4.4.23}$$

which holds for any tripartite state ρ_{ABC} [62], combined with other observations recalled in this section connecting discord with QCMI, gives us that there exists an entanglement breaking channel $\mathcal{E}_A$ such that

$$D\left(\overline{A};B\right)_\rho \geq -\log F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right) \tag{4.4.24}$$

$$\geq -\log\left(1 - \frac{1}{4}\left\|\rho_{AB} - \mathcal{E}_A\left(\rho_{AB}\right)\right\|_1^2\right) \tag{4.4.25}$$

$$\geq \frac{1}{4}\left\|\rho_{AB} - \mathcal{E}_A\left(\rho_{AB}\right)\right\|_1^2, \tag{4.4.26}$$

where the second inequality follows from well known relations between trace distance and fidelity [66] and the last from $-\log\left(1-x\right) \geq x$, valid for $x \leq 1$. This is sufficient to conclude (4.4.16)-(4.4.17). ■

Remark 4.31. *The main conclusion we can take from Proposition 4.30 is that quantum states with discord nearly equal to zero are such that they are recoverable after performing some measurement on one share of them, making precise the quote from [207] given above. In prior work [78, Lemma 8.12], quantum states with discord exactly equal to zero were characterized as being entirely classical on the system being measured, but this condition is perhaps too restrictive for characterizing states with discord approximately equal to zero.*

Remark 4.32. *In prior work, discord-like measures of the following form have been widely considered throughout the literature [129]:*

$$\inf_{\chi_{AB}\in CQ} \Delta\left(\rho_{AB}, \chi_{AB}\right), \tag{4.4.27}$$

$$\inf_{\chi_{AB}\in CC} \Delta\left(\rho_{AB}, \chi_{AB}\right), \tag{4.4.28}$$

where CQ and CC are the respective sets of classical-quantum and classical-classical states and Δ is some suitable (pseudo-)distance measure such as relative entropy, trace distance, or Hilbert-Schmidt distance. The larger message of Proposition 4.30 is that it seems more reasonable from the physical perspective argued in this section and in the original discord paper [207] to consider discord-like measures of the following form:

$$\inf_{\mathcal{E}_A} \Delta\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right), \tag{4.4.29}$$

$$\inf_{\mathcal{E}_A,\mathcal{E}_B} \Delta\left(\rho_{AB}, \left(\mathcal{E}_A\otimes\mathcal{E}_B\right)\left(\rho_{AB}\right)\right), \tag{4.4.30}$$

where the optimization is over the convex set of entanglement breaking channels and Δ is again some suitable (pseudo-)distance measure as mentioned above. One can understand these measures as being a special case of the proposed measures in [146], but we stress here that we arrived at them independently through the line of reasoning given in this section.

We now establish some properties of the surprisal of measurement recoverability:

Proposition 4.33. $D_F\left(\overline{A};B\right)_\rho$ *is invariant under local isometries, in the sense that*

$$D_F\left(\overline{A};B\right)_\rho = D_F(\overline{A'};B')_\sigma, \tag{4.4.31}$$

where

$$\sigma_{A'B'} \equiv \left(\mathcal{U}_{A\to A'}\otimes\mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right) \tag{4.4.32}$$

and $\mathcal{U}_{A\to A'}$ *and* $\mathcal{V}_{B\to B'}$ *are isometric CPTP maps.*

Proof. Let $\mathcal{E}_A$ be some entanglement-breaking channel and let $U_{A\to A'}$ and $V_{B\to B'}$ denote the local isometries, with corresponding isometric maps $\mathcal{U}_{A\to A'}$ and $\mathcal{V}_{B\to B'}$. Let $\mathcal{T}_{A'\to A}$ and $\mathcal{T}_{B'\to B}$ denote the following CPTP maps:

$$\mathcal{T}_{A'\to A}\left(\omega_{A'}\right) \equiv U^\dagger\omega_{A'}U + \operatorname{Tr}\left\{\left(I_{A'} - UU^\dagger\right)\omega_{A'}\right\}\tau_A, \tag{4.4.33}$$

$$\mathcal{T}_{B'\to B}\left(\omega_{B'}\right) \equiv V^\dagger\omega_{B'}V + \operatorname{Tr}\left\{\left(I_{B'} - VV^\dagger\right)\omega_{B'}\right\}\tau_B, \tag{4.4.34}$$

where τ_A and τ_B are some states on systems A and B, respectively. Observe that

$$\mathcal{T}_{A'\to A} \circ \mathcal{U}_{A\to A'} = \mathrm{id}_A, \tag{4.4.35}$$

$$\mathcal{T}_{B'\to B} \circ \mathcal{V}_{B\to B'} = \mathrm{id}_B, \tag{4.4.36}$$

where id denotes the identity map. Then from invariance of fidelity under isometries and the above fact, we find that

$$F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right)$$

$$= F\left(\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right), \left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\mathcal{E}_A\left(\rho_{AB}\right)\right)\right) \tag{4.4.37}$$

$$= F\left(\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right), \left(\mathcal{U}_{A\to A'} \circ \mathcal{E}_A \circ \mathcal{T}_{A'\to A}\right)\left[\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right)\right]\right) \tag{4.4.38}$$

$$\leq \sup_{\mathcal{E}_{A'}} F\left(\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right), \mathcal{E}_{A'}\left(\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right)\right)\right). \tag{4.4.39}$$

Since the inequality is true for any entanglement breaking channel $\mathcal{E}_A$, we find after applying a negative logarithm that

$$D_F\left(\overline{A}; B\right)_\rho \geq D_F\left(\overline{A}; B\right)_{(\mathcal{U}\otimes\mathcal{V})(\rho)}. \tag{4.4.40}$$

Now consider that

$$F\left(\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right), \mathcal{E}_{A'}\left[\left(\mathcal{U}_{A\to A'} \otimes \mathcal{V}_{B\to B'}\right)\left(\rho_{AB}\right)\right]\right)$$

$$= F\left(\mathcal{U}_{A\to A'}\left(\rho_{AB}\right), \left(\mathcal{E}_{A'} \circ \mathcal{U}_{A\to A'}\right)\left(\rho_{AB}\right)\right) \tag{4.4.41}$$

$$\leq F\left(\left(\mathcal{T}_{A'\to A} \circ \mathcal{U}_{A\to A'}\right)\left(\rho_{AB}\right), \left(\mathcal{T}_{A'\to A} \circ \mathcal{E}_{A'} \circ \mathcal{U}_{A\to A'}\right)\left(\rho_{AB}\right)\right) \tag{4.4.42}$$

$$= F\left(\rho_{AB}, \left(\mathcal{T}_{A'\to A} \circ \mathcal{E}_{A'} \circ \mathcal{U}_{A\to A'}\right)\left(\rho_{AB}\right)\right) \tag{4.4.43}$$

$$\leq \sup_{\mathcal{E}_A} F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right). \tag{4.4.44}$$

Since the inequality is true for any entanglement breaking channel $\mathcal{E}_{A'}$, we find after applying a negative logarithm that

$$D_F\left(\overline{A}; B\right)_\rho \leq D_F\left(\overline{A}; B\right)_{(\mathcal{U}\otimes\mathcal{V})(\rho)}, \tag{4.4.45}$$

which gives the statement of the proposition. ■

Proposition 4.34. *The surprisal of measurement recoverability $D_F\left(\overline{A}; B\right)_\rho$ is equal to zero if and only if ρ_{AB} is a classical-quantum state, having the form*

$$\rho_{AB} = \sum_x p_X\left(x\right) |x\rangle \langle x|_A \otimes \rho_B^x, \tag{4.4.46}$$

for some orthonormal basis $\{|x\rangle\}$, probability distribution $p_X\left(x\right)$, and states $\{\rho_B^x\}$.

Proof. Suppose that the state is classical-quantum. Then it is a fixed point of the entanglement breaking map $\sum_x |x\rangle \langle x|_A \left(\cdot\right) |x\rangle \langle x|_A$, so that the fidelity of measurement recovery is equal to one and its surprisal is equal to zero. On the other hand, suppose that $D_F\left(\overline{A}; B\right)_\rho = 0$. Then this means that there exists an entanglement breaking channel $\mathcal{E}_A$

of which ρ_{AB} is a fixed point (since $F(\rho_{AB}, \mathcal{E}_A(\rho_{AB})) = 1$ is equivalent to $\rho_{AB} = \mathcal{E}_A(\rho_{AB})$), and furthermore, applying the fixed point projection

$$\overline{\mathcal{E}_A} \equiv \lim_{K\to\infty} \frac{1}{K} \sum_{k=1}^{K} \mathcal{E}_A^k \tag{4.4.47}$$

leaves ρ_{AB} invariant. The map $\overline{\mathcal{E}_A}$ has been characterized in [67, Theorem 5.3] to be an entanglement breaking channel of the following form:

$$\overline{\mathcal{E}_A}(\cdot) = \sum_i \text{Tr}\{M_i(\cdot)\}\,\sigma_i, \tag{4.4.48}$$

where the states σ_i have orthogonal support. Applying this channel to ρ_{AB} then gives a classical-quantum state, and since ρ_{AB} is invariant under the action of this channel to begin with, it must have been classical-quantum from the start. ■

Proposition 4.35. *The surprisal of measurement recoverability obeys the following dimension bound:*

$$D_F\left(\overline{A}; B\right)_\rho \leq \log|A|, \tag{4.4.49}$$

or equivalently,

$$\sup_{\mathcal{E}_A} F(\rho_{AB}, \mathcal{E}_A(\rho_{AB})) \geq \frac{1}{|A|}. \tag{4.4.50}$$

Proof. The idea behind the proof is to consider an entanglement breaking channel $\mathcal{E}_A$ that completely dephases the system A. Let $\overline{\Delta}_A$ denote such a channel, so that

$$\overline{\Delta}_A(\cdot) \equiv \sum_i |i\rangle\langle i|_A (\cdot) |i\rangle\langle i|_A, \tag{4.4.51}$$

where $\{|i\rangle_A\}$ is some orthonormal basis spanning the space for the A system. Let a spectral decomposition of ρ_{AB} be given by

$$\rho_{AB} = \sum_x p_X(x) |\psi^x\rangle\langle\psi^x|_{AB}, \tag{4.4.52}$$

where p_X is a probability distribution and $\{|\psi^x\rangle_{AB}\}$ is a set of pure states. We then find that

$$\begin{aligned}
D_F\left(\overline{A}; B\right)_\rho &\leq -\log F\left(\rho_{AB}, \overline{\Delta}_A(\rho_{AB})\right) && (4.4.53)\\
&= -2\log\sqrt{F\left(\rho_{AB}, \overline{\Delta}_A(\rho_{AB})\right)} && (4.4.54)\\
&\leq \sum_x p_X(x)\left[-2\log\sqrt{F\left(\psi^x_{AB}, \overline{\Delta}_A(\psi^x_{AB})\right)}\right] && (4.4.55)\\
&= \sum_x p_X(x)\left[-\log\langle\psi^x|_{AB}\,\overline{\Delta}_A(\psi^x_{AB})\,|\psi^x\rangle_{AB}\right] && (4.4.56)\\
&= \sum_x p_X(x)\left[-\log\sum_i \left[\langle i|_A\, \psi^x_A\, |i\rangle_A\right]^2\right] && (4.4.57)\\
&\leq \log|A|. && (4.4.58)
\end{aligned}$$

The second inequality follows from joint concavity of the root fidelity $\sqrt{F}$ and convexity of $-\log$. The last equality is a consequence of a well known expression for the entanglement fidelity of a channel (see, e.g., [196, Theorem 9.5.1]). The last inequality follows by recognizing

$$-\log \sum_i \left[\langle i|_A \psi_A^x |i\rangle_A\right]^2 \tag{4.4.59}$$

as the Rényi 2-entropy of the probability distribution $\langle i|_A \psi_A^x |i\rangle_A$ and from the fact that all Rényi entropies are bounded from above by the logarithm of the alphabet size of the distribution, which in this case is $\log|A|$. ■

By making use of the special form of the entanglement fidelity for a quantum channel (see, e.g., [196, Theorem 9.5.1]), we arrive at the following form for $D_F\left(\overline{A};B\right)$ when evaluated for a pure state:

Proposition 4.36. *Let ψ_{AB} be a pure state. Then*

$$D_F\left(\overline{A};B\right)_\psi = -\log \sup_{|\phi_x\rangle,|\varphi_x\rangle:\sum_x|\varphi_x\rangle\langle\varphi_x|=I} \sum_x \left|\langle\varphi_x|_A \psi_A |\phi_x\rangle_A\right|^2, \tag{4.4.60}$$

where the optimization is over pure-state vectors $|\phi_x\rangle$ and corresponding measurement vectors $|\varphi_x\rangle$ satisfying $\sum_x |\varphi_x\rangle\langle\varphi_x| = I$.

Proposition 4.37. *The surprisal of measurement recoverability $D_F\left(\overline{A};B\right)_\Phi$ is equal to $\log d$ for a maximally entangled state with Schmidt rank d.*

Proof. The following bound is a consequence of [152, Lemma 2]

$$F\left(\Phi_{AB}, \mathcal{E}_A\left(\Phi_{AB}\right)\right) \leq \frac{1}{d} \tag{4.4.61}$$

because $\mathcal{E}_A\left(\Phi_{AB}\right)$ is a separable state. Since the bound holds for any entanglement breaking channel, we get

$$D_F\left(\overline{A};B\right)_\Phi \geq \log d. \tag{4.4.62}$$

On the other hand, Proposition 4.35 gives $D_F\left(\overline{A};B\right)_\Phi \leq \log d$, which concludes the proof. ■

Proposition 4.38. *The surprisal of measurement recoverability is monotone with respect to quantum operations on the unmeasured system, i.e.,*

$$D_F\left(\overline{A};B\right)_\rho \geq D_F\left(\overline{A};B'\right)_\sigma, \tag{4.4.63}$$

where $\sigma_{AB'} \equiv \mathcal{N}_{B\to B'}\left(\rho_{AB}\right)$.

Proof. Intuitively, this follows because it is easier to recover from a measurement when the state is noisier to begin with. Indeed, let $\mathcal{E}_A$ be an entanglement breaking channel. Then

$$\begin{aligned} F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right) &\leq F\left(\sigma_{AB'}, \mathcal{E}_A\left(\sigma_{AB'}\right)\right) && (4.4.64)\\ &\leq \sup_{\mathcal{E}_A} F\left(\sigma_{AB'}, \mathcal{E}_A\left(\sigma_{AB'}\right)\right), && (4.4.65) \end{aligned}$$

where the first inequality is due to the fact that $\mathcal{E}_A$ commutes with $\mathcal{N}_{B\to B'}$ and monotonicity of the fidelity under quantum operations. Since the inequality holds for all entanglement breaking channels, we can conclude that

$$\sup_{\mathcal{E}_A} F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right) \leq \sup_{\mathcal{E}_A} F\left(\sigma_{AB'}, \mathcal{E}_A\left(\sigma_{AB'}\right)\right). \tag{4.4.66}$$

Taking a negative logarithm gives the statement of the proposition. ■

With a proof nearly identical to that for Proposition 4.27, we find that $D_F\left(\overline{A};B\right)_\rho$ is continuous:

Proposition 4.39. $D_F\left(\overline{A};B\right)$ *is a continuous function of its input. That is, given two bipartite states* ρ_{AB} *and* σ_{AB} *such that* $F\left(\rho_{AB},\sigma_{AB}\right) \geq 1-\varepsilon$ *where* $\varepsilon \in [0,1]$*, then the following inequalities hold*

$$\left|\sup_{\mathcal{E}_A} F\left(\rho_{AB}, \mathcal{E}_A\left(\rho_{AB}\right)\right) - \sup_{\mathcal{E}_A} F\left(\sigma_{AB}, \mathcal{E}_A\left(\sigma_{AB}\right)\right)\right| \leq 8\sqrt{\varepsilon}, \tag{4.4.67}$$

$$\left|D_F\left(\overline{A};B\right)_\rho - D_F\left(\overline{A};B\right)_\sigma\right| \leq |A|\, 8\sqrt{\varepsilon}. \tag{4.4.68}$$

4.5 Discussion

To summarize, in this chapter we defined the fidelity of recovery $F\left(A;B|C\right)_\rho$ of a tripartite state ρ_{ABC} to quantify how well one can recover the full state on all three systems if system A is lost and the recovery map can act only on system C. By taking the negative logarithm of the fidelity of recovery, we obtain an entropic quantity $I_F\left(A;B|C\right)_\rho$ which obeys nearly all of the entropic relations that the conditional mutual information does (non-negativity, monotonicity under local operations, duality, and dimension bounds). The quantities $F\left(A;B|C\right)_\rho$ and $I_F\left(A;B|C\right)_\rho$ are rooted in the Rényi generalizations of the QCMI presented in Appendix B. Whereas we have not been able to prove that all of the aforementioned properties hold for the Rényi QCMI from Appendix A, it is pleasing to us that it is relatively straightforward to show that these properties hold for $I_F\left(A;B|C\right)_\rho$.

We then defined a geometric squashed entanglement measure $E_F^{\text{sq}}\left(A;B\right)_\rho$, inspired by the original squashed entanglement measure from [40]. We proved that $E_F^{\text{sq}}\left(A;B\right)_\rho$ is a 1-LOCC monotone, is faithful, reduces to a variant of the well known geometric measure of entanglement [195, 35], normalized on maximally entangled states, subadditive, and continuous. The new entanglement measure could find applications in "one-shot" scenarios of quantum information theory, since it is fundamentally a one-shot measure based on the fidelity.

Further, we also defined the surprisal of measurement recoverability $D_F\left(\overline{A};B\right)_\rho$, a quantum correlation measure having physical roots in the same vein as those used to justify the definition of the quantum discord. We showed that it is non-negative, invariant under local isometries, faithful on classical-quantum states, obeys a dimension bound, and is continuous. Furthermore, we used this quantity to characterize quantum states with discord nearly equal to zero, finding that such states are approximate fixed points of an entanglement breaking channel.

From here, there are several interesting lines of inquiry to pursue. Can we prove a stronger chain rule for the fidelity of recovery? If something along these lines holds, it might be helpful in establishing that the geometric squashed entanglement is monogamous. Can we use geometric squashed entanglement to characterize the one-shot distillable entanglement or secret key of a bipartite state? Is it possible to improve our continuity bounds? Can one show that geometric squashed entanglement is non-lockable [36]? Preliminary evidence from considering the strongest known locking schemes from [61] suggests that it might not be lockable. We are also interested in a multipartite geometric squashed entanglement, but we face similar challenges as those discussed in [120] for establishing its faithfulness.

Part II
Parity-based Quantum Optical Metrology

Chapter 5
Optimal Phase Estimation with Parity Detection[1]

5.1 Introduction

The role of measurement in any metrology scheme cannot be overemphasized. It is perhaps as important as, if not more than, preparing probe systems. In quantum metrology, probe systems are typically prepared in optimal quantum states such that they can acquire maximal information about the unknown parameter of interest. Yet, it is equally crucial that the observable that is used to measure the probes also be optimal. In other words, the measurement observable should be able to fetch all the information acquired about the unknown parameter by the probes, so that a good estimate of the unknown value of the parameter can be made. In quantum parameter estimation theory (see Section 2.5), this optimality of a measurement observable translates into the condition that the classical Cramér-Rao bound of the observable for a given quantum state be equal to the quantum Cramér-Rao bound of the state [27].

In Appendix C, we mention various detection strategies that have been considered for phase estimation in two-mode quantum optical interferometry. Some of them involve classical ideas, e.g., homodyne detection [69], where a strong local oscillator is mixed with the signal-carrying beam and intensity difference is measured at the output. On the other hand,

[1]This chapter is reproduced by updating and adapting the contents of Kaushik P. Seshadreesan, Petr M. Anisimov, Hwang Lee, and Jonathan P. Dowling, New Journal of Physics, 13(8):083026, August 2011, and Kaushik P. Seshadreesan, Sejong Kim, Jonathan P. Dowling, and Hwang Lee, Physical Review A, 87:043833, April 2013, with the permission of IOP Publishing and APS, respectively. See Appendix E for the copyright permission from the publishers.

recent technological advances have enabled detection of light at the level of single-photon resolution (at least for small photon numbers) [125]. As a result, photon-number counting-based measurement observables have attracted a lot of attention recently. They have opened up new vistas in low-power applications of quantum optical interferometry that could not have been possible with classical detection schemes. In particular, it has been shown that in the small photon number regime, photon-number counting-based observables in two-mode interferometry could be used to achieve optimal phase sensitivities independent of the actual value of the phase [143]—a feat impossible to achieve, e.g., with homodyne detection.

In this chapter, we present phase estimation based on a measurement observable, which is nonclassical as is photon-number counting, and in fact very related to the latter—namely, photon-number parity detection [72]. One way to think of the parity measurement, which is perhaps obvious, is counting the number of photons and inferring parity depending on whether the count is even or odd. Photon-number parity has been shown to be optimal for several interferometric states. In our work, we make an attempt to characterize pure states for which photon-number parity is optimal. Also, we explicitly show optimality of photon-number parity for the interferometry with coherent light mixed with squeezed vacuum light. This state is known to be optimal for phase estimation when the coherent and squeezed-vacuum states are mixed in equal intensities, i.e., it is capable of Heisenberg limited phase estimation. We show that photon-number parity is an optimal measurement observable for this interferometry, including when the state itself is optimal. In other words, we demonstrate Heisenberg-limited phase estimation for this optimal state with photon-number parity detection.

The chapter is organized as follows. We begin by setting up the mathematical condition for a measurement observable to be optimal for phase estimation with any given pure state preparation of the probes. We then review Hofmann's work [87] on pure-state interferometry with photon-number counting. This includes a description of the "path-symmetric" states, which is a class of pure states for which photon-number counting-based observables are optimal for phase estimation. Almost all states considered for interferometric metrology thus far, such as the coherent state, the squeezed states, the twin-Fock state, are path symmetric. We present photon-number parity-based phase estimation for the path-symmetric states and show that parity measurement is locally optimal at some bias values of the unknown phase for a restricted class of path-symmetric states. Interestingly, the commonly considered states for interferometric metrology also satisfy this restricted path symmetry condition, which seems to be a more natural condition on two-mode states than complete path symmetry. We apply photon-number parity detection to the particular interferometry with coherent light mixed with squeezed-vacuum light input and demonstrate Heisenberg-limited phase estimation. Finally, for the same optimal state prepared by mixing coherent and squeezed vacuum states in equal intensities, we compare the performance of photon-number parity detection with another homodyne-based detection scheme that has been proposed in the literature. We show that although both the measurement observables are optimal at particular values of phase, parity offers better phase sensitivities over a broader range of values of phase than the other detection scheme.

5.2 Condition for Optimality of a Measurement Observable with Pure States

Consider a typical MZI with an unknown phase φ, as shown in Fig. 5.1, where we have labeled the states at various stages of the interferometer. Here, we use the Schwinger representation [205] presented in C.3.3 to describe the interferometer. Recall that a two-mode N-photon state in this representation resides in the $j = N/2$ subspace of the angular momentum Hilbert space, with the angular momentum operators operators $\hat{J}_x$, $\hat{J}_y$, and $\hat{J}_z$ given in terms of the mode operators $\hat{a}_1$, $\hat{a}_1^\dagger$, $\hat{b}_1$, and $\hat{b}_1^\dagger$ inside the interferometer as:

$$\hat{J}_x = \frac{1}{2}(\hat{a}_1^\dagger \hat{b}_1 + \hat{b}_1^\dagger \hat{a}_1),\ \hat{J}_y = \frac{1}{2i}(\hat{a}_1^\dagger \hat{b}_1 - \hat{b}_1^\dagger \hat{a}_1),\ \hat{J}_z = \frac{1}{2}(\hat{a}_1^\dagger \hat{a}_1 - \hat{b}_1^\dagger \hat{b}_1), \tag{5.2.1}$$

where $\hat{N} = \hat{a}_1^\dagger \hat{a}_1 + \hat{b}_1^\dagger \hat{b}_1$ and $J^2 = \hat{N}/2\left(\hat{N}/2 + 1\right)$ is the Casimir invariant of the group. Also, the unitary phase evolution in the MZI is represented as $\hat{U}_\varphi = \exp(-i\varphi \hat{J}_z)$, and the 50:50 beam splitter transformation can be chosen to be $\hat{U}_{BS} = \exp(-i\frac{\pi}{2}\hat{J}_y)$. [2] Using the SU(2) algebra of the angular momentum operators, namely $[\hat{J}_q, \hat{J}_r] = i\hat{J}_s\epsilon_{qrs}$ where $q, r, s \in \{x, y, z\}$ and ϵ is the antisymmetric tensor, and the Baker-Hausdorff lemma [160], the overall MZI transformation, $\hat{U}_{MZI} = \hat{U}_{BS}^\dagger \hat{U}_\varphi \hat{U}_{BS}$, can be shown to be $\hat{U}_{MZI} = \exp(-i\varphi \hat{J}_x)$.

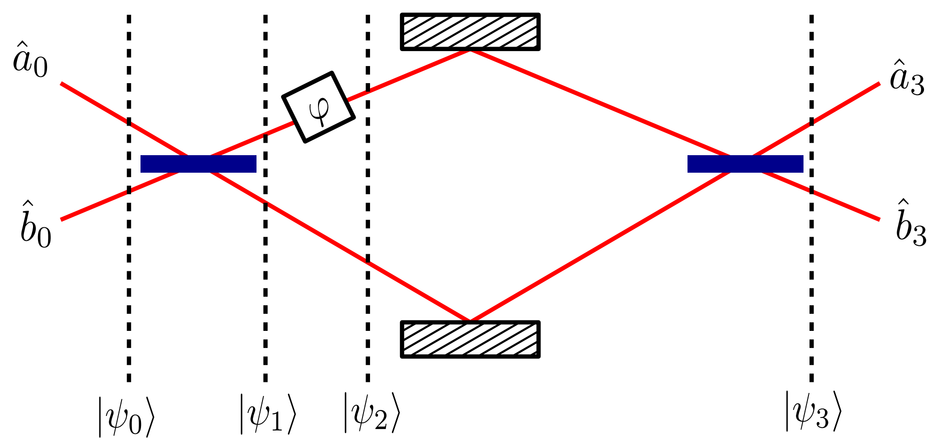

Figure 5.1: (Color online) A MZI with a two-mode input $|\psi_0\rangle$, which after the 50:50 beam splitter and phase shifter transformations $\hat{U}_{BS} = \exp(-i\frac{\pi}{2}\hat{J}_y)$, $\hat{U}_\varphi = \exp(-i\varphi \hat{J}_z)$ and $\hat{U}_{BS}^\dagger = \exp(i\frac{\pi}{2}\hat{J}_y)$ (in that order), is denoted by $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$, at the respective stages.

Our goal is to estimate the unknown phase φ. The error in the estimate based on the measurement of an observable $\hat{O}$ on state $|\psi_2\rangle$ can be written as:

$$\delta\varphi = \left|\Delta O/(\partial \left\langle \hat{O} \right\rangle /\partial\varphi)\right|. \tag{5.2.2}$$

where $\left\langle \hat{O} \right\rangle$ is the expectation value of $\hat{O}$, and ΔO is the uncertainty in the measurement. Based on the Heisenberg equation of motion for operators, the expectation value of observable

[2] Note that all the results presented in this chapter can also be obtained if the beam-splitter transformation is chosen to be $\exp(-i\frac{\pi}{2}\hat{J}_x)$ with minor modifications.

$\hat{O}$ with respect to the state $|\psi_2\rangle$ satisfies

$$\frac{\partial}{\partial\varphi}\left\langle\hat{O}\right\rangle = -i\left[\hat{O},\hat{J}_z\right], \tag{5.2.3}$$

where the commutator is with respect to the $\hat{J}_z$ operator—the generator of phase evolution in the MZI. According to the uncertainty principle [168], we have:

$$\Delta O\Delta J_z \geq \frac{1}{2}\left|\left[\hat{O},\hat{J}_z\right]\right| = \frac{1}{2}\left|\frac{\partial}{\partial\varphi}\left\langle\hat{O}\right\rangle\right|. \tag{5.2.4}$$

Consequently, the error in the estimate $\delta\varphi$ obeys:

$$\delta\varphi = \left|\Delta O/(\partial\left\langle\hat{O}\right\rangle/\partial\varphi)\right| \geq \frac{1}{2\Delta J_z}. \tag{5.2.5}$$

For pure quantum states $|\psi_3\rangle$, the right-hand side of the above inequality is identically equal to the QCRB of the state [27]. The equivalent (necessary and sufficient) condition on an observable $\hat{O}$ and state $|\psi_2\rangle$ for achieving the bound is identically the same as the condition for equality in Eq. (5.2.4), given by:

$$\tilde{O}\,|\psi_2\rangle = i\lambda\tilde{J}_z\,|\psi_2\rangle\,, \tag{5.2.6}$$

for any nonzero $\lambda\in\mathbb{R}$, where $\tilde{O} = \hat{O} - \left\langle\hat{O}\right\rangle\hat{I}$, $\tilde{J}_z = \hat{J}_z - \left\langle\hat{J}_z\right\rangle\hat{I}$, and $\hat{I}$ is the $(2j+1)\times(2j+1)$ identity operator [168]. (Note that $\tilde{O}$ and $\tilde{J}_z$ are also Hermitian operators.)

5.3 Photon-Number Counting and Path-Symmetric States

We now consider the above interferometry for the case of photon-number detection. In particular, we examine the condition in (5.2.6) for measurement observables that are diagonal in the photon-number basis. The goal is to describe the class of pure states for which such observables are optimal in the task of phase estimation, as originally done by Hofmann [87].

In the MZI of Fig. 5.1, the photon-number difference measurement observable at the output is given by $\hat{a}_3^\dagger\hat{a}_3 - \hat{b}_3^\dagger\hat{b}_3$. For the chosen beam-splitter transformation $\hat{U}_{BS} = \exp(-i\frac{\pi}{2}\hat{J}_y)$, this observable is given by the $\hat{J}_x$ operator in the Schwinger representation of (5.2.1) up to a factor of half. This is because

$$\frac{1}{2}\left(\hat{a}_3^\dagger\hat{a}_3 - \hat{b}_3^\dagger\hat{b}_3\right) = \hat{U}_{BS}\hat{U}_\varphi\hat{J}_z\hat{U}_\varphi^\dagger\hat{U}_{BS}^\dagger \tag{5.3.1}$$

$$= \hat{U}_{BS}\hat{U}_\varphi\frac{1}{2}\left(\hat{a}_1^\dagger\hat{a}_1 - \hat{b}_1^\dagger\hat{b}_1\right)\hat{U}_\varphi^\dagger\hat{U}_{BS}^\dagger \tag{5.3.2}$$

$$= \hat{J}_x, \tag{5.3.3}$$

which follows from the Baker-Hausdorff lemma [160]. Note that the observable diagonal in the $\hat{J}_x$ basis acts not on $|\psi_3\rangle$, but instead on $|\psi_1\rangle$ (and$|\psi_2\rangle$since $\hat{U}_\varphi$ commutes with $\hat{J}_z$). In a sense, we have transformed the observable acting on $|\psi_3\rangle$ to an observable that acts on $|\psi_1\rangle$ via the SU(2) equivalence given in (5.3.3).

Theorem 5.1. *In two-mode optical interferometric phase estimation, photon-number counting-based measurement observables are optimal for pure states that satisfy the following condition*

$$\langle m_x | \psi_2 \rangle = \langle m_x | \psi_2 \rangle^* e^{-i2\chi} \; \forall \; m_x \in \{-j, ..., +j\} \tag{5.3.4}$$

where $|m_x\rangle$ are the eigenkets of the $\hat{J}_x$ operator and the expectation is with respect to $|\psi_2\rangle$.

Proof. For a photon-number counting-based observable $\tilde{O}$ acting on the state $|\psi_2\rangle$, multiplying both sides of Eq. (5.2.6) by an eigenbra of $\hat{J}_x$, $\langle m_x|$, we get:

$$p_m \langle m_x | \psi_2 \rangle = i\lambda \langle m_x| \tilde{J}_z |\psi_2\rangle , \tag{5.3.5}$$

where p_m is the eigenvalue of $\tilde{O}$ satisfying:

$$\tilde{O} |m_x\rangle = p_m |m_x\rangle . \tag{5.3.6}$$

Rearranging the terms of Eq. (5.3.5), we obtain:

$$\frac{p_m}{\lambda} = i \frac{\langle m_x| \tilde{J}_z |\psi_2\rangle}{\langle m_x | \psi_2\rangle}. \tag{5.3.7}$$

Since p_m and λ are purely real numbers, $\langle m_x| \tilde{J}_z |\psi_2\rangle / \langle m_x| |\psi_2\rangle$ has to be purely imaginary in order for the state $|\psi_2\rangle$ to satisfy Eq. (5.3.7).

We can rewrite $\langle m_x| \tilde{J}_z |\psi_2\rangle / \langle m_x| |\psi_2\rangle$ by inserting the identity operator $\hat{I} = \sum_{|m\rangle} |m\rangle \langle m|$ as:

$$\frac{\langle m_x| \tilde{J}_z |\psi_2\rangle}{\langle m_x | \psi_2\rangle} = \sum_{|m\rangle} \frac{\langle m_x| \tilde{J}_z |m\rangle \langle m| |\psi_2\rangle}{\langle m_x | \psi_2\rangle}, \tag{5.3.8}$$

where $\{|m\rangle\}$ is the eigenbasis of the $\hat{J}_x$ operator. (Note that we call the basis elements as $|m\rangle$ in order to distinguish it from a specific $|m_x\rangle$.) The matrix elements of $\hat{J}_z$ in the $\hat{J}_x$ basis are all purely imaginary due to the cyclic property of the commutation relation between the angular momentum operators. (For example, recall that the matrix elements of the $\hat{J}_y$ operator are purely imaginary in the $\hat{J}_z$ basis.) This implies all the non-zero off-diagonal entries of $\tilde{J}_z$ are purely imaginary numbers, and all the diagonal entries are identically equal to $\left\langle \hat{J}_z \right\rangle$. Therefore, Eq. (5.3.8) reduces to:

$$\frac{\langle m_x| \tilde{J}_z |\psi_2\rangle}{\langle m_x | \psi_2\rangle} = \sum_{|m\rangle \neq |m_x\rangle} \langle m_x| \hat{J}_z |m\rangle \frac{\langle m | \psi_2\rangle}{\langle m_x | \psi_2\rangle} - \left\langle \hat{J}_z \right\rangle, \tag{5.3.9}$$

where $\langle m_x| \hat{J}_z |m\rangle$, $|m\rangle \neq |m_x\rangle$ are all purely imaginary numbers. Clearly, the following is a sufficient condition so that the right-hand side of (5.3.9) is purely imaginary:

$$\langle m | \psi_2\rangle / \langle m_x | \psi_2\rangle \in \mathbb{R} \; \forall \; \{m, \; m_x\} \in \{-j, ..., +j\}, \tag{5.3.10}$$
$$\left\langle \hat{J}_z \right\rangle = 0.$$

Further, the condition in (5.3.10) can be rewritten as

$$\langle m_x | \psi_2 \rangle = \langle m_x | \psi_2 \rangle^* e^{-i2\chi}, \ \forall \ m_x \in \{-j, ..., +j\}, \tag{5.3.11}$$

i.e., the state must have purely real coefficients in the $\hat{J}_x$ basis (up to a global phase) in order for (5.3.10) to be true. That proves the statement of the theorem. ■

As a result, we know that states that satisfy the condition given in Theorem 5.1 are capable of reaching their maximal phase sensitivities at the QCRB with photon-number counting-based detection strategies. Hofmann [87] identified these conditions with a symmetry property in the alternative picture, where the abstract angular momentum operator $\mathbf{J} = \{J_x, J_y, J_z\}$ undergo rotation instead of the state. The property can be explained as follows. Consider the $\hat{J}_x$-basis complex-conjugation operation of (5.3.4) on the angular momentum vector instead of the state $|\psi_2\rangle$. Since in the $\hat{J}_x$-basis $\hat{J}_x$ and $\hat{J}_y$ are real, but $\hat{J}_z$ imaginary, the above operation leaves the former invariant, but flips the latter, i.e., $\hat{J}_z \to -\hat{J}_z$. Therefore, the condition in (5.3.4) translates to the condition of invariance under the transformation $\hat{J}_z \to -\hat{J}_z$. Note that this condition implicitly conveys that $\left\langle \hat{J}_z \right\rangle = 0$. Hofmann calls this the "path-symmetry" condition, since the operation $\hat{J}_z \to -\hat{J}_z$ corresponds to an exchange of paths (modes) in the Schwinger representation. However, it is important to realize that it is an unphysical exchange of paths, because $\hat{J}_x$ and $\hat{J}_y$ remain unchanged all along, while that is not the case in general with an exchange of paths.

The condition of (5.3.4) is also sometimes referred to as the path-symmetry condition on a pure state. When transformed to the eigenbasis of the $\hat{J}_z$ operator, the condition of (5.3.4) yields

$$\langle m_z | |\psi_2 \rangle = \langle -m_z | |\psi_2 \rangle^* e^{-i2\chi}, \ \forall \ m_z \in \{-j, ..., +j\}. \tag{5.3.12}$$

It is easy to verify that states $|\psi_2\rangle$ that obey (5.3.12) implicitly satisfy $\left\langle \hat{J}_z \right\rangle = 0$. Also, if $|\psi_2\rangle = \sum_{m_z=-j}^{+j} c_m |m_z\rangle$, then $|\psi_1\rangle = \sum_{m_z=-j}^{+j} c_m e^{i m_z \varphi} |m\rangle$. Hence, $\langle m_z | |\psi_2\rangle / \langle -m_z | |\psi_2\rangle^* = e^{-i2\chi}$ also implies $\langle m_z |\psi_1\rangle / \langle -m_z |\psi_1\rangle^*$ also equals $e^{-i2\chi}$. In other words, the condition of (5.3.12) is satisfied independently of the value of the unknown phase φ. Thus, path-symmetric states are capable of reaching their QCRB with photon-number counting-based measurement observables independent of the actual value of phase φ. Almost all quantum states that have been considered for interferometric metrology, such as the coherent state, the squeezed vacuum states, the twin-Fock state, are path-symmetric states. Therefore, photon-number counting-based observables are optimal for all such states.

5.4 Photon-Number Parity and Path-Symmetric States

Photon number parity, in a nutshell, is the Hermitian observable $(-1)^{\hat{n}}$, where $\hat{n} \equiv \hat{b}^\dagger \hat{b}$ is the number operator of a mode labeled by $\hat{b}$. It is a two-valued observable described by the projection operators Π^+, Π^- with eigenvalues $+1$ and -1, respectively, where

$$\Pi^+ = |0\rangle \langle 0| + |2\rangle \langle 2| + \cdots \tag{5.4.1}$$

$$\Pi^- = |1\rangle \langle 1| + |3\rangle \langle 3| + \cdots . \tag{5.4.2}$$

Consider the parity operator for the mode $\hat{b}_3$ of Fig. 5.1, $\hat{\Pi} = (-1)^{\hat{b}_3^\dagger \hat{b}_3}$. For the chosen beam-splitter transformation $\hat{U}_{BS} = \exp(-i\frac{\pi}{2}\hat{J}_y)$, this can be written in the Schwinger representation as $(-1)^j \exp(-i\pi\hat{J}_x)$, where $j = N/2$. Similar to (5.3.3), this follows from an application of the Baker-Hausdorff lemma [160]

$$(-1)^{\hat{b}_3^\dagger \hat{b}_3} = \hat{U}_{BS}\hat{U}_\varphi(-1)^{j-\hat{J}_z}\hat{U}_\varphi^\dagger \hat{U}_{BS}^\dagger, \tag{5.4.3}$$

$$= (-1)^j \exp(-i\pi\hat{J}_x). \tag{5.4.4}$$

We call this operator $\hat{Q}$. It acts on the states $|\psi_1\rangle$ and $|\psi_2\rangle$ of Fig. 5.1. When expanded in the eigenbasis of the $\hat{J}_z$ operator, $\{|m_z\rangle\}$, the $\hat{Q}$ operator takes the form:

$$\hat{Q} = \sum_{|m_z\rangle} |m_z\rangle\langle -m_z|. \tag{5.4.5}$$

Our goal is to identify the class of pure states for which photon-number parity measurement observables are optimal in the task of phase estimation. However, since photon-number parity is implicitly based on photon-number counting (although it is of interest to try and implement parity without having to count photons), we expect it to be optimal only for a subset of any class of states for which photon-number counting-based observables are optimal. Therefore, we focus our analysis on studying the performance of parity-based detection strategies for the path-symmetric states of Section 5.3.

We now state our main theorem. The theorem is given for the parity measurement $\hat{Q}$. However, the result can be generalized to other observables that are diagonal in the eigenbasis of $\hat{Q}$. For convenience of notation, we omit the subscript z from the eigenkets of $\hat{J}_z$ $\{|m_z\rangle\}$.

Theorem 5.2. *In two-mode optical interferometric phase estimation, the photon-number parity measurement observable $\hat{Q}$ is optimal for a path symmetric state if and only if*

$$\langle\hat{Q}\rangle = \pm 1. \tag{5.4.6}$$

Proof. Let $|\psi_2\rangle$ be an N-photon path-symmetric state given by

$$|\psi_2\rangle = \sum_{m=-j}^{j} r_m e^{i(\theta_m - m\varphi)}|m\rangle, \tag{5.4.7}$$

where $\{|m\rangle\}$ are the eigenkets of $\hat{J}_z$. Recall the optimality condition for a measurement observable in phase estimation given in (5.2.6). In order to be optimal, the parity observable $\hat{Q}$ acting on a path-symmetric state $|\psi_2\rangle$ must satisfy

$$\tilde{Q}|\psi_2\rangle = i\lambda\hat{J}_z|\psi_2\rangle \tag{5.4.8}$$

for some nonzero $\lambda \in \mathbb{R}$, where $\tilde{Q} = \hat{Q} - \langle\hat{Q}\rangle\hat{I}$, and $\hat{I}$ is the $(2j+1)\times(2j+1)$ identity operator. (Note that $\langle\hat{J}_z\rangle$ is zero since $|\psi_2\rangle$ is taken to be path symmetric.) Multiplying throughout by the identity operator $\hat{I} = \sum_{|m\rangle}|m\rangle\langle m|$, we can rewrite Eq. (5.4.8) as

$$\sum_{|m\rangle}|m\rangle\langle m|\left(\tilde{Q} - i\lambda\hat{J}_z\right)|\psi_2\rangle = 0,$$

$$\Rightarrow \sum_{|m\rangle}\left(\langle m|\hat{Q}|\psi_2\rangle - \langle\hat{Q}\rangle\langle m|\psi_2\rangle - i\lambda m\langle m|\psi_2\rangle\right)|m\rangle = 0 \tag{5.4.9}$$

Dividing (5.4.9) throughout by $\langle m|\psi_2\rangle$ (assuming them to be nonzero without loss of generality), we obtain

$$\sum_{|m\rangle}\left(\frac{\langle m|\hat{Q}|\psi_2\rangle}{\langle m|\psi_2\rangle}-\langle\hat{Q}\rangle-i\lambda m\right)|m\rangle=0. \tag{5.4.10}$$

At this point, we can say that (5.4.10) holds if and only if

$$\langle\hat{Q}\rangle+i\lambda m=\frac{\langle m|\hat{Q}|\psi_2\rangle}{\langle m|\psi_2\rangle}\ \forall\ m\in\{-j,...,+j\}. \tag{5.4.11}$$

Let us define

$$S\left(m\right)\equiv\frac{\langle m|\hat{Q}|\psi_2\rangle}{\langle m|\psi_2\rangle}. \tag{5.4.12}$$

Using $\langle m|\psi_2\rangle=c_m e^{-im\varphi}$, and the form in (5.4.5) for the $\hat{Q}$ operator, $S\left(m\right)$ can be rewritten as

$$S\left(m\right)=\frac{c_{-m}}{c_m}e^{i2m\varphi}. \tag{5.4.13}$$

Let $c_m=r_m e^{i\theta_m}$, where r_m and θ_m are real. Then, based on the path-symmetry condition of (5.3.12), it is easy to show that $\frac{c_{-m}}{c_m}=e^{-2i(\theta_m+\chi)}$, and therefore, we have

$$S\left(m\right)=e^{i2(m\varphi-\chi-\theta_m)}. \tag{5.4.14}$$

We note that for all m, $|S\left(m\right)|^2=1$. Further, for all m, we decompose $S\left(m\right)$ as $S\left(m\right)\equiv S'\left(m\right)+iS''\left(m\right)$, where $S'\left(m\right)$ and $S''\left(m\right)$ are the real and imaginary parts, respectively.

Meanwhile, the expectation of the $\hat{Q}$ operator with the state $|\psi_2\rangle$, $\langle\hat{Q}\rangle$, can be written as

$$\langle\hat{Q}\rangle=\sum_{m=-j}^{j}c_{-m}c_m^*e^{i2m\varphi}. \tag{5.4.15}$$

Also, the real number λ can be determined by multiplying each side of (5.4.8) with its own conjugate transpose, to be

$$\lambda=\pm\frac{\Delta Q}{\Delta J_z}, \tag{5.4.16}$$

where $\Delta Q=\langle\hat{Q}^2\rangle-\langle\hat{Q}\rangle^2$ and similarly ΔJ_z. Since $\langle\hat{Q}^2\rangle=1$, and for any path-symmetric state, $\langle\hat{J}_z\rangle=0$, we have

$$\lambda=\pm\sqrt{\frac{1-\langle\hat{Q}\rangle^2}{\langle\hat{J}_z^2\rangle}}. \tag{5.4.17}$$

We note that λ is a function of $\langle\hat{Q}\rangle$.

The condition in (5.4.11) can now be rewritten in terms of $S'\left(m\right)$ and $S''\left(m\right)$ as

$$S'\left(m\right)+iS''\left(m\right)=\langle\hat{Q}\rangle+i\lambda m\ \forall\ m\in\{-j,...,+j\}. \tag{5.4.18}$$

In other words, for all $m\in\{-j,...,+j\}$, the real part of the left-hand side of (5.4.18) has to be equal to the real part of the right-hand side, and similarly the imaginary parts, i.e.,

$$S'\left(m\right)=\langle\hat{Q}\rangle\quad\text{and}\quad S''\left(m\right)=\lambda m\ \forall\ m\in\{-j,...,+j\}. \tag{5.4.19}$$

Notice in (5.4.15) that $\langle\hat{Q}\rangle$ is independent of m and a function of φ alone. Then $S'(m)$ has to be independent of m too in order for (5.4.18) to be satisfied.

We now prove that (5.4.6) is a *sufficient* condition. Say for some bias value of the phase, i.e., for $\varphi = \varphi_0$, $\langle\hat{Q}\rangle = \pm 1$. Then, $S'(m)|_{\varphi_0} = \pm 1 \; \forall \; m \in \{-j, ..., +j\}$ has to be true in order for (5.4.18) to be satisfied. Since $|S(m)|^2 = 1 \; \forall \; m \in \{-j, ..., +j\}$, fixing all the $S'(m) = \pm 1 \; \forall \; m \in \{-j, ..., +j\}$ automatically fixes all the $S''(m) = 0 \; \forall \; m \in \{-j, ..., +j\}$. From (5.4.17), we find that $\lambda m = 0$, when $\langle\hat{Q}\rangle = \pm 1$. Therefore, (5.4.18) holds when $\langle\hat{Q}\rangle = \pm 1$.

We now prove that (5.4.6) is also a *necessary* condition. Say for some fixed value $\varphi = \varphi_0$, $\langle\hat{Q}\rangle = q$, where $-1 \leq q \leq 1$ is a constant. Then, $S'(m)|_{\varphi_0} = q \; \forall \; m \in \{-j, ..., +j\}$ has to be true in order for (5.4.18) to be satisfied. However, since $|S(m)|^2 = 1 \; \forall \; m \in \{-j, ..., +j\}$, fixing all the $S'(m)$s to a constant automatically fixes all the $S''(m)$s to $\pm\sqrt{1-q^2}$ too, but the imaginary part of the right-hand side of (5.4.18) is clearly dependent on m. Therefore, (5.4.18) cannot hold for all values q. The only values of q for which it can hold are $q = \pm 1$. That completes the proof of the theorem. ■

Next we ask the question, "For a given path-symmetric state $|\psi_2\rangle$, does there exist a bias phase φ_0 for which $\langle\hat{Q}\rangle = \pm 1$?" The quantity $\langle\hat{Q}\rangle$ can be rewritten as

$$\begin{aligned}\langle\hat{Q}\rangle &= \sum_{m=-j}^{j} c_{-m} c_m^* e^{i2m\varphi} \\ &= \sum_{m=-j}^{j} S(m) |c_m|^2 \\ &= \sum_{m=-j}^{j} |c_m|^2 e^{i2(m\varphi - \chi - \theta_m)},\end{aligned}$$

where we have used (5.4.13) and (5.4.14) for $S(m)$. Therefore, the following should hold in order for $\langle\hat{Q}\rangle = \pm 1$:

$$\begin{aligned}e^{i2(m\varphi - \chi - \theta_m)} &= \pm 1 \; \forall \; m \in \{-j, ..., +j\} \\ \Rightarrow 2(m\varphi - \chi - \theta_m) &= n\pi, \; n \in \mathbb{Z}.\end{aligned}$$

Although it is hard to say something general here, the following are two sufficient conditions for the above to hold:

- $\theta_m = 0 \; \forall \; m \in \{-j, ..., +j\}$
- $\theta_m = m\theta$ for a constant θ.

Note that both the above conditions imply $\chi = 0$ in the path symmetry condition of (5.3.12). Consider $\varphi \to \varphi + \varphi_0$ and set $\varphi = 0$. Then the values of φ_0 in the first condition and $\varphi_0 - \theta$ in the second, when chosen as

$$\begin{cases} \frac{\pi}{2}, \; \frac{3\pi}{2}; & N \text{ odd} \\ 0, \; \frac{\pi}{2}, \; \pi, \; \frac{3\pi}{2}; & N \text{ even} \end{cases}, \tag{5.4.20}$$

satisfy $\langle \hat{Q} \rangle = \pm 1$ for the respective types of restricted path-symmetric states. Interestingly, almost all the states considered for interferometric metrology in fact belong to this restricted class of path-symmetric states. This is related to linearity and how the beam splitter transformation $\hat{U}_{BS} = \exp(-i\frac{\pi}{2}\hat{J}_y)$ operates.

Since optimality with parity is achieved only at specific values of phase φ, the applicability of parity detection, is restricted to estimating "local" phases (the $N00N$ state being an exception since it satisfies Eq. (5.4.6) independently of the value of φ). Local parameter estimation is concerned with detecting small changes of parameters that are more or less known, as opposed to the "global" one, wherein a complete lack of knowledge about the parameter is initially assumed [54]. It is assumed that we have complete control over the initial phase of the interferometer, which is tuned to an optimal bias phase or "sweet spot" given in (5.4.20). At the optimal operating point, our scheme can detect very tiny changes in phase with sensitivity at the QCRB of the quantum state used. Potential applications include quantum sensing and imaging.

5.5 Coherent-mixed with Squeezed Vacuum Light Interferometry

In this section, we focus on a particular interferometry scheme, namely the one based on mixing coherent light and squeezed vacuum light. This interferometric state, as mentioned before, holds an important place in the history of quantum metrology. It is where the possibility of sub-shot noise phase estimation was originally unearthed [34]. This scheme has been revisited recently. Hofmann and Ono [88] showed that when these inputs are mixed in equal intensities, namely such that $\sinh^2 r = |\alpha|^2 = \overline{n}/2$ (for any value of average photon number $\overline{n}$), then the state that results past the mixing splitter is such that each N-photon component in the state has a fidelity higher than 90% with the corresponding $N00N$ state. This provides an alternative explanation for the sub-shot-noise phase precision capabilities of the scheme. The scheme has been widely used to generate $N00N$ states in experiments. Afek et al. [3, 101] used this scheme to generate $N00N$ states of up to $N = 5$; the state of the art in the generation of such states.

5.5.1 Performance with photon-number detection

Pezze and Smerzi [143] calculated the classical Cramér-Rao bound for the interferometer with coherent light and squeezed vacuum light along with photon-number detection at the output, and found it to be:

$$F_{\text{Cl}} = |\alpha|^2 e^{2r} + \sinh^2 r. \tag{5.5.1}$$

When the average photon numbers of the two inputs are about the same, i.e., $\sinh^2 r = |\alpha|^2 = \overline{n}/2$, the classical Fisher information is approximately $\overline{n}^2 + \overline{n}/2$, which results in Heisenberg scaling for the phase precision, namely $\Delta\varphi = 1/(\sqrt{\nu}\overline{n})$, where ν is the number of data points gathered from measuring identical copies of the state. Note that the classical Fisher information is independent of the phase. Thus, the scheme is capable of Heisenberg-limited phase estimation independent of the actual value of phase, as was shown with the help of a Bayesian update protocol in [143].

5.5.2 Performance with photon-number parity detection

We now describe our analysis of the interferometry with coherent light mixed with squeezed vacuum light for parity detection [165]. In this section, since the states are Gaussian, it is easier to analyze the interferometry in terms of phase space representations. We choose to use the Wigner functions.

The input to the interferometer is in the product state $|\alpha_0\rangle \otimes |\xi = r\ e^{i\phi_s}\rangle$ that describes coherent light with amplitude $\alpha_0 = \sqrt{n_c}e^{-i\phi_c}$ in one mode and squeezed vacuum with parameters r and φ_s in the other. The corresponding Wigner function of the input state is the product of the respective Wigner functions as well [69]:

$$W_{\rm in}(\alpha, \alpha_0; \beta, r) = W_c(\alpha, \alpha_0) W_s(\beta, r), \tag{5.5.2}$$

with the Wigner function for the corresponding states being

$$W_c(\alpha, \alpha_0) = \tfrac{2}{\pi} e^{-2|\alpha-\alpha_0|^2},\ W_s(\beta, r) = \tfrac{2}{\pi} e^{-2|\beta|^2 \cosh 2r - \left(\beta^2+\beta^{*2}\right)\sinh 2r}, \tag{5.5.3}$$

and where we have made $\phi_s = 0$ by appropriately fixing the irrelevant absolute phase. This choice implies that the phase of the coherent light ϕ_c is now measured with respect to the phase of the squeezed vacuum state. The state of light at the output of the Mach-Zehnder interferometer is described by the following Wigner function:

$$\begin{aligned} W_{\rm out}(\alpha_f, \beta_f) &= \frac{4}{\pi^2} e^{-2|ie^{i\frac{\varphi}{2}}(\alpha_f \sin\frac{\varphi}{2} + \beta_f \cos\frac{\varphi}{2}) + \alpha_0|^2} \\ &\times\ e^{-2|\alpha_f \cos\frac{\varphi}{2} - \beta_f \sin\frac{\varphi}{2}|^2 \cosh 2r} \times e^{2\ \mathrm{Re}\left[e^{i\varphi}\left(\alpha_f \cos\frac{\varphi}{2} - \beta_f \sin\frac{\varphi}{2}\right)^2\right]\sinh 2r}. \end{aligned}$$

An expected signal of the parity detection scheme $\langle\hat{\Pi}_a\rangle$ is calculated as the value of the Wigner function at the origin for the corresponding mode. In the case of mode $\hat{a}_f$, $\langle\hat{\Pi}_{a_f}\rangle = \frac{\pi}{2}\int W_{\rm out}(0,\beta) d^2\beta$, and is found to be:

$$\langle\hat{\Pi}_{a_f}\rangle = \frac{\exp\left[-n_c\left(\frac{\sqrt{n_s^2+n_s}\sin^2\varphi\cos 2\phi_c - \cos\varphi}{n_s\sin^2\varphi+1} + 1\right)\right]}{\sqrt{n_s \sin^2\varphi + 1}}, \tag{5.5.4}$$

where the coherent light amplitude and the squeezing parameter have been expressed in terms of the average photon numbers, n_c and n_s, using the relations $\alpha_0 = \sqrt{n_c}e^{-i\phi_c}$ and $r = \sinh^{-1}\sqrt{n_s}$.

The signal of the parity detection scheme is periodic with period 2π and attains its maximum value of one at $\varphi = 0$. Although this maximum value is independent of the phase of the coherent light ϕ_c and the light intensities n_c and n_s, the visibility of the signal and its width are functions of these parameters. The visibility of the signal is found to be best when $\phi_c = 0$ and to diminish as ϕ_c drifts away from zero, becoming worst at $\phi_c = \pi/2$. Since it is reasonable to assume the coherent and squeezed vacuum light to be locked to the same external phase, ϕ_c can be set to zero for optimal performance. Further, the dependence of the signal on the light intensities is studied in terms of the total input intensity, $n_{\rm in} = n_c + n_s$, and the fraction of total intensity in the squeezed vacuum state, $\eta = n_s/n_{in}$. When η is increased from zero, the signal is found to grow narrower until reaching an optimal width, and then to broaden again, but with reduced visibility as η approaches one. For $\eta = 0$ and $\eta = 1$, the width of the signal is found to be proportional to $\pi/\sqrt{n_{\text{in}}}$, which is narrower than the resolution of conventional interferometry by a factor of $\sqrt{n_{\text{in}}}$ and thus demonstrates super-resolution [22]. The fraction $\eta = 0.5$ is found to be the most optimal choice for distributing the input light intensity, since it allows a higher narrowing factor of n_{in}. Figure 5.2 demonstrates this result by comparing the parity signals for interferometry with only coherent light ($\eta = 0$) [68] or squeezed light ($\eta = 1$) and interferometry with coherent and squeezed vacuum light of equal intensities ($\eta = 0.5$). We see that for the same total input photon number, $n_{\text{in}} = 10$, the parity signal for the latter case is narrower than any other case.

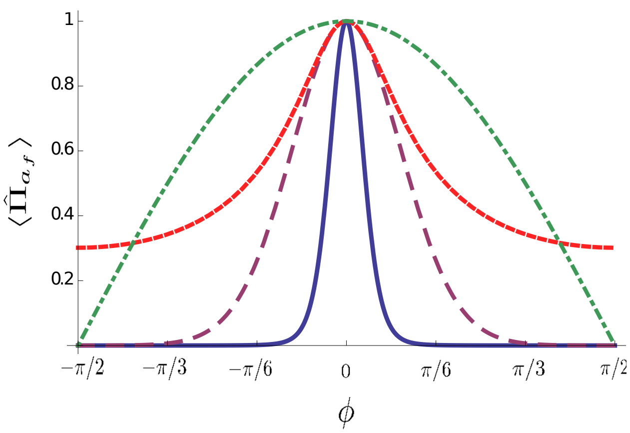

Figure 5.2: (Color online) The parity signal $\langle\hat{\Pi}_{a_f}\rangle$, as a function of the accumulated phase between the arms of the MZI φ: dashed (purple) line for coherent light interferometry ($\eta = 0$) with $n_c = 10$, $\phi_c = 0$; dotted (red) line for squeezed vacuum light interferometry ($\eta = 1$) with $n_s = 10$; and solid (blue) line for coherent and squeezed vacuum light interferometry ($\eta = 0.5$) with $n_c = n_s = 5$, $\phi_c = 0$. The dot-dashed (green) line is the scaled-down signal for conventional coherent light interferometry with intensity difference measurement.

The phase sensitivity $\Delta\varphi$ of the scheme with parity detection can be characterized using the error propagation formula of (C.3.13) with $\hat{O} = \hat{\Pi}_{a_f}$. The smaller the value of $\Delta\varphi$, the higher is the phase sensitivity. Interestingly, for the parity operator, this formula is equivalent to the classical Fisher information. The classical Fisher information is given by [190]

$$F_C = \sum_i \frac{1}{P(i|\varphi)} \left(\frac{dP(i|\varphi)}{d\varphi}\right)^2, \tag{5.5.5}$$

where i represents the outcome of the measurement and $P(i|\varphi)$ is the probability of the measurement resulting in the i-th outcome conditioned on a specific value of phase φ. For parity measurement described by the operator $\hat{\Pi} = (-1)^{\hat{n}}$, the two outcomes denoted by $+$ for even and $-$ for odd, are such that

$$\begin{aligned} P(+|\varphi) + P(-|\varphi) &= 1, \\ (+1)P(+|\varphi) + (-1)P(-|\varphi) &= \langle\hat{\Pi}\rangle. \end{aligned} \tag{5.5.6}$$

Also, $\hat{\Pi}^2 = 1$, and therefore,

$$\Delta\Pi^2 = 1 - \langle\hat{\Pi}\rangle^2 = 4P(+|\varphi)P(-|\varphi), \tag{5.5.7}$$

$$\frac{dP(+|\varphi)}{d\varphi} = \frac{1}{2}\frac{d\langle\hat{\Pi}\rangle}{d\varphi} = -\frac{dP(-|\varphi)}{d\varphi}. \tag{5.5.8}$$

From (5.5.5-5.5.8) we can see that the classical Fisher information for parity measurement is:

$$F_C = \left(\Delta\Pi^2 \Big/ \left|\frac{d\langle\hat{\Pi}\rangle}{d\varphi}\right|^2\right)^{-1} = \left(\frac{1 - \langle\hat{\Pi}\rangle^2}{\left|\frac{d\langle\hat{\Pi}\rangle}{d\varphi}\right|^2}\right)^{-1}. \tag{5.5.9}$$

The phase sensitivity with parity detection for coherent and squeezed vacuum light interferometry is in general a function of the actual value of the phase. (We don't show it here since it is a complicated expression that does't say much anyway). However, we find the best phase precision to be at $\varphi = 0$, which is given by:

$$\Delta\varphi^2 = \frac{1}{2n_c\sqrt{n_s(n_s+1)}\cos 2\phi_c + 2n_c n_s + n_c + n_s}. \tag{5.5.10}$$

For a detection scheme to be optimal, it has to saturate the quantum Cramér-Rao bound. The quantum Cramér-Rao bound for the interferometry with coherent light and squeezed vacuum was derived in Ref. [143]:

$$\Delta\varphi^2_{\text{QCRB}} = \frac{1}{|\alpha_0|^2 e^{2r} + \sinh^2 r}. \tag{5.5.11}$$

This expression can be shown to be identical to the phase sensitivity with parity detection, given in (5.5.10) (under the condition $\phi_c = 0$), when α_0 and r are expressed in terms of the average photon numbers, n_c and n_s. Thus, parity detection saturates the quantum Cramér-Rao bound and is optimal for the considered interferometric scheme for accumulated phases around zero.

Although parity detection is optimal for the considered interferometric scheme irrespective of the input intensities, the combination as a whole achieves its best phase sensitivity when $\eta = 0.5$. Figure 5.3 is a plot of the quantum Cramér-Rao bound $\Delta\varphi_{\text{QCRB}}$ for the interferometry with coherent and squeezed vacuum light given in (5.5.11), as a function of the fraction of squeezed vacuum in the input η. The phase sensitivity $\Delta\varphi_{\text{QCRB}}$ can be seen to be best when $\eta \approx 0.5$. At this value of η, under the condition $\phi_c = 0$, (5.5.10) reveals that the phase sensitivity $\Delta\varphi$ of the considered interferometric scheme with parity detection coincides with the Heisenberg-limit, $\Delta\varphi \approx 1/n_{\text{in}}$, while it coincides with the shot-noise limit, $\Delta\varphi \approx 1/\sqrt{n_{\text{in}}}$, when $\eta = 0$ or 1.

Figure 5.4 compares the phase sensitivity $\Delta\phi$ with parity detection for the cases corresponding to $\eta = 0$, $\eta = 1$ and $\eta = 0.5$. It reveals that $\eta = 0.5$ with $n_c = n_s = 5$ provides sub-shot noise phase sensitivities up to accumulated phases of about ± 0.2 away from the optimum value of $\varphi = 0$, but the phase sensitivity plummets in a dramatic fashion beyond

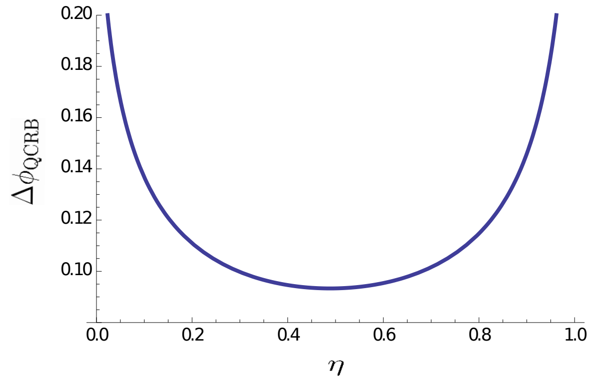

Figure 5.3: The quantum Cramér-Rao bound $\Delta\varphi_{\mathrm{QCRB}}$ for the interferometry with coherent and squeezed vacuum light, as a function of the fraction of squeezed vacuum in the input η. The total input photon number $n_{\mathrm{in}} = 10$.

these values of accumulated phase. However, $\eta = 0$ provides a fairly constant phase sensitivity at about the shot-noise limit over a much broader range of accumulated phases. (The case $\eta = 0$ is not of much interest since it's phase sensitivity $\Delta\varphi$ also deteriorates rather quickly, from the shot noise limit, as one moves away from the optimal value of $\varphi = 0$.) Thus, a suggested way to perform phase estimation is to start with coherent light $\eta = 0$ and roughly learn the value of the accumulated phase; move the accumulated phase closer to the origin and then tune-up η to 0.5 for an improved phase sensitivity.

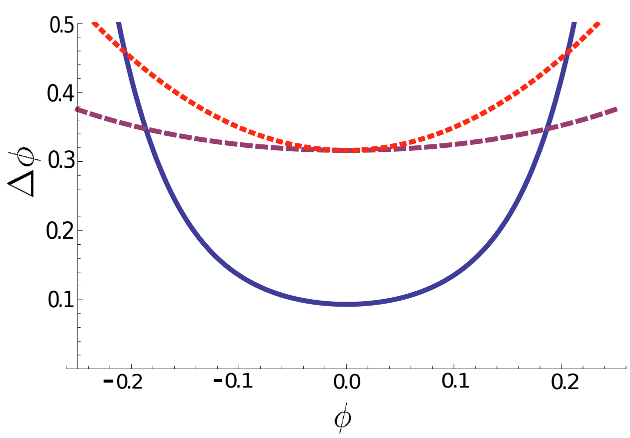

Figure 5.4: (Color online) Phase sensitivity $\Delta\varphi$ with parity detection, as a function of the accumulated phase between the arms of the MZI φ: dashed (purple) line for coherent light interferometry ($\eta = 0$) with $n_c = 10$, $\phi_c = 0$, dotted (red) line for squeezed vacuum interferometry ($\eta = 1$) with $n_s = 10$ and solid (blue) line for coherent and squeezed vacuum light interferometry ($\eta = 0.5$) with $n_c = n_s = 5$, $\phi_c = 0$.

5.5.3 Performance with a particular homodyne-based detection

So far, we have shown that parity detection could be used to achieve Heisenberg-limited phase estimation in the interferometry with coherent and squeezed vacuum light. In Ref. [137], Ono and Hofmann discussed a different detection scheme that implements the measurement of a symmetric logarithmic derivative. Implementation of this measurement is based on interference with a local oscillator and intensity difference measurement as shown in Fig. 5.5. Since symmetric logarithmic derivative based phase estimators saturate the quantum Cramér-Rao bound, Heisenberg-limited phase sensitivity was anticipated with this scheme for the interferometry with coherent and squeezed vacuum light mixed in equal proportions ($\eta = 0.5$). Here, we present a brief study of the Ono-Hofmann detection scheme (in the absence of losses), for the purpose of comparing it with parity detection.

The Ono-Hofmann detection scheme consists of a second MZI appended at the output of the first, with a phase ϕ, which is set to π [3]. A local oscillator field, which is in the coherent state, $|\gamma_{\text{lo}}\rangle = \sqrt{n_{\text{lo}}/T}e^{i\phi_{\text{lo}}}$, is introduced by mixing with the mode $\hat{a}_{f'}$ through a highly reflective beam splitter of transmissivity, $T << 1$, where n_{lo} is the average number of photons in the field that eventually enters the interferometer, and ϕ_{lo}, its phase. In the end, the difference in intensities at the two output modes is measured.

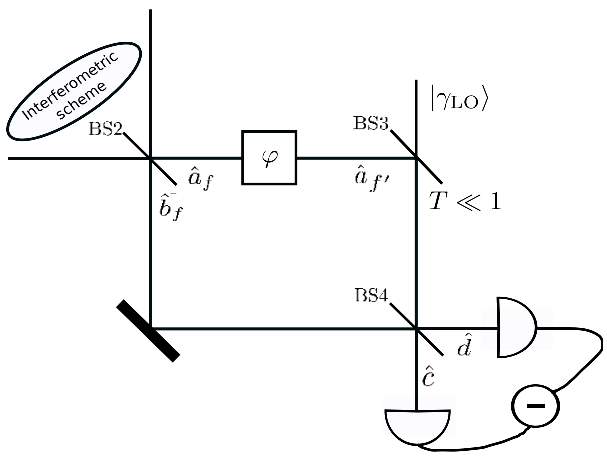

Figure 5.5: The Ono-Hofmann detection scheme for interferometry with coherent and squeezed vacuum light. The detection scheme uses interference with an auxiliary local oscillator and intensity difference measurement for phase estimation. A highly reflective beam splitter is used to mix the local oscillator field into the interferometer.

Intensity measurements at the output provide:

$$\begin{aligned} \langle \hat{c}^\dagger \hat{c} \rangle &= \langle \left\{ \hat{c}^\dagger \hat{c} \right\}_s \rangle - \tfrac{1}{2}, \\ \langle \hat{d}^\dagger \hat{d} \rangle &= \langle \left\{ \hat{d}^\dagger \hat{d} \right\}_s \rangle - \tfrac{1}{2}, \end{aligned} \tag{5.5.12}$$

$\left\{ \hat{c}^\dagger \hat{c} \right\}_s$ ($\left\{ \hat{d}^\dagger \hat{d} \right\}_s$) being the symmetric form of the operator, which can be evaluated based on

[3]We have also analyzed the case $\varphi = 0$. The phase sensitivity is found to be the same, but the signal turns out to be different.

the final Wigner function of the state W_f as:

$$\langle \{\hat{c}^\dagger \hat{c}\}_s \rangle = \int \int |\alpha|^2 W_f(\alpha, \beta) d^2\alpha d^2\beta, \tag{5.5.13}$$

$$\langle \left\{\hat{d}^\dagger \hat{d}\right\}_s \rangle = \int \int |\beta|^2 W_f(\alpha, \beta) d^2\alpha d^2\beta, \tag{5.5.14}$$

where α and β are the complex amplitudes in the modes $\hat{c}$ and $\hat{d}$ respectively.

The signal, which is the difference in intensities at the output ports, is thus given by:

$$I = \int \int \left(|\alpha|^2 - |\beta|^2\right) W_f(\alpha, \beta) d^2\alpha d^2\beta, \tag{5.5.15}$$

and is found to be:

$$I = -2\sqrt{n_c n_{\text{lo}}} \cos \tfrac{\varphi}{2} \cos\left(\tfrac{\varphi}{2} + \phi_c - \phi_{\text{lo}}\right) - (n_c - n_s) \sin \varphi. \tag{5.5.16}$$

It is plotted in Fig. 5.6, as a function of φ, under the condition $\phi_c = 0$, $\phi_{\text{lo}} = \pi/2$ and $n_{\text{lo}} = n_c(e^{2\sinh^{-1}(\sqrt{n_s})} + 1)^2$ (the condition when the phase sensitivity is found to be optimal, as mentioned later in the paper). The figure compares the signal for the interferometry with equal intensities of coherent and squeezed vacuum light ($\eta = 0.5$), with those of interferometry with only coherent light ($\eta = 0$) and very little coherent light ($\eta \approx 1$). We see that for the same total input photon number, $n_{\text{in}} = 10$, the signal for the former is stronger than any other case. However, unlike with parity detection, there is no super-resolution in the signal for the Ono-Hofmann detection scheme.

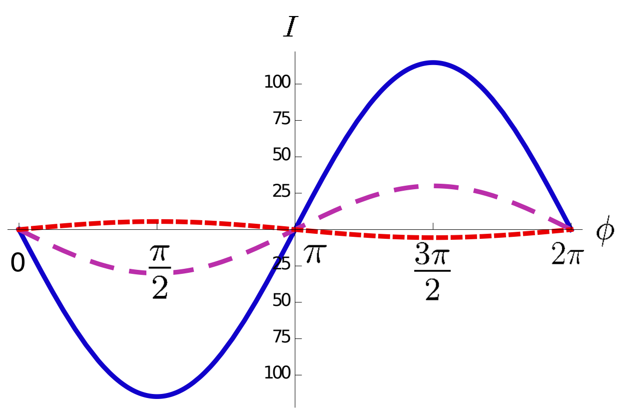

Figure 5.6: (Color online) The signal with the Ono-Hofmann detection scheme—the intensity difference I, plotted as a function of the accumulated phase between the arms of the MZI φ: dashed (purple) line for coherent light interferometry ($\eta = 0$) with $n_c = 10$, $\phi_c = 0$, dotted (red) line for squeezed vacuum light interferometry ($\eta \approx 1$) with $n_s = 9.9$, $n_c = 0.1$, $\phi_c = 0$ and solid (blue) line for coherent and squeezed vacuum light interferometry ($\eta = 0.5$) with $n_c = n_s = 5$, $\phi_c = 0$. A local oscillator of strength $n_{\text{lo}} = n_c(e^{2\sinh^{-1}(\sqrt{n_s})} + 1)^2$ and phase $\phi_{\text{lo}} = \pi/2$ is used in each case.

We calculate the phase sensitivity with the Ono-Hofmann detection scheme for the interferometry with coherent and squeezed vacuum light based on the error propagation formula mentioned in (C.3.13). Variance of the signal ΔI^2 which is required in the formula, can be shown to be:

$$\Delta I^2 = \int\int \left(|\alpha|^2 - |\beta|^2\right)^2 W_f(\alpha,\beta) d^2\alpha d^2\beta - \tfrac{1}{2}. \tag{5.5.17}$$

The phase sensitivity thus calculated, is found to be optimal at $\varphi = \pi$, under the condition $\phi_c = 0,\ \phi_{\rm lo} = \pi/2$, and is given by:

$$\Delta\varphi^2 = \frac{-2\left(-2n_s+2\sqrt{n_s^2+n_s}-1\right)(\sqrt{n_c}-\sqrt{n_{\rm lo}})^2+2n_s+1}{2(\sqrt{n_c n_{\rm lo}}-n_c+n_s)^2}. \tag{5.5.18}$$

(5.5.18) attains it's minimum value at $n_{\rm lo} = \frac{n_c\left(-e^{2r}+e^{4r}+e^{6r}+1\right)^2}{(e^{2r}-1)^4}$ (where $r = \sinh^{-1}\sqrt{n_s}$), which is only slightly different from the optimal value of $n_{\rm lo}$ given in Ref. [137], namely $n_{\rm lo} = n_c(e^{2r}+1)^2$. This difference can be explained as due to not optimizing the error propagation formula. When evaluated at $n_{\rm lo} = n_c(e^{2r}+1)^2$, Eq. (5.5.18) takes the form:

$$\Delta\varphi^2 = \frac{1}{n_c e^{2r}+n_s} + \frac{1}{2(n_c e^{2r}+n_s)^2}. \tag{5.5.19}$$

The leading term of this expression is nothing but the quantum Cramér-Rao bound mentioned in (5.5.11), while the second term is negligibly small and can be ignored. Thus, the Ono-Hofmann detection scheme indeed saturates the quantum Cramér-Rao bound for accumulated phases of value around π.

For $n_s \approx n_c \approx \frac{n_{\rm in}}{2}$ ($\eta = 0.5$) and $n_{\rm lo} = n_c(e^{2r}+1)^2$, (5.5.18) takes the form:

$$\Delta\varphi^2 = \frac{2\left(n_{\rm in}\left(n_{\rm in}+\sqrt{n_{\rm in}+2}\sqrt{n_{\rm in}}+2\right)+1\right)}{n_{\rm in}^2\left(n_{\rm in}+\sqrt{n_{\rm in}+2}\sqrt{n_{\rm in}}+2\right)^2}. \tag{5.5.20}$$

In the limit of large $n_{\rm in}$, namely the regime of interest of the Ono-Hofmann detection scheme, this can be expanded in a series as:

$$\Delta\varphi^2 = \left(\frac{1}{n_{\rm in}}\right)^2 - \frac{3}{2n_{\rm in}^3} + O\left(\left(\frac{1}{n_{\rm in}}\right)^4\right). \tag{5.5.21}$$

The above expression for phase sensitivity $\Delta\varphi$ shows Heisenberg-limited scaling with the total number of photons n_{in} and thus proves that the Ono-Hofmann scheme provides Heisenberg-limited phase sensitivity as anticipated.

Figure 5.7 compares the phase sensitivity $\Delta\varphi$ with the Ono-Hofmann detection scheme for the cases corresponding to $\eta = 0$, $\eta \approx 1$ and $\eta = 0.5$. Similar to the results with parity detection, the case $\eta = 0.5$ with $n_c = n_s = 5$, provides sub-shot noise phase sensitivities up to accumulated phases of about ± 0.3 away from the optimum value of $\varphi = \pi$, but the phase sensitivity diminishes beyond these values of accumulated phase. However, $\eta = 0$ provides a fairly constant phase sensitivity at about the shot-noise limit over a broader range of accumulated phases. (Note: Although the phase sensitivity of the case $\eta \approx 1$ reaches below the shot noise limit around $\varphi = \pi$, it is found to deteriorate even faster than the case $\eta = 0.5$ as one moves away from $\varphi = \pi$ and hence is not of much interest with the Ono-Hofmann detection scheme either.) Thus, very similar to what was suggested for parity detection, phase estimation with the Ono-Hofmann detection scheme may be best performed by starting with coherent light $\eta = 0$ and roughly learning the value of the accumulated phase; moving the accumulated phase closer to $\varphi = \pi$ and then tuning up η to 0.5 for an improved phase sensitivity.

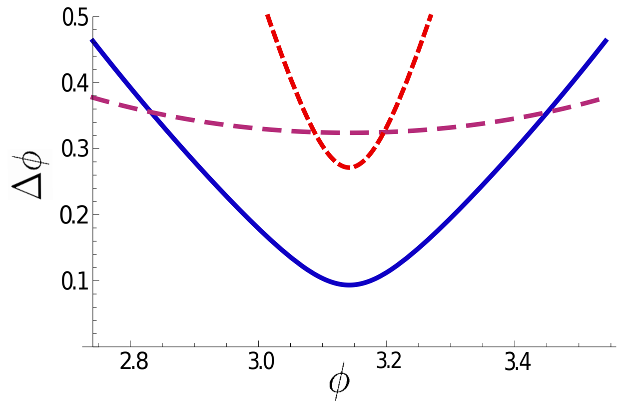

Figure 5.7: (Color online) Phase sensitivity with the Ono-Hofmann detection scheme $\Delta\varphi$, as a function of the accumulated phase between the arms of the MZI φ: dashed (purple) line for coherent light interferometry ($\eta = 0$) with $n_c = 10$, $\phi_c = 0$, dotted (red) line for squeezed vacuum interferometry ($\eta \approx 1$) with $n_s = 9.9$, $n_c = 0.1$, $\phi_c = 0$ and solid (blue) line for coherent and squeezed vacuum light interferometry ($\eta = 0.5$) with $n_c = n_s = 5$, $\phi_c = 0$. A local oscillator of strength $n_{\mathrm{lo}} = n_c(e^{2\sinh^{-1}(\sqrt{n_s})} + 1)^2$ and phase $\phi_{\mathrm{lo}} = \pi/2$ is used in each case.

5.6 Discussion

In this chapter, we discussed two-mode optical interferometry with the non-classical detection strategy based on photon-number parity measurement. In particular, we studied the question "For what class of two-mode pure states is the photon-number parity observable optimal for phase estimation?" We began by reviewing Hofmann's work on a the same question for photon-number detection-based measurement observables. We discussed the condition of path symmetry, which was introduced in that work as a sufficient condition on a two-mode pure state so that photon-number counting-based measurement observables are optimal for the state. We then analyzed the performance of photon-number parity detection for the path-symmetric states. We showed that photon-number parity is an optimal measurement for a restricted class of path-symmetric states, and that there exists a bias phase where the optimality is achieved.

In the latter part of the chapter, we discussed the interferometry with coherent light mixed with squeezed vacuum light, which is known to achieve the Heisenberg limit when the inputs are mixed in equal intensities. We showed that photon-number parity is optimal for this scheme and thus enables Heisenberg-limited phase estimation with the state. We also compared the performance of parity with a homodyne-based detection scheme proposed by Ono and Hofmann. Though this other scheme also achieves the Heisenberg limit, we showed that parity provides better phase sensitivities than the other scheme over a broad range of values of the unknown phase.

One may ask, what is the advantage of photon-number parity detection over photon-number counting-based observables? On the one hand, for a path-symmetric state, photon-number counting reveals all possible information about the unknown phase and leads to phase estimation at the QCRB for all values of phase (global phase estimation). On the other hand, (assuming we are able to measure parity directly without having to count photons) parity only fetches partial information about the unknown phase and leads to phase estimation at the QCRB for some particular values of phase (local phase estimation). The important advantage of parity measurement over photon counting, however, is that there is no need for any pre–, or post–data processing. Photon counting-based strategies typically work via the construction of the likelihood function ahead of every detection event based on the conditional probability distribution of phase conditioned on the previous detection outcome [93, 143]. In general, after a sequence of detection events, the error in the phase estimate is determined by the variance of the likelihood function, $\sigma^2 = 1/(MF_C)$, where M is the number of measurements and F_C is the classical Fisher information. The classical Fisher information for parity detection, however, as shown in (5.5.9), is equivalent to the error propagation formula. Hence, the phase sensitivity can be calculated as a simple function of the expectation value of parity (the signal) alone, without the need for much pre–, or post–data processing as is required with photon-number counting.

On the flip side, parity detection suffers from some major drawbacks. First of all, its performance is highly susceptible to photon losses. Thus, it becomes very crucial to maintain lossless conditions in order to apply parity detection. Secondly, an efficient implementation of photon-number parity measurement without having to count photons and infer parity remains elusive. There have been some promising proposals for its efficient implementation. Gerry and co-workers suggested the use of optical nonlinearities [70, 71]. Plick *et al.* showed that homodyne quantum state tomography can be used to construct the expected parity signal, at least in the case of Gaussian states, since the expectation value of the parity operator is proportional to the value of the Wigner function of the state at the origin in phase space for such states [149, 157]. However, remain unsatisfactory. For example, the latter scheme of [149, 157] successfully reconstructs the parity expectation value (the signal) from homodyne measurements. Those homodyne measurements are but themselves shot noise limited and hence the scheme is essentially shot-noise limited. Thus, it remains an open problem to find a way to implement photon number parity observable efficiently.

Chapter 6
Conclusions and Outlook

6.1 Summary of Findings

In the first part of the thesis, we considered the Rényi generalizations of the quantum conditional mutual information (QCMI) proposed in [18, 17] (also discussed in Appendix B). Such generalizations of the QCMI have been much sought after for quite some time now. For a tripartite state ρ_{ABC}, the proposed quantities $I_\alpha(A; B|C)$ and $\widetilde{I}_\alpha(A; B|C)$ (Definitions B.1 and B.3) satisfy many of the desired properties of such a Rényi generalization for the QCMI, e.g., they are non-negative, converge to the von Neumann entropy-based QCMI in a suitable limit of the Rényi parameter, obey a duality relation and are monotone non-increasing under local quantum operations on system B. Numerical evidence has not ruled out monotonicity under local operations on system A either, but unfortunately it has not been proven yet. We used one of the proposed Rényi QCMIs to define a Rényi bipartite squashed entanglement and a Rényi bipartite quantum discord. By taking as a conjecture that the Rényi QCMI of a tripartite state ρ_{ABC} is monotone under local CPTP maps on both systems A and B, we proved various properties of these quantities and establish them as valid measures of quantum correlation.

One important contribution of the work in Appendix B on the Rényi QCMI was a conjecture that the proposed Rényi QCMIs are monotone increasing in the Rényi parameter. If proven to be true, this conjecture would imply the following lower bound on von Neumann entropy-based QCMI

$$
\begin{aligned}
I(A; B|C) &\geq I_{1/2}(A; B|C) && (6.1.1)\\
&= -\log F\left(\rho_{ABC}, \mathcal{R}^{\mathcal{P}}_{C\to AC}(\rho_{BC})\right), && (6.1.2)
\end{aligned}
$$

where $\mathcal{R}^{\mathcal{P}}_{C\to AC}$ is a quantum channel known as the Petz recovery map. Inspired by this lower bound, we defined a new quantum called the fidelity of recovery of a tripartite state, given by

$$F(A; B|C)_\rho \equiv \sup_{\mathcal{R}_{C\to AC}} F(\rho_{ABC}, \mathcal{R}_{C\to AC}(\rho_{BC})). \tag{6.1.3}$$

The fidelity of recovery $F(A; B|C)_\rho$ of a tripartite state ρ_{ABC} captures how well a lost system A can be recovered by performing a local quantum operation on system C alone. Assuming the truth of (6.1.1), the $-\log$ of "surprisal" of the fidelity of recovery $I_F(A; B|C)_\rho$ also gives a lower bound on the QCMI as

$$I(A; B|C) \geq -\log F\left(\rho_{ABC}, \mathcal{R}^{\mathcal{P}}_{C\to AC}(\rho_{BC})\right) \geq I_F(A; B|C)_\rho \equiv -\log F(A; B|C)_\rho. \tag{6.1.4}$$

In a recent breakthrough result, Fawzi and Renner have proven the latter lower bound on the QCMI, namely the bound given by the surprisal of the fidelity of recovery. That is, we now know it is indeed true that if the QCMI of a tripartite state is small, then the state has a smaller surprisal of fidelity of recovery, or equivalently a very high fidelity of recovery. This gives a new operational characterization of approximate quantum Markov-chain states, namely states with QCMI approximately zero. The new characterization is that such states are approximately recoverable. This is in contrast with the earlier notion of approximate Markov chain states being close in trace distance from the set of quantum Markov chain states, for which counter examples are known. Our contribution for the surprisal of the fidelity of recovery was to show that it obeys all the same properties are the QCMI, e.g., it is non-negative, monotone non-increasing under local quantum operations on both systems A and B, obeys a duality relation, and satisfies a dimension bound given by $2\log|A|$.

Unlike the Rényi QCMIs, the surprisal of the fidelity of recovery is monotone under local operations on both A and B. Therefore, we further defined a squashed entanglement and quantum discord with $I_F(A;B|C)_\rho$ in place of $I(A;B|C)_\rho$. We proved that these measures satisfy many of the same properties as the original squashed entanglement and discord based on von Neumann entropies. In the case of the surprisal of measurement recoverability, we remark that the quantity is an important step forward conceptually in the understanding of quantum discord. While the traditional discord quantity captures how much correlations are lost to the environment in the act of a quantum measurement, the surprisal of measurement recoverability captures how well the lost correlations could be recovered. Further, the quantity can be equivalently be thought of as capturing how close a given state is from being a fixed point of an entanglement-breaking channel. This should be put in contrast against other discord-like measures that have been proposed in the literature that capture how close a given state is from being a zero-discord state. Given our recent understanding of approximate quantum Markov chain states as being approximately recoverable and not necessarily close in trace distance to the set of quantum Markov chain states, we draw into question discord-like measures of the latter type.

In the second part of the thesis, we presented results on pure-state quantum optical metrology based on the measurement of photon-number parity. We considered the general problem of identifying the class of pure states for which photon number parity detection is optimal. Hofmann had already solved the analogous problem for photon number counting-based detection strategies. He had derived a condition called path symmetry as a sufficient condition on pure states for which photon number counting was optimal. Since photon number parity is a subset of photon number counting, we narrowed down our search to Hofmann's path-symmetric states. We analytically proved that photon number parity is optimal for local phase estimation, i.e., at particular values of phase, for a restricted class of path-symmetric states. The restricted class is characterized by two conditions: a) path-symmetric states that have all real coefficients in the Schwinger basis, or b) path-symmetric states whose coefficients in the Schwinger basis have periodic phases. We argued that these restriction occur rather naturally in a linear interferometer, and therefore still capture almost all pure states that have been considered for quantum metrology. This includes coherent states, squeezed states, twin Fock states, N00Nstates, etc.

Further, we applied parity detection to the particular case of coherent-mixed with squeezed vacuum light interferometry. This state is evidently path symmetric. Therefore, as expected, photon number parity detection was found to be optimal for this state. Since when coherent state and squeezed vacuum state are mixed in equal intensities, the interferometric scheme is capable of Heisenberg-limited phase estimation, we demonstrated that parity achieves the Heisenberg limit with this scheme at particular values of phase. We also compared the performance of photon number parity with respect to a homodyne-based detection scheme proposed by Ono and Hofmann, which was also shown to be optimal for the coherent-mixed with squeezed vacuum light interferometry. We found that although both the detection schemes achieve optimality, parity performances better over a broader range of values of the phase around the optimum as compared to the scheme suggested by Ono and Hofmann.

6.2 Future Directions

Rényi generalizations of the quantum conditional mutual information. As mentioned before, the proposed Rényi generalizations of the QCMIs have only been proven to be monotone non-increasing under local quantum operations on one of the two systems A or B, while numerical tests have not failed in upholding the monotonicity with respect to the other system either. It is thus an important open question to prove this monotonicity in order to completely validate the proposed quantities as truly useful Rényi generalizations of the QCMI. Another problem that has been left open is the proof of the conjectured monotonicity of the proposed Rényi QCMIs in the Rényi parameter. Finally, it is largely left open to use the proposed Rényi QCMIs to characterize quantum state redistribution in the one-shot setting [7, 127].

Rényi squashed entanglement and discord. As far as properties of these quantities are concerned, there are several of them left to be proved. For example, we have left open the converse part of faithfulness for both the Rényi squashed entanglement as well as the Rényi discord; i.e., the proof of the statements that the Rényi squashed entanglement is equal to zero only if the state is separable, and Rényi discord is equal to zero only if the state is classical-quantum. Also, while the von Neumann entropy-based squashed entanglement is known to be superadditive in general and additive on tensor-product states, we have only been able to show that the Rényi squashed entanglement is subadditive on tensor-product states; super-additivity of the Rényi squashed entanglement in general has been left open.

As far as applications are concerned, it is an open question if the von Neumann entropy based squashed entanglement is a strong converse rate for entanglement distillation. The Rényi squashed entanglement may potentially be of use in proving this. One may also try to use the Rényi squashed entanglement to strengthen the results of [178, 177] by showing that the von Neumann entropy-based squashed entanglement is a strong converse rate for the two-way assisted quantum capacity of any channel. As for the Rényi discord, one interesting open question is to determine if a Koashi-Winter type [112] relation holds.

Fidelity of recovery, geometric squashed entanglement and surprisal of measurement recoverability. At the moment, we only have a weak chain rule for the fidelity of recovery. It is thus an open question to prove a chain rule akin to that of the von Neumann entropy-based QCMI. Such a chain rule might also be helpful in establishing that the geometric squashed entanglement is monogamous. As for the geometric squashed entanglement, an interesting question is if the geometric squashed entanglement can be used to characterize the one-shot distillable entanglement or secret key of a bipartite state. Another interesting question is on the continuity. At the moment, we have only proven continuity, and not asymptotic continuity as in the Alicki-Fannes' inequality. So, asymptotic continuity of the quantity is left open. Also, another question of interest is if we can show that geometric squashed entanglement is non-lockable [36]. Preliminary evidence from considering the strongest known locking schemes from [61] suggests that it might not be lockable.

Bibliography

[1] Luigi Accardi and Alberto Frigerio. Markovian Cocycles. *Proceedings of the Royal Irish Academy. Section A: Mathematical and Physical Sciences*, 83A(2):251–263, December 1983.

[2] Gerardo Adesso, Davide Girolami, and Alessio Serafini. Measuring Gaussian quantum information and correlations using the Rényi entropy of order 2. *Physical Review Letters*, 109(19):190502, November 2012. arXiv:1203.5116.

[3] Itai Afek, Oron Ambar, and Yaron Silberberg. High-N00N states by mixing quantum and classical light. *Science*, 328(5980):879–881, 2010.

[4] Robert Alicki and Mark Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37(5):L55, February 2004. arXiv:quant-ph/0312081.

[5] Tsuyoshi Ando. Convexity of certain maps on positive definite matrices and applications to Hadamard products. *Linear Algebra and its Applications*, 26:203–241, 1979.

[6] Petr M. Anisimov, Gretchen M. Raterman, Aravind Chiruvelli, William N. Plick, Sean D. Huver, Hwang Lee, and Jonathan P. Dowling. Quantum metrology with two-mode squeezed vacuum: Parity detection beats the Heisenberg limit. *Physical Review Letters*, 104:103602, Mar 2010.

[7] Anurag Anshu, Vamsi Krishna Devabathini, and Rahul Jain. Near optimal bounds on quantum communication complexity of single-shot quantum state redistribution, 2014. arXiv:1410.3031v2.

[8] Suguru Arimoto. On the converse to the coding theorem for discrete memoryless channels (corresp.). *IEEE Transactions on Information Theory*, 19(3):357–359, 1973.

[9] John C. Baez. Rényi Entropy and Free Energy, 2011. arXiv:1102.2098v3.

[10] Pascal Basler. Characterization of correlations in classical and quantum systems. Master's thesis, ETH Zurich, October 2012.

[11] Salman Beigi. Sandwiched Rényi divergence satisfies data processing inequality. *Journal of Mathematical Physics*, 54(12):122202, December 2013. arXiv:1306.5920.

[12] C H Bennett and G Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages pp. 175–179. IEEE, 1984.

[13] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046–2052, April 1996. arXiv:quant-ph/9511030.

[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. *Physical Review Letters*, 70:1895–1899, Mar 1993.

[15] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, November 1996. arXiv:quant-ph/9604024.

[16] D. W. Berry and H. M. Wiseman. Optimal states and almost optimal adaptive measurements for quantum interferometry. *Physical Review Letters*, 85:5098–5101, Dec 2000.

[17] Mario Berta, Kaushik P. Seshadreesan, and Mark M. Wilde. Rényi generalizations of quantum information measures. *Physical Review A*, 91:022333, Feb 2015.

[18] Mario Berta, Kaushik P. Seshadreesan, and Mark M. Wilde. Rényi generalizations of the conditional quantum mutual information. *Journal of Mathematical Physics*, 56(2):022205, 2015.

[19] J. J . Bollinger, Wayne M. Itano, D. J. Wineland, and D. J. Heinzen. Optimal frequency measurements with maximally correlated states. *Physical Review A*, 54:R4649–R4652, Dec 1996.

[20] Luca Bombelli, Rabinder K. Koul, Joohan Lee, and Rafael D. Sorkin. Quantum source of entropy for black holes. *Physical Review D*, 34:373–383, Jul 1986.

[21] Roy S. Bondurant and Jeffrey H. Shapiro. Squeezed states in phase-sensing interferometers. *Physical Review D*, 30:2548–2556, Dec 1984.

[22] Agedi N. Boto, Pieter Kok, Daniel S. Abrams, Samuel L. Braunstein, Colin P. Williams, and Jonathan P. Dowling. Quantum interferometric optical lithography: Exploiting entanglement to beat the diffraction limit. *Physical Review Letters*, 85:2733–2736, Sep 2000.

[23] Dirk Bouwmeester. Quantum physics: High noon for photons. *Nature*, 429:139–141, May 2004.

[24] Fernando G S L Brandao and Michal Horodecki. An area law for entanglement from exponential decay of correlations. *Nature Physics*, 9(11):721–726, November 2013. arXiv:1309.3789.

[25] Fernando G.S.L. Brandao, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, September 2011. arXiv:1010.1750.

[26] Samuel L. Braunstein and Carlton M. Caves. Statistical distance and the geometry of quantum states. *Physical Review Letters*, 72:3439–3443, May 1994.

[27] Samuel L. Braunstein, Carlton M. Caves, and Gerard J. Milburn. Generalized uncertainty relations: Theory, examples, and Lorentz invariance. *Annals of Physics*, 247:135, 1996.

[28] Mark Braverman. Interactive information complexity. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 505–524, New York, NY, USA, 2012. ACM.

[29] G. Brida, M. Genovese, and Ruo BercheraI. Experimental realization of sub-shot-noise quantum imaging. *Nature Photonics*, 4(4):227–230, April 2010.

[30] Pasquale Calabrese and John Cardy. Entanglement entropy and quantum field theory. *Journal of Statistical Mechanics: Theory and Experiment*, 2004(06):P06002, 2004.

[31] Pasquale Calabrese and John Cardy. Entanglement entropy and conformal field theory. *Journal of Physics A: Mathematical and Theoretical*, 42(50):504005, 2009. arXiv:0905.4013.

[32] J. Calsamiglia, R. Muñoz Tapia, Ll. Masanes, A. Acin, and E. Bagan. Quantum Chernoff bound as a measure of distinguishability between density matrices: Application to qubit and Gaussian states. *Physical Review A*, 77:032311, March 2008. arXiv:0708.2343.

[33] Eric A. Carlen and Elliott H. Lieb. Remainder terms for some quantum entropy inequalities. *Journal of Mathematical Physics*, 55(4):042201, April 2014. arXiv:1402.3840.

[34] Carlton M. Caves. Quantum-mechanical noise in an interferometer. *Physical Review D*, 23:1693–1708, Apr 1981.

[35] Lin Chen, Martin Aulbach, and Michal Hajdusek. Comparison of different definitions of the geometric measure of entanglement. *Physical Review A*, 89:042305, Apr 2014.

[36] Matthias Christandl. *The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography*. PhD thesis, University of Cambridge, April 2006. arXiv:quant-ph/0604183.

[37] Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner. *Proceedings of the 4th Theory of Cryptography Conference, Lecture Notes in Computer Science*, 4392:456–478, 2007. arXiv:quant-ph/0608199.

[38] Matthias Christandl, Robert Kónig, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[39] Matthias Christandl, Norbert Schuch, and Andreas Winter. Entanglement of the antisymmetric state. *Communications in Mathematical Physics*, 311(2):397–422, April 2012. arXiv:0910.4151.

[40] Matthias Christandl and Andreas Winter. "Squashed entanglement": An additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, March 2004. arXiv:quant-ph/0308088.

[41] Nikola Ciganovic, Normand J. Beaudry, and Renato Renner. Smooth max-information as one-shot generalization for mutual information. *IEEE Transactions on Information Theory*, 60(3):1573–1581, March 2014. arXiv:1308.5884.

[42] Thomas Cooney, Milan Mosonyi, and Mark M. Wilde. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. August 2014. arXiv:1408.3373.

[43] Andrea Crespi, Mirko Lobino, Jonathan C. F. Matthews, Alberto Politi, Chris R. Neal, Roberta Ramponi, Roberto Osellame, and Jeremy L. O'Brien. Measuring protein concentration with entangled photons. *Applied Physics Letters*, 100(23):233704, 2012.

[44] Toby Cubitt. Matlab quantum information package (quantinf v0.5.1). `http://www.dr-qubit.org/matlab.php`, 2009.

[45] Oscar C O Dahlsten, Renato Renner, Elisabeth Rieper, and Vlatko Vedral. Inadequacy of von Neumann entropy for characterizing extractable work. *New Journal of Physics*, 13(5):053015, 2011.

[46] Nilanjana Datta and Felix Leditzky. A limit of the quantum Rényi divergence. *Journal of Physics A: Mathematical and Theoretical*, 47(4):045304, January 2014. arXiv:1308.5961.

[47] Nilanjana Datta and Mark M. Wilde. Quantum Markov chains, sufficiency of quantum channels, and Rényi information measures, 2015. arXiv:1501.05636v3.

[48] Rafal Demkowicz-Dobrzanski, Jan Kolodynski, and Madalin Guta. The elusive Heisenberg limit in quantum-enhanced metrology. *Nature Communications*, 3:1063, September 2012.

[49] Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Physical Review Letters*, 100(23):230501, June 2008.

[50] U. Dorner, R. Demkowicz-Dobrzanski, B. J. Smith, J. S. Lundeen, W. Wasilewski, K. Banaszek, and I. A. Walmsley. Optimal quantum phase estimation. *Physical Review Letters*, 102:040403, Jan 2009.

[51] Jonathan P. Dowling. Quantum optical metrology—the lowdown on high-N00N states. *Contemporary Physics*, 49(2):125–143, 2008.

[52] Jonathan P. Dowling and Gerard J. Milburn. Quantum technology: the second quantum revolution. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 361(1809):1655–1674, 2003.

[53] W. Dür, L. Hartmann, M. Hein, M. Lewenstein, and H.-J. Briegel. Entanglement in spin chains and lattices with long-range ising-type interactions. *Physical Review Letters*, 94:097203, Mar 2005.

[54] Gabriel A. Durkin and Jonathan P. Dowling. Local and global distinguishability in quantum interferometry. *Physical Review Letters*, 99:070801, Aug 2007.

[55] J. Eisert, M. Cramer, and M. B. Plenio. Colloquium. *Reviews of Modern Physics*, 82:277–306, Feb 2010.

[56] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, Aug 1991.

[57] Berthold-Georg Englert. Fringe visibility and which-way information: An inequality. *Physical Review Letters*, 77:2154–2157, Sep 1996.

[58] Paul Erker. How not to Rényi generalize the quantum conditional mutual information. April 2014. arXiv:1404.3628.

[59] B M Escher, R L de Matos Filho, and L Davidovich. General framework for estimating the ultimate precision limit in noisy quantum-enhanced metrology. *Nature Physics*, 7(5):406–411, May 2011.

[60] Fabian H. L. Essler, Andreas M. Läuchli, and Pasquale Calabrese. Shell-filling effect in the entanglement entropies of spinful fermions. *Physical Review Letters*, 110:115701, Mar 2013.

[61] Omar Fawzi, Patrick Hayden, and Pranab Sen. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, pages 773–782, 2011. arXiv:1010.3007.

[62] Omar Fawzi and Renato Renner. Quantum conditional mutual information and approximate Markov chains. October 2014. arXiv:1410.0664.

[63] Steven T. Flammia, Alioscia Hamma, Taylor L. Hughes, and Xiao-Gang Wen. Topological entanglement Rényi entropy and reduced density matrix structure. *Physical Review Letters*, 103(26):261601, December 2009. arXiv:0909.3305.

[64] F Franchini, A R Its, and V E Korepin. Rényi entropy of the XY spin chain. *Journal of Physics A: Mathematical and Theoretical*, 41(2):025302, 2008.

[65] Rupert L. Frank and Elliott H. Lieb. Monotonicity of a relative Rényi entropy. *Journal of Mathematical Physics*, 54(12):122201, December 2013. arXiv:1306.5358.

[66] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, May 1998. arXiv:quant-ph/9712042.

[67] Motohisa Fukuda, Ion Nechita, and Michael M. Wolf. Quantum channels with polytopic images and image additivity. August 2014. arXiv:1408.2340.

[68] Yang Gao, Petr M. Anisimov, Christoph F. Wildfeuer, Jerome Luine, Hwang Lee, and Jonathan P. Dowling. Super-resolution at the shot-noise limit with coherent states and photon-number-resolving detectors. *Journal of the Optical Society of America B*, 27(6):A170–A174, Jun 2010.

[69] C. C. Gerry and P. L. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[70] Christopher C. Gerry. Heisenberg-limit interferometry with four-wave mixers operating in a nonlinear regime. *Physical Review A*, 61(4):043811, Mar 2000.

[71] Christopher C. Gerry, A. Benmoussa, and R. A. Campos. Quantum nondemolition measurement of parity and generation of parity eigenstates in optical fields. *Physical Review A*, 72(5):053818, Nov 2005.

[72] Christopher C. Gerry and Jihane Mimih. The parity operator in quantum optical metrology. *Contemporary Physics*, 51(6):497–511, 2010.

[73] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced positioning and clock synchronization. *Nature*, 412(6845):417–419, July 2001.

[74] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum metrology. *Physical Review Letters*, 96:010401, Jan 2006.

[75] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, pages 212–219. ACM, 1996.

[76] ManishK. Gupta and MarkM. Wilde. Multiplicativity of completely bounded p-norms implies a strong converse for entanglement-assisted capacity. *Communications in Mathematical Physics*, 334(2):867–887, 2015.

[77] M B Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, 2007(08):P08024, 2007. arXiv:0705.2024.

[78] Masahito Hayashi. *Quantum Information: An Introduction*. Springer, 2006.

[79] Masahito Hayashi. Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding. *Physical Review A*, 76:062301, Dec 2007.

[80] Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of states which satisfy strong subadditivity of quantum entropy with equality. *Communications in Mathematical Physics*, 246(2):359–374, April 2004. arXiv:quant-ph/0304007.

[81] Patrick M Hayden, Michal Horodecki, and Barbara M Terhal. The asymptotic entanglement cost of preparing a quantum state. *Journal of Physics A: Mathematical and General*, 34(35):6891, 2001.

[82] Matthew Headrick. Entanglement Rényi entropies in holographic theories. *Physical Review D*, 82(12):126010, December 2010. arXiv:1006.0047.

[83] Matthew Headrick and Tadashi Takayanagi. Holographic proof of the strong subadditivity of entanglement entropy. *Physical Review D*, 76(10):106013, November 2007. arXiv:0704.3719.

[84] Carl W. Helstrom. Quantum detection and estimation theory. *Academic Press*, 1976.

[85] Fumio Hiai. Concavity of certain matrix trace and norm functions. *Linear Algebra and its Applications*, 439(5):1568–1589, 2013. arXiv:1210.7524.

[86] B. L. Higgins, D. W. Berry, S. D. Bartlett, H. M. Wiseman, and G. J. Pryde. Entanglement-free Heisenberg-limited phase estimation. *Nature*, 450(7168):393–396, 11 2007.

[87] Holger F. Hofmann. All path-symmetric pure states achieve their maximal phase sensitivity in conventional two-path interferometry. *Physical Review A*, 79:033822, Mar 2009.

[88] Holger F. Hofmann and Takafumi Ono. High-photon-number path entanglement in the interference of spontaneously down-converted photon pairs with coherent laser light. *Physical Review A*, 76:031806, Sep 2007.

[89] Alexander S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[90] Alexander S. Holevo. *Probabilistic and Statistical Aspects of Quantum Theory*. North Holland, Amsterdam, 1982.

[91] A.S. Holevo. The capacity of the quantum channel with general signal states. *Information Theory, IEEE Transactions on*, 44(1):269–273, Jan 1998.

[92] AS. Holevo. Reliability function of general classical-quantum channel. *Information Theory, IEEE Transactions on*, 46(6):2256–2261, Sep 2000.

[93] M. J. Holland and K. Burnett. Interferometric detection of optical phase shifts at the Heisenberg limit. *Physical Review Letters*, 71:1355–1358, Aug 1993.

[94] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94:160502, Apr 2005.

[95] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(06):629–641, 2003.

[96] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. arXiv:quant-ph/0702225v2.

[97] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac. Improvement of frequency standards with quantum entanglement. *Physical Review Letters*, 79:3865–3868, Nov 1997.

[98] Sean D. Huver, Christoph F. Wildfeuer, and Jonathan P. Dowling. Entangled fock states for robust quantum optical metrology, imaging, and sensing. *Physical Review A*, 78:063828, Dec 2008.

[99] Philipp Hyllus, Otfried Gühne, and Augusto Smerzi. Not all pure entangled states are useful for sub-shot-noise interferometry. *Physical Review A*, 82:012337, Jul 2010.

[100] Ben Ibinson, Noah Linden, and Andreas Winter. Robustness of quantum Markov chains. *Communications in Mathematical Physics*, 277(2):289–304, January 2008. arXiv:quant-ph/0611057.

[101] Y. Israel, I. Afek, S. Rosen, O. Ambar, and Y. Silberberg. Experimental tomography of noon states with large photon numbers. *Physical Review A*, 85:022115, Feb 2012.

[102] Yonatan Israel, Shamir Rosen, and Yaron Silberberg. Supersensitive polarization microscopy using noon states of light. *Physical Review Letters*, 112:103604, Mar 2014.

[103] Anna Jencova and Denes Petz. Sufficiency in quantum statistical inference. *Communications in Mathematical Physics*, 263(1):259–276, January 2006. arXiv:math-ph/0412093.

[104] Anna Jencova and Mary Beth Ruskai. A unified treatment of convexity of relative entropy and related trace functions, with conditions for equality. *Reviews in Mathematical Physics*, 22(9):1099–1121, October 2010. arXiv:0903.2895.

[105] Kebei Jiang, Chase J. Brignac, Yi Weng, Moochan B. Kim, Hwang Lee, and Jonathan P. Dowling. Strategies for choosing path-entangled number states for optimal robust quantum-optical metrology in the presence of loss. *Physical Review A*, 86:013826, Jul 2012.

[106] Kebei Jiang, Hwang Lee, Christopher C. Gerry, and Jonathan P. Dowling. Super-resolving quantum radar: Coherent-state sources with homodyne detection suffice to beat the diffraction limit. *Journal of Applied Physics*, 114(19):193102, 2013.

[107] B. E. Kardyna, Z. L. Yuan, and A. J. Shields. An avalanche-photodiode-based photon-number-resolving detector. *Nature Photonics*, 2:425–428, Jun 2008.

[108] Isaac Kim. unpublished manuscript. communicated by email on March 27, 2014.

[109] Isaac H. Kim. Application of conditional independence to gapped quantum many-body systems. http://www.physics.usyd.edu.au/quantum/Coogee2013, January 2013. Slide 43.

[110] Sergey Knysh, Vadim N. Smelyanskiy, and Gabriel A. Durkin. Scaling laws for precision in quantum interferometry and the bifurcation landscape of the optimal state. *Physical Review A*, 83:021804, Feb 2011.

[111] Sergey I. Knysh, Edward H. Chen, and Gabriel A. Durkin. True Limits to Precision via Unique Quantum Probe, 2014. arXiv:1402.0495v1.

[112] Masato Koashi and Andreas Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69:022309, Feb 2004.

[113] Pieter Kok, Agedi N. Boto, Daniel S. Abrams, Colin P. Williams, Samuel L. Braunstein, and Jonathan P. Dowling. Quantum-interferometric optical lithography: Towards arbitrary two-dimensional patterns. *Physical Review A*, 63:063407, May 2001.

[114] Pieter Kok, Samuel L Braunstein, and Jonathan P Dowling. Quantum lithography, entanglement and Heisenberg-limited parameter estimation. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(8):S811, 2004.

[115] Jan Kolodynski. *Precision bounds in noisy quantum metrology.* PhD thesis, 2014. arXiv:1409.0535v1.

[116] Robert Konig and Stephanie Wehner. A strong converse for classical channel coding using entangled inputs. *Physical Review Letters*, 103:070504, August 2009. arXiv:0903.2838.

[117] Oscar E. Lanford and Derek W. Robinson. Mean entropy of states in quantum statistical mechanics. *Journal of Mathematical Physics*, 9(7):1120–1125, July 1968.

[118] Tae-Woo Lee, Sean D. Huver, Hwang Lee, Lev Kaplan, Steven B. McCracken, Changjun Min, Dmitry B. Uskov, Christoph F. Wildfeuer, Georgios Veronis, and Jonathan P. Dowling. Optimization of quantum interferometric metrological sensors in the presence of photon loss. *Physical Review A*, 80:063803, Dec 2009.

[119] Hui Li and F. D. M. Haldane. Entanglement spectrum as a generalization of entanglement entropy: Identification of topological order in non-abelian fractional quantum Hall effect states. *Physical Review Letters*, 101(1):010504, July 2008. arXiv:0805.0332.

[120] Ke Li and Andreas Winter. Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps. 2014. arXiv:1410.4184v2.

[121] Elliot H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Advances in Mathematics*, 11(3):267–288, December 1973.

[122] Elliott H. Lieb and Mary Beth Ruskai. A fundamental property of quantum-mechanical entropy. *Physical Review Letters*, 30(10):434–436, March 1973.

[123] Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. *Journal of Mathematical Physics*, 14(12):1938–1941, December 1973.

[124] Noah Linden, Milán Mosonyi, and Andreas Winter. The structure of Rényi entropic inequalities. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, 469(2158):20120737, October 2013. arXiv:1212.0248.

[125] Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency. *Optics Express*, 16(5):3032–3040, Mar 2008.

[126] L A Lugiato, A Gatti, and E Brambilla. Quantum imaging. *Journal of Optics B: Quantum and Semiclassical Optics*, 4(3):S176, 2002.

[127] Dave Touchette Mario Berta, Matthias Christandl. Smooth Entropy Bounds on One-Shot Quantum State Redistribution, 2014. arXiv:1409.4338v1.

[128] Avijit Misra, Anindya Biswas, Arun K. Pati, Aditi Sen De, and Ujjwal Sen. Quantum correlation with sandwiched relative entropies. June 2014. arXiv:1406.5065v1.

[129] Kavan Modi, Aharon Brodutch, Hugo Cable, Tomasz Paterek, and Vlatko Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Reviews of Modern Physics*, 84(4):1655–1707, November 2012. arXiv:1112.6238.

[130] Milán Mosonyi and Fumio Hiai. On the quantum Rényi relative entropies and related capacity formulas. *IEEE Transactions on Information Theory*, 57(4):2474–2487, April 2011. arXiv:0912.1286.

[131] Miln Mosonyi and Tomohiro Ogawa. Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. *Communications in Mathematical Physics*, 334(3):1617–1648, 2015.

[132] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. On quantum Rényi entropies: a new definition and some properties. *Journal of Mathematical Physics*, 54(12):122203, December 2013. arXiv:1306.3142.

[133] Tomohisa Nagata, Ryo Okamoto, Jeremy L. O'Brien, Keiji Sasaki, and Shigeki Takeuchi. Beating the standard quantum limit with four-entangled photons. *Science*, 316(5825):726–729, 2007.

[134] Tomohiro Ogawa and Hiroshi Nagaoka. Strong converse to the quantum channel coding theorem. *IEEE Transactions on Information Theory*, 45(7):2486–2489, November 1999. arXiv:quant-ph/9808063.

[135] Robert Olkiewicz and Boguslaw Zegarlinski. Hypercontractivity in noncommutative L_p spaces. *Journal of Functional Analysis*, 161(1):246–285, January 1999.

[136] Harold Ollivier and Wojciech H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Physical Review Letters*, 88(1):017901, December 2001. arXiv:quant-ph/0105072.

[137] Takafumi Ono and Holger F. Hofmann. Effects of photon losses on phase estimation near the Heisenberg limit using coherent light and squeezed vacuum. *Physical Review A*, 81(3):033819, Mar 2010.

[138] Takafumi Ono, Ryo Okamoto, and Shigeki Takeuchi. An entanglement-enhanced microscope. *Nature Communications*, 4, September 2013.

[139] D. T. Pegg and S. M. Barnett. Unitary phase operator in quantum mechanics. *Europhysics Letters*, 6(6):483, 1988.

[140] Dénes Petz. Quasi-entropies for finite quantum systems. *Reports in Mathematical Physics*, 23(1):57–65, February 1986.

[141] Denes Petz. Sufficiency of channels over von neumann algebras. *The Quarterly Journal of Mathematics*, 39(1):97–108, 1988.

[142] Dénes Petz. Monotonicity of quantum relative entropy revisited. *Reviews in Mathematical Physics*, 15(1):79, March 2003. arXiv:quant-ph/0209053.

[143] Luca Pezzé and Augusto Smerzi. Mach-zehnder interferometry at the Heisenberg limit with coherent and squeezed-vacuum light. *Physical Review Letters*, 100:073601, Feb 2008.

[144] Luca Pezzé and Augusto Smerzi. Entanglement, nonlinear dynamics, and the Heisenberg limit. *Physical Review Letters*, 102:100401, Mar 2009.

[145] M. Piani. Problem with geometric discord. *Physical Review A*, 86:034101, Sep 2012.

[146] M Piani, V Narasimhachar, and J Calsamiglia. Quantumness of correlations, quantumness of ensembles and quantum data hiding. *New Journal of Physics*, 16(11):113001, 2014.

[147] Matthew Pitkin, Stuart Reid, Sheila Rowan, and James Hough. Gravitational wave detection by interferometry (ground and space). *Living Reviews in Relativity*, 14(5), 2011.

[148] M. B. Plenio, J. Eisert, J. Dreißig, and M. Cramer. Entropy, entanglement, and area: Analytical results for harmonic lattice systems. *Physical Review Letters*, 94:060503, Feb 2005.

[149] William N Plick, Petr M Anisimov, Jonathan P Dowling, Hwang Lee, and Girish S Agarwal. Parity detection in quantum optical metrology without number-resolving detectors. *New Journal of Physics*, 12(11):113025, 2010.

[150] Y. Polyanskiy and S. Verdú. Arimoto channel coding converse and Rényi divergence. *Proceedings of the 48th Allerton Conference on Communication, Control, and Computing, (Monticello, USA)*, September 2010.

[151] M. Jarzyna R. Demkowicz-Dobrzanski and J. Kolodynski. Quantum limits in optical interferometry, 2014. arXiv:1405.7703v2.

[152] Eric M. Rains. Bound on distillable entanglement. *Physical Review A*, 60(1):179–184, July 1999. arXiv:quant-ph/9809082.

[153] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zürich, December 2005. arXiv:quant-ph/0512258.

[154] A. Rényi. A matrix convexity approach to some celebrated quantum inequalities. *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability: held at the Statistical Laboratory, University of California, 1960, edited by J. Neyman (University of California Press, Berkeley, 1961)*, page 547, 1961.

[155] Danna Rosenberg, Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. Noise-free high-efficiency photon-number-resolving detectors. *Physical Review A*, 71:061803, Jun 2005. arXiv:quant-ph/0506175v1.

[156] Bhaskar Roy Bardhan, Kebei Jiang, and Jonathan P. Dowling. Effects of phase fluctuations on phase sensitivity and visibility of path-entangled photon Fock states. *Physical Review A*, 88:023857, Aug 2013.

[157] Antoine Royer. Wigner function as the expectation value of a parity operator. *Physical Review A*, 15:449–450, Feb 1977.

[158] Lee A. Rozema, James D. Bateman, Dylan H. Mahler, Ryo Okamoto, Amir Feizpour, Alex Hayat, and Aephraim M. Steinberg. Scalable spatial superresolution using entangled photons. *Physical Review Letters*, 112:223602, Jun 2014. arXiv:1312.2012v1.

[159] Mary Beth Ruskai. Inequalities for quantum entropy: A review with conditions for equality. *Journal of Mathematical Physics*, 43(9):4358–4375, September 2002. arXiv:quant-ph/0205064.

[160] J. J. Sakurai. *Modern Quantum Mechanics*. Addison Wesley, 1994.

[161] Barry C. Sanders. Quantum dynamics of the nonlinear rotator and the effects of continual spin measurement. *Physical Review A*, 40:2417–2427, Sep 1989.

[162] Benjamin Schumacher. Quantum coding. *Physical Review A*, 51(4):2738–2747, April 1995.

[163] Benjamin Schumacher and Michael D. Westmoreland. Sending classical information via noisy quantum channels. *Physical Review A*, 56:131–138, Jul 1997.

[164] Kaushik Seshadreesan, Mario Berta, and Mark M. Wilde. Rényi squashed entanglement, discord, and relative entropy differences. October 2014. arXiv:1410.1443.

[165] Kaushik P. Seshadreesan, Petr M. Anisimov, Hwang Lee, and Jonathan P. Dowling. Parity detection achieves the Heisenberg limit in interferometry with coherent mixed with squeezed vacuum light. *New Journal of Physics*, 13(8):083026, 2011.

[166] Kaushik P. Seshadreesan, Sejong Kim, Jonathan P. Dowling, and Hwang Lee. Phase estimation at the quantum Cramér-Rao bound via parity detection. *Physical Review A*, 87:043833, Apr 2013.

[167] Kaushik P. Seshadreesan and Mark M. Wilde. Fidelity of recovery and geometric squashed entanglement. October 2014. arXiv:1410.1441.

[168] R. Shankar. *Principles of Quantum Mechanics (2nd Ed. Springer, 1994), Chap. 9, p. 237-240.*

[169] Naresh Sharma and Naqueeb Ahmad Warsi. On the strong converses for the quantum channel capacity theorems. June 2012. arXiv:1205.1712.

[170] Y. Shih. Quantum imaging. *Selected Topics in Quantum Electronics, IEEE Journal of*, 13(4):1016–1030, July 2007.

[171] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Scientific Computing*, 26:1484, 1997.

[172] Robin Sibson. Information radius. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 14(2):149160, 1969.

[173] Sergey N. Solodukhin. Entanglement entropy of black holes. *Living Reviews in Relativity*, 14(8), 2011.

[174] Mark Srednicki. Entropy and area. *Physical Review Letters*, 71:666–669, Aug 1993.

[175] W. F. Stinespring. Positive functions on C*-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, April 1955.

[176] Masuo Suzuki. Transfer-matrix method and Monte Carlo simulation in quantum spin systems. *Physical Review B*, 31(5):2957, March 1985.

[177] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5:5235, October 2014.

[178] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, August 2014. arXiv:1310.0129.

[179] Michael A Taylor, Jiri Janousek, Vincent Daria, Joachim Knittel, Boris Hage, BachorHans-A., and Warwick P Bowen. Biological measurement beyond the quantum limit. *Nature Photonics*, 7(3):229–233, March 2013.

[180] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *Information Theory, IEEE Transactions on*, 56(9):4674–4681, Sept 2010.

[181] Marco Tomamichel. private communication, April 2014.

[182] Marco Tomamichel, Mario Berta, and Masahito Hayashi. A duality relation connecting different quantum generalizations of the conditional Rényi entropy. November 2013. arXiv:1311.3887.

[183] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55(12):5840–5847, December 2009. arXiv:0811.1221.

[184] Marco Tomamichel, Mark M. Wilde, and Andreas Winter. Strong converse rates for quantum communication. June 2014. arXiv:1406.2946.

[185] Dave Touchette. Direct Sum Theorem for Bounded Round Quantum Communication Complexity, 2014. arXiv:1409.4391v1.

[186] Dave Touchette. Quantum information complexity and amortized communication. April 2014. arXiv:1404.3733.

[187] Mankei Tsang. Quantum imaging beyond the diffraction limit by optical centroid measurements. *Physical Review Letters*, 102:253601, Jun 2009.

[188] Armin Uhlmann. Endlich-dimensionale Dichtematrizen II. *Wiss. Z. Karl-Marx-Univ. Leipzig, Math.-Nat. R.*, 22:139–177, 1973.

[189] Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

[190] H. Uys and P. Meystre. Quantum states for Heisenberg-limited interferometry. *Physical Review A*, 76:013804, Jul 2007.

[191] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev. Entanglement in quantum critical phenomena. *Physical Review Letters*, 90:227902, Jun 2003.

[192] Guifre Vidal. Entanglement monotones. *Journal of Modern Optics*, 47:355, 2000. arXiv:quant-ph/9807077.

[193] Mihai D Vidrighin, Gaia Donati, Marco G Genoni, Xian-Min Jin, W Steven Kolthammer, M S Kim, Animesh Datta, Marco Barbieri, and Ian A Walmsley. Joint estimation of phase and phase diffusion for quantum metrology. *Nature Communications*, 5, April 2014.

[194] Christian Weedbrook, Stefano Pirandola, Raúl Garcia-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84:621–669, May 2012.

[195] Tzu-Chieh Wei and Paul M. Goldbart. Geometric measure of entanglement and applications to bipartite and multipartite quantum states. *Physical Review A*, 68:042307, Oct 2003.

[196] Mark M. Wilde. *Quantum Information Theory.* Cambridge University Press, 2013. arXiv:1106.1445.

[197] Mark M. Wilde. Multipartite quantum correlations and local recoverability, 2014. arXiv:1412.0333v3.

[198] Mark M. Wilde, Andreas Winter, and Dong Yang. Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. *Communications in Mathematical Physics*, 331(2):593–622, October 2014. arXiv:1306.1586.

[199] Andreas Winter and Ke Li. A stronger subadditivity relation? http://www.maths.bris.ac.uk/∼csajw/stronger_subadditivity.pdf, 2012.

[200] H. M. Wiseman. Adaptive phase measurements of optical modes: Going beyond the marginal Q distribution. *Physical Review Letters*, 75:4587–4590, Dec 1995.

[201] Florian Wolfgramm, Chiara Vitelli, Federica A Beduini, Nicolas Godbout, and Morgan W Mitchell. Entanglement-enhanced probing of a delicate material system. *Nature Photonics*, 7(1):28–32, January 2013.

[202] G. Y. Xiang, B. L. Higgins, D. W. Berry, H. M. Wiseman, and G. J. Pryde. Entanglement-enhanced measurement of a completely unknown optical phase. *Nature Photonics*, 5:43–47, Jan 2011.

[203] Jon Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions in Information Theory*, 55(11):5339–5351, November 2009. arXiv:0706.2907.

[204] Horace P. Yuen and Vincent W. S. Chan. Noise in homodyne and heterodyne detection. *Optics Letters*, 8(3):177–179, Mar 1983.

[205] Bernard Yurke, Samuel L. McCall, and John R. Klauder. SU(2) and SU(1,1) interferometers. *Physical Review A*, 33:4033–4054, Jun 1986.

[206] Lin Zhang. A lower bound of quantum conditional mutual information. March 2014. arXiv:1403.1424.

[207] Wojciech H. Zurek. Einselection and decoherence from an information theory perspective. *Annalen der Physik*, 9(11-12):855–864, November 2000. arXiv:quant-ph/0011039.

Appendix A
Quantum Conditional Mutual Information[1]

A.1 Introduction

Quantum information theory is built on a powerful toolset consisting of the quantum entropy and various other information measures that are linear combinations of entropies. Entropic quantities emerge rather naturally in quantum information-theoretic problems, similar to classical information theory of Shannon. For example, consider the quantum noiseless-source coding problem studied by Schumacher [162], where an independent and identically-distributed (i.i.d.) quantum information source emits quantum states from an ensemble described by a density operator $\rho_A \equiv \{p(x), |\psi_x\rangle\}$. The entropy of ρ_A, defined as the von Neumann entropy (discussed earlier in Section 2.2.2)

$$H(A)_\rho \equiv -\operatorname{Tr}\{\rho_A \log \rho_A\}, \tag{A.1.1}$$

emerges as the optimal rate for error-free compression of the quantum data arising from the source in the limit of a large number of invocations of the source. This can be understood as due to the entropy capturing the average information content of a quantum state ρ_A. Similarly, also consider the canonical noisy channel-coding problem for classical communication over a quantum channel [91, 163]. The relevant quantity in this context is the following optimized mutual information between a classical input X and the quantum output B of the noisy channel

$$\chi(\mathcal{N}) \equiv \max_\rho I(X;B) = \max_\rho \left[H(X)_\rho + H(B)_\rho - H(XB)_\rho\right], \tag{A.1.2}$$

where the maximization is over classical-quantum states ρ_{XB} of the form

$$\rho_{XB} \equiv \sum_x p_X(x) |x\rangle\langle x|_X \otimes \mathcal{N}_{A'\to B}(\psi^x_{A'}) \tag{A.1.3}$$

and $\{\psi^x\}$ are pure states that form the codebook for the communication. This is the celebrated Holevo information $\chi(\mathcal{N})$ [89], whose regularization

$$\lim_{n\to\infty} \frac{\chi(\mathcal{N}^{\otimes n})}{n}$$

is found to be an upper bound on the optimal rate of channel encoding for error-free communication in the asymptotic limit of a large number of channel uses.

[1]This appendix is reproduced by updating and adapting the contents of Mario Berta, Kaushik P. Seshadreesan, and Mark M. Wilde, Journal of Mathematical Physics, 56(2):022205, February 2015, with the permission of AIP Publishing LLC. See Appendix E for the copyright permission from the publishers.

The usefulness of such entropic quantities transcends quantum information theory and permeates many areas of physics too. In particular, they are naturally suited to capture quantum correlations in various physical theories. For example, the von Neumann entropy, which is a central measure of information is widely used under the name of entanglement entropy to study entanglement in ground states (which are pure states) of quantum many body systems and lattice systems [191, 53], relativistic quantum field theory [30, 31], and the holographic theory of black holes [173, 83]. The entanglement entropy of a bipartite pure quantum state is calculated as the entropy of the reduced state on one of the subsystems; i.e., for a pure state $|\psi\rangle_{AB}$, it is defined to be

$$E_E\left(A;B\right)_\psi \equiv H\left(A\right) = -\operatorname{Tr}\left\{\psi_A \log \psi_A\right\} = -\operatorname{Tr}\left\{\psi_B \log \psi_B\right\}, \tag{A.1.4}$$

where $\psi_A = \operatorname{Tr}_B\left\{\psi_{AB}\right\}$ for example. It has been shown to obey many of the desired properties of an entanglement measure (see Section 2.3). In the case of a many-body ground state, the entanglement entropy captures the entanglement shared between the subsystem, whose reduced density matrix is considered, and the rest of the system across the boundary. A large body of work in the quantum many-body physics literature has focused on various questions related to the entanglement entropy, such as its scaling with respect to the size of the subsystem. The area law establishes that this scaling depends only on the area of the boundary [24, 20, 174, 148, 77, 55]. For a more general mixed bipartite state ρ_{AB}, the mutual information $I\left(A;B\right)_\rho$ offers use as a correlation measure. In essence, it captures how much more information about a bipartite quantum state can be obtained when having joint access to the two subsystems in comparison to when only having access to them separately.

In this appendix, we discuss the entropic quantity called quantum conditional mutual information (QCMI). There is plenty of motivation to study this quantity in detail. For example, in quantum information theory, while the quantum mutual information could be used to capture how correlated two quantum systems held by Alice and Bob are, it is sometimes also important to consider those correlations from the perspective of a third quantum system held by an eavesdropper Eve. This is particularly relevant in quantum cryptography, since Eve might have access to the rest of the universe (with respect to Alice and Bob) and could potentially be correlated with Alice and Bob. Likewise, in quantum many-body physics, the quantum mutual information could capture the resulting correlation between parts of a large system of particles. However, it is necessary that we consider those correlations with respect to a third system if we want to learn something about the type of interactions that caused the correlation [10]. The QCMI is the quantity of interest in both these scenarios.

We discuss various properties of the QCMI. We describe the information-theoretic task of quantum state redistribution, where the QCMI finds operational meaning. This is followed by various possible descriptions of the structure of quantum states that have zero QCMI, namely the quantum Markov chain states. Finally, we give different possible representations of the quantity in terms of the relative entropy. These representations pave the way forward towards Rényi generalizations of the quantity, which are presented in Appendix B.

A.2 Definition and Properties

Definition A.1. *The quantum conditional mutual information of a tripartite state* ρ_{ABC} *is defined as*

$$I(A;B|C)_\rho \equiv H(AC)_\rho + H(BC)_\rho - H(C)_\rho - H(ABC)_\rho, \tag{A.2.1}$$

where $H(F)_\sigma \equiv -Tr\{\sigma_F \log \sigma_F\}$ *is the von Neumann entropy of a state* σ_F *on system* F.

The QCMI is non-negative for any tripartite quantum state, a nontrivial fact, known as *strong subadditivity of quantum entropy* [122, 123]. Strong subadditivity can be viewed as a general constraint imposed on the correlations that could exist in any tripartite state, and finds extensive use in nearly all coding theorems in quantum information theory. Thus, it is widely regarded as a fundamental law of quantum information theory. Strong subadditivity also implies that the QCMI is non-increasing under the action of local quantum operations performed on the systems A and B [40]. That is, the following inequality holds

$$I(A;B|C)_\rho \geq I(A';B'|C)_\omega, \tag{A.2.2}$$

where $\omega_{A'B'C} \equiv (\mathcal{N}_{A\to A'} \otimes \mathcal{M}_{B\to B'})(\rho_{ABC})$ with $\mathcal{N}_{A\to A'}$ and $\mathcal{M}_{B\to B'}$ arbitrary local quantum operations performed on the input systems A and B, leading to output systems A' and B', respectively. This monotonicity of the QCMI under local quantum operations justifies its use as a measure of correlation between systems A and B from the perspective of C. Another interesting property of the QCMI is that for a four-party pure state ψ_{ABCD} it obeys a duality relation given by $I(A;B|C)_\psi = I(B;A|D)_\psi$ [49]. Further, the QCMI of a four-party state ρ_{ABCD} obeys an additive chain rule given by

$$I(AB;C|D)_\rho = I(A;C|D)_\rho + I(B;C|AD)_\rho, \tag{A.2.3}$$

which augments its usability in applications. Also, the QCMI obeys a dimension bound, given by

$$I(A;B|C)_\rho \leq 2\log|A|, \tag{A.2.4}$$

where $|A|$ is the dimension of system A. This bound is attained by a state of the form

$$\rho_{ABC} = \Psi_{AB} \otimes \sigma_C, \tag{A.2.5}$$

where the systems A and B are in a maximally entangled state, and are in product with some state on the system C.

A.3 Quantum State Redistribution

The QCMI finds an operational meaning in the information-theoretic task called quantum state redistribution. We describe this task now.

In quantum information theory, the task of quantum state redistribution represents the most general bipartite noiseless source coding problem. Suppose that Bob and Charlie share a tripartite state ρ_{BCD}, such that Bob holds system BD and Charlie holds system C. Let ρ_{BCD} be purified by a reference system A held by Alice, so that the overall state is a pure state $|\psi\rangle_{ABCD}$. Then the quantum state redistribution task requires Bob to transfer the share

B to Charlie using minimal resources needed to do so, such that the overall state $|\psi\rangle_{ABCD}$ remains undisturbed. The allowed resources, which are also the quantities of interest, are shared entanglement and noiseless quantum channels. (Note that classical communication other than what can be encoded in qubits is not allowed). Figure A.1 provides a pictorial description of the initial and final configurations of the task.

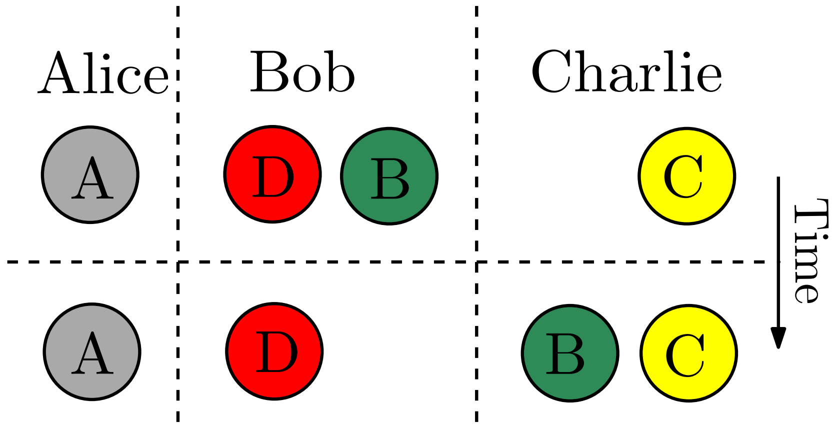

Figure A.1: The task of quantum state redistribution. Alice, Bob and Charlie share a large number of i.i.d. copies of a four-party pure state. Initially, Bob holds the systems BD and Charlie holds C. At the end of the protocol, Bob would hold system D alone, while Charlie would hold BC. The quantities of interest are the optimal rate of quantum communication and shared entanglement that are required for a protocol that achieves the task on an asymptotically large number of copies of the state such that the overall state is preserved after redistribution with nearly unit fidelity.

Luo, Devetak and Yard [49, 203] studied this task in the i.i.d. asymptotic limit, where Alice and Bob share many copies of the state ρ_{BCD}. For rates of quantum communication from Alice to Bob and entanglement consumption Q and E, Luo and Devetak proved the converse theorem that the said quantum state redistribution can be achieved if and only if the following conditions are satisfied:

$$\begin{aligned} Q &\geq \frac{1}{2} I\left(A; B\,|C\right)_{\psi} \\ Q + E &\geq H\left(B\,|C\right)_{\psi}. \end{aligned} \tag{A.3.1}$$

The theorem can be written in a compact manner in terms of the following resource inequality. It is given as

$$\psi_{A|BD|C} + Q\left[q \rightarrow q\right] + E\left[qq\right] \geq \psi_{A|D|BC}, \tag{A.3.2}$$

if and only if Q and E satisfy the conditions in $(A.3.1)$. Subsequently Devetak and Yard showed that these rates are achievable. That is, they showed that for any $\epsilon > 0$, there exist (n, Q, E, ϵ)-protocols for the rates of quantum communication and entanglement consumption precisely given by $Q = \frac{1}{2} I\left(A; B\,|C\right)_{\psi}$ and $E = H\left(B\,|C\right)_{\psi} - \frac{1}{2} I\left(A; B\,|C\right)_{\psi}$ that achieves the redistribution from $\psi_{A|BD|C}$ to $\psi_{A|D|BC}$ in the limit of a large n number of copies of the state ψ_{ABCD} within an error ϵ. This means that for a large number of copies of ψ_{ABCD}

(denoted together as ψ^n_{ABCD}), there exists a protocol that operates at the above mentioned rates and accomplishes the task such that $\|\psi^n_{ABCD} - \rho_{A^nB^nC^nD^n}\| \leq \epsilon$, where the output state after redistribution is denoted by $\rho_{A^nB^nC^nD^n}$, a large combined state on n copies of the individual systems A, B, C and D.

When an optimal protocol is employed (i.e., when we have equalities in (A.3.1)), there are three distinct possibilities. In the case that $\frac{1}{2}I\left(A;B\left|C\right.\right)_\psi = H\left(B\left|C\right.\right)_\psi$, the optimal protocol redistributes the state without consuming any shared entanglement, and can be described as

$$\psi_{A|BD|C} + \frac{1}{2}I\left(A;B\left|C\right.\right)_\psi [q \to q] \geq \psi_{A|D|BC}. \tag{A.3.3}$$

In the case that $\frac{1}{2}I\left(A;B\left|C\right.\right)_\psi < H\left(B\left|C\right.\right)_\psi$, the optimal protocol redistributes the state, while consuming shared entanglement, and can be described as

$$\psi_{A|BD|C} + \frac{1}{2}I\left(A;B\left|C\right.\right)_\psi [q \to q] + \left(H\left(B\left|C\right.\right)_\psi - \frac{1}{2}I\left(A;B\left|C\right.\right)_\psi\right) E\left[qq\right] \geq \psi_{A|D|BC}. \tag{A.3.4}$$

Finally, in the case that $\frac{1}{2}I\left(A;B\left|C\right.\right)_\psi > H\left(B\left|C\right.\right)_\psi$, the optimal protocol redistributes the state, and in the meantime generates shared entanglement, described as

$$\psi_{A|BD|C} + \frac{1}{2}I\left(A;B\left|C\right.\right)_\psi [q \to q] \geq \psi_{A|D|BC} + \left(-H\left(B\left|C\right.\right)_\psi + \frac{1}{2}I\left(A;B\left|C\right.\right)_\psi\right) E\left[qq\right]. \tag{A.3.5}$$

A.4 Quantum Markov Chain States

In classical information theory, a tripartite probability distribution $p_{A,B,C}\left(a,b,c\right)$ has QCMI $I\left(A;B|C\right)$ equal to zero if and only if it can be written as a Markov distribution

$$p_{A,B,C}\left(a,b,c\right) = p_C\left(c\right) p_{A|C}\left(a|c\right) p_{B|C}\left(b|c\right). \tag{A.4.1}$$

Equivalently, it is equal to zero if and only if the distribution $p_{A,B,C}\left(a,b,c\right)$ is recoverable after marginalizing over the random variable A, that is, if there exists a classical channel $q\left(a|c\right)$ such that $p_{A,B,C}\left(a,b,c\right) = q\left(a|c\right) p_{B,C}\left(b,c\right)$.

The quantum analog of the above states were introduced in [1] and studied for finite-dimensional tripartite states in [80]. Following [80], we define a state ρ_{ABC} to be a quantum Markov state if $I\left(A;B|C\right)_\rho = 0$. Let $\mathcal{M}_{A-C-B}$ denote this class of states. The main result of [80] is that such a state has the following explicit form:

$$\rho_{ABC} = \bigoplus_j q\left(j\right) \sigma_{AC^L_j} \otimes \sigma_{C^R_j B}, \tag{A.4.2}$$

for some probability distribution $q\left(j\right)$, density operators $\{\sigma_{AC^L_j}, \sigma_{C^R_j B}\}$, and a decomposition of the Hilbert space for C as $\mathcal{H}_C = \bigoplus_j \mathcal{H}_{C^L_j} \otimes \mathcal{H}_{C^R_j}$. We also know that a state ρ_{ABC} is a quantum Markov state if any of the following conditions hold [142, 159]:

$$\rho_{ABC} = \rho_{AC}^{1/2} \rho_C^{-1/2} \rho_{BC} \rho_C^{-1/2} \rho_{AC}^{1/2}, \tag{A.4.3}$$

$$\rho_{ABC} = \rho_{BC}^{1/2} \rho_C^{-1/2} \rho_{AC} \rho_C^{-1/2} \rho_{BC}^{1/2}, \tag{A.4.4}$$

$$\rho_{ABC} = \exp\left\{\log \rho_{AC} + \log \rho_{BC} - \log \rho_C\right\}. \tag{A.4.5}$$

Interestingly, if ρ_C is positive definite, then the map $(\cdot) \to \rho_{AC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{AC}^{1/2}$ is a quantum channel from system C to AC, as one can verify by observing that it is completely positive and trace preserving. Otherwise, the map is trace non-increasing. These same statements also obviously apply to the map $(\cdot) \to \rho_{BC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{BC}^{1/2}$. See [103, 104] for more conditions for a tripartite state to be a quantum Markov state.

A.5 Various Representations of the Quantum Conditional Mutual Information in terms of the Relative Entropy

In this section, we write the QCMI of Definition A.1 in terms of the relative entropy.

Consider the following function of four density operators $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)$:

$$\Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C) \equiv \operatorname{Tr}\{\rho_{ABC}[\log\rho_{ABC} - \log\tau_{AC} - \log\theta_{BC} + \log\omega_C]\}. \quad \text{(A.5.1)}$$

This function forms our core quantity in order to write the QCMI as a relative entropy. Let I_{ABC} denote the identity operator acting on $\mathcal{H}_{ABC}$. A sufficient condition for

$$\lim_{\xi\searrow 0} \Delta(\rho_{ABC}, \tau_{AC} + \xi I_{ABC}, \theta_{BC} + \xi I_{ABC}, \omega_C + \xi I_{ABC}) \quad \text{(A.5.2)}$$

to be finite and equal to (A.5.1) is that

$$\operatorname{supp}(\rho_{ABC}) \subseteq \operatorname{supp}(\tau_{AC}), \operatorname{supp}(\theta_{BC}), \operatorname{supp}(\omega_C), \quad \text{(A.5.3)}$$

for the same reason given after (2.2.33). When comparing with $\operatorname{supp}(\rho_{ABC})$, it is implicit throughout this thesis that $\operatorname{supp}(\tau_{AC}) \equiv \operatorname{supp}(I_B \otimes \tau_{AC})$, $\operatorname{supp}(\theta_{BC}) \equiv \operatorname{supp}(I_A \otimes \theta_{BC})$, and $\operatorname{supp}(\omega_C) \equiv \operatorname{supp}(I_{AB} \otimes \omega_C)$. The condition in (A.5.3) is equivalent to $\operatorname{supp}(\rho_{ABC})$ being in the intersection of the supports of τ_{AC}, θ_{BC}, and ω_C. Note that there are more general support conditions which lead to a finite value for (A.5.2), but for simplicity, we focus exclusively on the above support condition. If the support condition in (A.5.3) holds, then by inspection we can write

$$\Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C) = D(\rho_{ABC} \| \exp\{\log\tau_{AC} + \log\theta_{BC} - \log\omega_C\}). \quad \text{(A.5.4)}$$

Furthermore, observe that

$$\lim_{\xi\searrow 0} \Delta(\rho_{ABC}, \rho_{AC} + \xi I_{ABC}, \rho_{BC} + \xi I_{ABC}, \rho_C + \xi I_{ABC}) \quad \text{(A.5.5)}$$

is finite and equal to (A.5.1) because the support condition in (A.5.3) holds when choosing τ_{AC}, θ_{BC}, and ω_C as the marginals of ρ_{ABC} (see, e.g., [153, Lemma B.4.1]).

Lemma A.2. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)$ and suppose that the support condition in* (A.5.3) *holds. Then*

$$\Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C) = I(A;B|C)_\rho + D(\rho_{AC}\|\tau_{AC}) + D(\rho_{BC}\|\theta_{BC}) - D(\rho_C\|\omega_C). \quad \text{(A.5.6)}$$

Proof. This follows simply by adding to and subtracting from $\Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C)$ each of $\text{Tr}\{\rho_{ABC} \log \rho_{AC}\}$, $\text{Tr}\{\rho_{ABC} \log \rho_{BC}\}$, and $\text{Tr}\{\rho_{ABC} \log \rho_C\}$. We then apply the definitions of $I(A;B|C)_\rho$, $D(\rho_{AC} \| \tau_{AC})$, $D(\rho_{BC} \| \theta_{BC})$, and $D(\rho_C \| \omega_C)$. ■

The mutual information of a bipartite state ρ_{AB} can be written as a relative entropy in one of four seemingly different ways [41], namely

$$I(A;B)_\rho = D(\rho_{AB} \| \rho_A \otimes \rho_B) \tag{A.5.7}$$

$$= \min_{\tau_A} D(\rho_{AB} \| \tau_A \otimes \rho_B) \tag{A.5.8}$$

$$= \min_{\theta_B} D(\rho_{AB} \| \rho_A \otimes \theta_B) \tag{A.5.9}$$

$$= \min_{\tau_A, \theta_B} D(\rho_{AB} \| \tau_A \otimes \theta_B). \tag{A.5.10}$$

For the QCMI, however, there are more ways of doing so, as summarized in the following proposition. The significance of Proposition A.3 is that it paves the way for designing many different Rényi generalizations of the QCMI.

Proposition A.3. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$. Then*

$$I(A;B|C)_\rho = \Delta(\rho_{ABC}, \rho_{AC}, \rho_{BC}, \rho_C) = \inf_{\tau_{AC}} \Delta(\rho_{ABC}, \tau_{AC}, \rho_{BC}, \rho_C) \tag{A.5.11}$$

$$= \inf_{\theta_{BC}} \Delta(\rho_{ABC}, \rho_{AC}, \theta_{BC}, \rho_C) = \sup_{\omega_C} \Delta(\rho_{ABC}, \rho_{AC}, \rho_{BC}, \omega_C) \tag{A.5.12}$$

$$= \inf_{\tau_{AC}} \Delta(\rho_{ABC}, \tau_{AC}, \rho_{BC}, \tau_C) = \inf_{\tau_{AC}} \sup_{\omega_C} \Delta(\rho_{ABC}, \tau_{AC}, \rho_{BC}, \omega_C) \tag{A.5.13}$$

$$= \inf_{\theta_{BC}} \Delta(\rho_{ABC}, \rho_{AC}, \theta_{BC}, \theta_C) = \inf_{\theta_{BC}} \sup_{\omega_C} \Delta(\rho_{ABC}, \rho_{AC}, \theta_{BC}, \omega_C) \tag{A.5.14}$$

$$= \inf_{\sigma_{ABC}} \Delta(\rho_{ABC}, \sigma_{AC}, \sigma_{BC}, \rho_C) = \inf_{\tau_{AC}, \theta_{BC}} \Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \rho_C) \tag{A.5.15}$$

$$= \inf_{\sigma_{ABC}} \Delta(\rho_{ABC}, \sigma_{AC}, \sigma_{BC}, \sigma_C) = \inf_{\tau_{AC}, \theta_{BC}} \Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \tau_C) \tag{A.5.16}$$

$$= \inf_{\tau_{AC}, \theta_{BC}} \Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \theta_C) = \inf_{\sigma_{ABC}} \sup_{\omega_C} \Delta(\rho_{ABC}, \sigma_{AC}, \sigma_{BC}, \omega_C) \tag{A.5.17}$$

$$= \inf_{\tau_{AC}, \theta_{BC}} \sup_{\omega_C} \Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C), \tag{A.5.18}$$

where the optimizations are over states on the indicated Hilbert spaces obeying the support condition in (A.5.3) *and over σ_{ABC} for which* $\text{supp}(\rho_{ABC}) \subseteq \text{supp}(\sigma_{ABC})$. *The infima and suprema can be interchanged in all of the above cases, are achieved by the marginals of ρ_{ABC}, and can thus be replaced by minima and maxima.*

Proof. We only prove two of these relations, noting that the rest follow from similar ideas. We first prove (A.5.18). Invoking Lemma A.2, we have that

$$\inf_{\tau_{AC}, \theta_{BC}} \sup_{\omega_C} \Delta(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C) = I(A;B|C)_\rho + \inf_{\tau_{AC}} D(\rho_{AC} \| \tau_{AC}) + \inf_{\theta_{BC}} D(\rho_{BC} \| \theta_{BC}) - \inf_{\omega_C} D(\rho_C \| \omega_C). \tag{A.5.19}$$

Invoking the fact that the relative entropy is minimized and equal to zero when its first argument is equal to its second, we see that the right hand side is equal to $I(A;B|C)_\rho$.

We now prove the first equality in (A.5.16). Let σ_{ABC} denote some tripartite state for which $\text{supp}(\rho_{ABC}) \subseteq \text{supp}(\sigma_{ABC})$. By Lemma A.2, we have that

$$\Delta(\rho_{ABC}, \sigma_{AC}, \sigma_{BC}, \sigma_C) = I(A;B|C)_\rho + D(\rho_{AC}\|\sigma_{AC}) + D(\rho_{BC}\|\sigma_{BC}) - D(\rho_C\|\sigma_C). \quad \text{(A.5.20)}$$

But it is known that the relative entropy is monotone under a partial trace, so that

$$D(\rho_{AC}\|\sigma_{AC}) \geq D(\rho_C\|\sigma_C). \quad \text{(A.5.21)}$$

Thus, we have that

$$D(\rho_{AC}\|\sigma_{AC}) + D(\rho_{BC}\|\sigma_{BC}) - D(\rho_C\|\sigma_C) \geq 0. \quad \text{(A.5.22)}$$

This implies that

$$\inf_{\sigma_{ABC}} \Delta(\rho_{ABC}, \sigma_{AC}, \sigma_{BC}, \sigma_C) = I(A;B|C)_\rho + \inf_{\sigma_{ABC}} \left[D(\rho_{AC}\|\sigma_{AC}) + D(\rho_{BC}\|\sigma_{BC}) - D(\rho_C\|\sigma_C)\right]. \quad \text{(A.5.23)}$$

The three rightmost terms are non-negative (as shown above), so that we can minimize them (to their absolute minimum of zero) by picking a state σ_{ABC} such that

$$\sigma_{AC} = \rho_{AC}, \qquad \log\sigma_{BC} - \log\sigma_C = \log\rho_{BC} - \log\rho_C, \quad \text{(A.5.24)}$$

or by symmetry, one such that

$$\sigma_{BC} = \rho_{BC}, \qquad \log\sigma_{AC} - \log\sigma_C = \log\rho_{AC} - \log\rho_C. \quad \text{(A.5.25)}$$

One clear choice satisfying this is $\sigma_{ABC} = \rho_{ABC}$, but there could be others. ■

Remark A.4. *A priori, we require infima and suprema in the above proposition because the sets over which the optimizations occur are not compact. More explicitly, suppose that* $\rho_{ABC} = \omega_{AB} \otimes \theta_C$ *for* $\omega_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ *and* $\theta_C \in \mathcal{S}(\mathcal{H}_C)$. *Then the sequence of states*

$$\omega_{AB}(n) \equiv \frac{1}{n}\frac{\omega^0_{AB}}{\text{Tr}\{\omega^0_{AB}\}} + \left(1 - \frac{1}{n}\right)\frac{I_{AB} - \omega^0_{AB}}{\text{Tr}\{I_{AB} - \omega^0_{AB}\}}, \quad \text{(A.5.26)}$$

is such that $\text{supp}(\rho_{ABC}) \subseteq \text{supp}(\omega_{AB}(n))$ *for all* $n \geq 1$, *but* $\text{supp}(\rho_{ABC}) \not\subseteq \text{supp}(\omega_{AB}(\infty))$.

Corollary A.5. *Let* $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$. *Then there is a Pinsker-like lower bound on the conditional mutual information* $I(A;B|C)_\rho$*:*

$$I(A;B|C)_\rho \geq \tfrac{1}{4}\left\|\rho_{ABC} - \exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}\right\|_1^2. \quad \text{(A.5.27)}$$

Proof. The corollary results from the following chain of inequalities:

$$\begin{aligned} &D(\rho_{ABC}\|\exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}) \\ &\quad \geq D_{1/2}(\rho_{ABC}\|\exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}) &\text{(A.5.28)} \\ &\quad = -2\log\text{Tr}\left\{\sqrt{\rho_{ABC}}\sqrt{\exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}}\right\} &\text{(A.5.29)} \\ &\quad \geq -\log F(\rho_{ABC}, \exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}) &\text{(A.5.30)} \\ &\quad \geq -\log\left(1 - \left(\tfrac{1}{2}\left\|\rho_{ABC} - \exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}\right\|_1\right)^2\right) &\text{(A.5.31)} \\ &\quad \geq \tfrac{1}{4}\left\|\rho_{ABC} - \exp\{\log\rho_{AC} + \log\rho_{BC} - \log\rho_C\}\right\|_1^2. &\text{(A.5.32)} \end{aligned}$$

The first step follows from monotonicity of the Rényi relative entropy with respect to the Rényi parameter (see Theorem 2.4). The equality in (A.5.29) and the inequality in (A.5.30) follow from the definition of $D_{1/2}$ and the fidelity. The inequality in (A.5.31) is a well-known relation between the fidelity and trace distance. Finally, the inequality in (A.5.32) holds because $-\log(1-x) \geq x$ for $x \leq 1$. This line of reasoning is similar to that in the proofs of [206, Theorem 2.1 and Corollary 2.2], which in turn follows from some of the development in [33]. ■

A.6 Discussion

To summarize, in this appendix we discussed the QCMI $I(A;B|C)$ of a tripartite state ρ_{ABC} and its properties including the strong subadditivity inequality, monotonicity under local quantum operations on A and B and duality for a purification ψ_{ABCD}. We then discussed the quantum state redistribution protocol, where the QCMI finds operational interpretation. This was followed by a brief description of the states for which QCMI is zero, namely the quantum Markov-chain states. Finally, we rewrote the QCMI as a relative entropy and showed that there exist several possible ways to do so.

As we will see in Appendix B, these relative entropy-based expressions pave the way towards Rényi QCMIs. It is desired that a Rényi QCMI also hold the same properties as those of the QCMI discussed in this appendix. Therefore, we will use the afore-mentioned properties to validate the proposed Rényi QCMIs.

The QCMI has many important applications. It underlies the squashed entanglement [40], which is a measure of entanglement that satisfies nearly all of the axioms desired for such a measure [4, 112, 25]. It also underlies the quantum discord [136], which is a measure of quantum correlations subsuming those due to entanglement. We described these measures in greater detail in Chapter 3. Newer applications of the QCMI include results in the areas of information and communication complexity [28, 186, 185].

Appendix B
Rényi Generalizations of the Quantum Conditional Mutual Information[1]

B.1 Introduction

The Rényi entropies [154] have attracted a lot of interest both in quantum information theory and in various areas of physics in recent times. The α-Rényi entropies have been shown to be useful for characterizing information processing tasks in the regimes of a single or finite number of resource utilizations [131, 92, 79, 130]. They have also been used to establish strong converse theorems [8, 134, 116, 150, 169, 198, 76, 184]. In many-body physics, the α-Rényi entanglement entropies have been shown to be useful in characterizing the entanglement spectra of condensed matter systems, akin to moments of a probability distribution [119, 63]. They have also been considered for similar applications in the contexts of relativistic quantum field theory and holographic theory of black holes [64, 82, 60]. In Gaussian quantum information theory, the $\alpha = 2$ Rényi entropy has been shown to be useful in studying Gaussian entanglement and other more general quantum correlations [2]. In quantum thermodynamics, α-Rényi entropies have been shown to represent the derivative of the free energy with respect to temperature [9] and are relevant for the work value of information [45].

Given the rich variety of applications of the Rényi entropies, there has been a substantial effort towards obtaining Rényi generalizations of other information measures, such as the quantum conditional entropy (QCE), or the quantum mutual information (QMI). While a Rényi QCE and QMI have been proposed, validated and studied extensively [134, 116, 130, 169, 132, 198, 76, 182], it has been a long-standing open problem to obtain a Rényi generalization of the quantum conditional mutual information (QCMI).

In this appendix, we propose Rényi generalizations of the QCMI and nearly validate them as appropriate generalizations by proving many of the desired properties of such a quantity. As discussed in Appendix A, the desired properties are those that are held by the von Neumann entropy-based QCMI, such as non-negativity, monotonicity under local quantum operations and duality for four-party pure states. We used the Rényi generalizations of the QCMI proposed here in Chapters 3 and 4 to define measures of quantum entanglement and quantum discord.

We begin this appendix by motivating the interest behind Rényi generalizations of quantum information measures. We give some background on the typical approach to obtaining

[1]This appendix is reproduced by updating and adapting the contents of Mario Berta, Kaushik P. Seshadreesan, and Mark M. Wilde, Journal of Mathematical Physics, 56(2):022205, February 2015, and Mario Berta, Kaushik P. Seshadreesan, and Mark M. Wilde, Physical Review A, 91:022333, February 2015, with the permission of AIP Publishing LLC and APS, respectively. See Appendix E for the copyright permission from the publishers.

Rényi generalizations of quantum information measures and briefly mention about the previous attempts at Rényi generalizing the QCMI. We then present our prescription to Rényi generalize any quantum information measure, which is a linear combination of von Neumann entropies. We apply this prescription to the case of the QCMI, and obtain various generalizations of the quantity. As said before, we prove many of the desired properties of these quantities and state some open questions about other properties that remain to be proven. We present numerical evidence, which suggests that these unproven properties should also hold for the proposed Rényi generalizations of the QCMI.

B.2 Background

Suppose that we would like to establish a Rényi generalization of the following linear combination of entropies:

$$\sum_{S\subseteq\{A_1,\ldots,A_l\}} a_S H(S)_\rho, \tag{B.2.1}$$

where $\rho_{A_1\ldots A_l}$ is a density operator on l systems, the coefficients $a_S \in \{-1,0,1\}$, and the sum runs over all subsets of the systems $A_1,\ldots,A_l$. This criterion is met by many useful measures; e.g., the QCE, the QMI, and the QCMI are defined respectively as

$$H(A|B)_\rho \equiv H(AB)_\rho - H(B)_\rho, \tag{B.2.2}$$

$$I(A;B)_\rho \equiv H(A)_\rho + H(B)_\rho - H(AB)_\rho, \tag{B.2.3}$$

$$I(A;B|C)_\rho \equiv H(AC)_\rho + H(BC)_\rho - H(C)_\rho - H(ABC)_\rho, \tag{B.2.4}$$

where ρ is taken to be a bipartite state ρ_{AB} in (B.2.2) and (B.2.3), and a tripartite state ρ_{ABC} in (B.2.4). A first approach one might consider is simply to replace the linear combination of von Neumann entropies with the corresponding linear combination of α-Rényi entropies:

$$\sum_{S\subseteq\{A_1,\ldots,A_l\}} a_S H_\alpha\left(S\right)_\rho. \tag{B.2.5}$$

However, the work of [124] establishes that there are no universal constraints on such a quantity. For example, consider the following quantity obtained by replacing the von Neumann entropies in (B.2.4) with α-Rényi entropies, namely

$$I'_\alpha(A;B|C)_\rho \equiv H_\alpha(AC)_\rho + H_\alpha(BC)_\rho - H_\alpha(C)_\rho - H_\alpha(ABC)_\rho. \tag{B.2.6}$$

For $\alpha \in (0,1)\cup(1,\infty)$, this quantity does not generally satisfy non-negativity [124], while the von Neumann QCMI is known to be non-negative, the latter being a result of the strong subadditivity inequality [123]. Since strong subadditivity is consistently useful in applications and often regarded as a "law of quantum information theory," the work in [124] suggests that the Rényi generalization in (B.2.5) is perhaps not the appropriate one to be using in applications [2].

[2]There are exceptions though, if we restrict ourselves to special types of quantum states. For example, for Gaussian states, the $\alpha = 2$ Rényi entropy satisfies strong subadditivity, as was shown in [2].

On the other hand, one can write a quantum information measure in terms of the relative entropy of Section 2.2.2, and subsequently replace the relative entropy with a Rényi relative entropy of Section 2.2.2 [140], [132], [198] in order to obtain a Rényi generalization of the measure. Recall that the von Neumann entropy of a state ρ_A on system A can itself be written in terms of the relative entropy as $-D(\rho_A \| I_A)$, where I_A is the identity operator. Also, the QCE and the QMI can also be written in terms of the relative entropy as

$$H(A|B)_\rho = -\min_{\sigma_B} D\left(\rho_{AB} \| I_A \otimes \sigma_B\right), \tag{B.2.7}$$

$$I(A;B)_\rho = \min_{\sigma_B} D\left(\rho_{AB} \| \rho_A \otimes \sigma_B\right), \tag{B.2.8}$$

respectively, where σ_B is any density operator on the Hilbert space $\mathcal{H}_B$ of system B. (The unique optimum σ_B in the above expressions turns out to be the reduced density operator ρ_B.) Therefore, one can obtain Rényi generalizations of the above quantities by using the Rényi relative entropy in place of the relative entropy. Rényi generalizations of quantum information measures obtained via the above procedure converge to the corresponding von Neumann entropy based quantities in the limit as α tends to one. They also retain most of the desired properties of the original quantities. For example, a Rényi QMI obtained from (B.2.8), just like the original von Neumann entropy based quantity, is non-negative and non-increasing under the action of local completely positive and trace preserving (CPTP) maps for $\alpha \in [0,1) \cup (1,2]$. This is because the Rényi relative entropy for $\alpha \in [0,1) \cup (1,2]$, just like the relative entropy, is non-negative and non-increasing under the action of any CPTP map, in the sense that

$$D_\alpha(\rho \| \sigma) \geq D_\alpha(\mathcal{N}(\rho) \| \mathcal{N}(\sigma)) \tag{B.2.9}$$

for a quantum map $\mathcal{N}$ [140].

One could also use the sandwiched Rényi relative entropy of Section 2.2.2 [132], [198] instead of the Rényi relative entropy. Recall that the sandwiched Rényi relative entropy is non-negative and non-increasing under the action of any CPTP map for $\alpha \in [1/2,1) \cup (1,\infty)$ [65]. Sandwiched Rényi generalizations of quantum information measures as discussed above thus also satisfy the above properties.

In order to write an information quantity in terms of a relative entropy, the key task is to identify the second argument for the relative entropy. This task, however, can be nontrivial in some cases. For example, it is not obvious as to what the second argument should be for the QCMI. Taking a cue from the QMI of (B.2.8), in which the second argument (when suitably normalized) has vanishing QMI, one may try to write the QCMI as an optimized relative entropy with respect to the set of quantum Markov states [80], which are defined as those tripartite states which have zero QCMI. This is indeed true for the classical conditional mutual information of a joint probability distribution $p_{A,B,C}$, that it can be written as the relative entropy distance between $p_{A,B,C}$ and the nearest Markov distribution [100, Section II]. However, a similar approach does not succeed in the case of the QCMI.

Let $M(\rho_{ABC})$ denote the relative entropy "distance" to quantum Markov states [100]:

$$M(\rho_{ABC}) \equiv \inf_{\sigma_{ABC} \in \mathcal{M}_{A-C-B}} D\left(\rho_{ABC} \| \sigma_{ABC}\right), \tag{B.2.10}$$

where $\mathcal{M}_{A-C-B}$ is the set of quantum Markov states defined above. Clearly, it suffices to restrict the above infimum to the set of Markov states σ_{ABC} for which $\operatorname{supp}(\rho_{ABC}) \subseteq \operatorname{supp}(\sigma_{ABC})$. We can now easily compare $I(A;B|C)$ with $M(\rho_{ABC})$, as done in [100]. First, since every quantum Markov state satisfies the condition

$$\sigma_{ABC} = \exp\{\log \sigma_{AC} + \log \sigma_{BC} - \log \sigma_C\}, \tag{B.2.11}$$

we see that this formula is equivalent to

$$M(\rho_{ABC}) = \inf_{\sigma_{ABC} \in \mathcal{M}_{A-C-B}} D(\rho_{ABC} \| \exp\{\log \sigma_{AC} + \log \sigma_{BC} - \log \sigma_C\}), \tag{B.2.12}$$

from which we obtain the following inequality:

$$\begin{aligned} M(\rho_{ABC}) &\geq \inf_{\omega_{ABC}} D(\rho_{ABC} \| \exp\{\log \omega_{AC} + \log \omega_{BC} - \log \omega_C\}) && \text{(B.2.13)} \\ &= \inf_{\omega_{ABC}} \Delta(\rho_{ABC}, \omega_{AC}, \omega_{BC}, \omega_C) && \text{(B.2.14)} \\ &= I(A;B|C)_\rho, && \text{(B.2.15)} \end{aligned}$$

where the infimum is over all states ω_{ABC} satisfying $\operatorname{supp}(\rho_{ABC}) \subseteq \operatorname{supp}(\omega_{ABC})$ and Δ is the function defined in $(A.5.1)$ of Section A.5 in Appendix A. The above inequality was already stated in [100, Theorem 4] (and with the simpler proof along the lines above given by Jenčov at the end of [100]), but one of the main contributions of [100] was to show that there are tripartite states ω_{ABC} for which there is a strict inequality $M(\omega_{ABC}) > I(A;B|C)_\omega$, and in fact [100, Section VI] showed that the gap can be arbitrarily large.

Thus, from the results in [100], we can already conclude that taking the Rényi relative entropy distance to quantum Markov states will not lead to a useful Rényi generalization of the QCMI as one might hope. This point was further reiterated in [58].

B.3 Prescription for Rényi Generalization

Having discussed the traditional approach towards obtaining Rényi generalizations of quantum information measures of the form given in (B.2.1), and the hurdles faced, we now give our prescription for a Rényi generalization. It is also based on the relative entropy and its variants.

In the case that $a_{A_1 \ldots A_l}$ is nonzero, without loss of generality, we can set $a_{A_1 \ldots A_l} = -1$ (otherwise, factor out -1 to make this the case). Then, we can rewrite the quantity in (B.2.1) in terms of the relative entropy as follows:

$$D\left(\rho_{A_1 \ldots A_l} \middle\| \exp\left\{\sum_{S \subseteq A'} a_S \log \rho_S\right\}\right), \tag{B.3.1}$$

where $A' = \{A_1, \ldots, A_l\} \setminus A_1 \cdots A_l$. On the other hand, if $a_{A_1 \ldots A_l} = 0$, i.e., if all the marginal entropies in the sum are on a number of systems that is strictly smaller than the number of systems over which the state ρ is defined (as is the case with $H(AB) + H(BC) + H(AC)$, for example), we can take a purification of the original state and call this purification the state $\rho_{A_1 \ldots A_l}$. This state is now a pure state on a number of systems strictly larger than the number of systems involved in all the marginal entropies. We then add the entropy $H(A_1 \ldots A_l)_\rho = 0$ to the sum of entropies and apply the above recipe (so we resolve the issue with this example by purifying to a system R, setting the sum formula to be $H(ABCR) + H(AB) + H(BC) + H(AC)$, and proceeding with the above recipe).

We then appeal to a multipartite generalization of the Lie-Trotter product formula $D.1$ [176], to rewrite the second argument in (B.3.1) as

$$\lim_{\alpha \to 1} \left[\bigcirc_{S \subseteq A'} \Theta_{\rho_S^{a_S(1-\alpha)/2}} \left(I_{A_1 \cdots A_l} \right) \right]^{1/(1-\alpha)}, \tag{B.3.2}$$

where the map

$$\Theta_{\rho_S^{a_S(1-\alpha)/2}} (X) \equiv \rho_S^{a_S(1-\alpha)/2} X \rho_S^{a_S(1-\alpha)/2} \tag{B.3.3}$$

and the composition $\bigcirc$ of maps $\Theta_{\rho_S^{a_S(1-\alpha)/2}}$ for all subsets S can proceed in any order, and $I_{A_1 \cdots A_l}$ is the identity operator on the support of the state $\rho_{A_1 \ldots A_l}$. Finally, we obtain a Rényi generalization of the linear combination in (B.2.1) as

$$D_\alpha \left(\rho_{A_1 \ldots A_l} \middle\| \left[\bigcirc_{S \subseteq A'} \Theta_{\rho_S^{a_S(1-\alpha)/2}} \left(I_{A_1 \cdots A_l} \right) \right]^{1/(1-\alpha)} \right), \tag{B.3.4}$$

where D_α is the Rényi relative entropy, and we have used (B.3.2) in (B.3.1) and promoted the parameter α in (B.3.2) to take the role of the Rényi parameter.

A similar Rényi generalization can also be obtained using the sandwiched Rényi relative entropy as

$$\widetilde{D}_\alpha \left(\rho_{A_1 \ldots A_l} \middle\| \left[\bigcirc_{S \subseteq A'} \Theta_{\rho_S^{a_S(1-\alpha)/(2\alpha)}} \left(I_{A_1 \cdots A_l} \right) \right]^{\alpha/(1-\alpha)} \right). \tag{B.3.5}$$

Note that there exist a number of different possible variants of the above Rényi generalizations since different choice of orderings of the maps $\Theta_{\rho_S^{a_S(1-\alpha)/2}}$ are possible. Moreover, we could also consider arbitrary density operators on the appropriate subsystems for the maps Θ instead of the reduced density operators (marginals) of $\rho_{A_1 \ldots A_l}$, and then optimize over these operators (under the assumption that the support of $\rho_{A_1 \ldots A_l}$ is contained in the intersection of the supports of these operators).

For any quantum information measure, it is possible to prove that these different Rényi generalizations converge to the original von Neumann entropy based quantity in (B.2.1) in the limit as $\alpha \to 1$. Also, consider that we can write the linear combination in (B.2.1) as

$$\sum_{S \subseteq \{A_1, \ldots, A_l\}} a_S H(S)_\rho = -\mathrm{Tr} \left\{ \rho_{A_1 \ldots A_l} \left[\sum_{S \subseteq \{A_1, \ldots, A_l\}} a_S \log \rho_S \right] \right\}. \tag{B.3.6}$$

The *information second moment* corresponding to this combination of entropies is then

$$V(\rho_{A_1 \ldots A_l}, \{a_S\}) \equiv \mathrm{Tr} \left\{ \rho_{A_1 \ldots A_l} \left[\sum_{S \subseteq \{A_1, \ldots, A_l\}} a_S \log \rho_S \right]^2 \right\}. \tag{B.3.7}$$

It can be shown that the Rényi generalization in (B.3.4) has the following Taylor expansion about $\gamma = 0$, where $\gamma = \alpha - 1$:

$$\frac{1}{\gamma} \log \left[\operatorname{Tr}\left\{\rho_{A_1 \ldots A_l}\right\} + \gamma \sum_{S \subseteq \{A_1, \ldots, A_l\}} a_S H(S)_\rho + \frac{\gamma^2}{2} V\left(\rho_{A_1 \ldots A_l}, \{a_S\}\right) + O\left(\gamma^3\right) \right], \tag{B.3.8}$$

thus recovering the information second moment as the second order term in the Taylor expansion. (See [18, Appendix E.1], for example, which shows the Taylor expansion in a neighborhood of $\gamma = 0$ for the Rényi QCMI.) Note that the Rényi generalization in (B.2.5) does not recover the information second moment in a Taylor expansion. Furthermore, we leave it as an open question to determine whether the following statement is generally true: *if a von Neumann entropy-based measure is non-negative and non-increasing under the action of local CPTP maps, then its Rényi generalizations of the above type are also non-negative and non-increasing under local CPTP maps.*

B.4 Definitions of Rényi Quantum Conditional Mutual Informations

We will now apply the above prescribed formula to obtain Rényi generalizations of the QCMI. We study generalizations based on both the Rényi, and sandwiched Rényi relative entropies. Note that throughout this appendix, for technical convenience and simplicity, some of our statements apply only to states in $\mathcal{S}(\mathcal{H})_{++}$ (strictly positive definite density operators). This might seem restrictive, but in the following sense, it is physically reasonable. Given any state $\omega \in \mathcal{S}(\mathcal{H}) \backslash \mathcal{S}(\mathcal{H})_{++}$, there is a state $\omega(\xi) = (1-\xi)\,\omega + \xi I / \dim(\mathcal{H})$ for a constant $\xi > 0$, so that $\omega(\xi) \in \mathcal{S}(\mathcal{H})_{++}$ and $\|\omega - \omega(\xi)\|_1 \leq 2\xi$. Thus, the bias in distinguishing ω from $\omega(\xi)$ is no more than $\xi/2$, so that $\omega(\xi)$ can "mask" as ω.

B.4.1 Rényi quantum conditional mutual informations based on the Rényi relative entropy

Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)$. We define the following quantities for $\alpha \in [0,1) \cup (1,\infty)$:

$$Q_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \equiv \operatorname{Tr}\left\{\rho_{ABC}^{\alpha} \tau_{AC}^{(1-\alpha)/2} \omega_C^{(\alpha-1)/2} \theta_{BC}^{1-\alpha} \omega_C^{(\alpha-1)/2} \tau_{AC}^{(1-\alpha)/2}\right\}, \tag{B.4.1}$$

$$\Delta_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \equiv \frac{1}{\alpha-1} \log Q_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}). \tag{B.4.2}$$

We stress that the formula in (B.4.2) is to be interpreted in the sense of generalized inverses, so that it is always finite if

$$\rho_{ABC} \not\perp \left| \tau_{AC}^{(1-\alpha)/2} \omega_C^{(\alpha-1)/2} \theta_{BC}^{(1-\alpha)/2} \right|^2. \tag{B.4.3}$$

The non-orthogonality condition in (B.4.3) is satisfied, e.g., if the support condition in (A.5.3) holds, so that (B.4.3) is satisfied when $\tau_{AC} = \rho_{AC}$, $\omega_C = \rho_C$, and $\theta_{BC} = \rho_{BC}$. It remains largely open to determine support conditions under which

$$\lim_{\xi \searrow 0} \Delta_\alpha(\rho_{ABC}, \tau_{AC} + \xi I_{ABC}, \omega_C + \xi I_{ABC}, \theta_{BC} + \xi I_{ABC}) \tag{B.4.4}$$

is finite and equal to (B.4.2), with complications being due to the fact that (B.4.1) features the multiplication of several non-commuting operators which can interact in non-trivial ways. We can also consider five other different operator orderings for the last three arguments of Q_α, i.e.,

$$Q_\alpha\left(\rho_{ABC},\theta_{BC},\omega_C,\tau_{AC}\right) \equiv \operatorname{Tr}\left\{\rho_{ABC}^\alpha \theta_{BC}^{(1-\alpha)/2}\omega_C^{(\alpha-1)/2}\tau_{AC}^{1-\alpha}\omega_C^{(\alpha-1)/2}\theta_{BC}^{(1-\alpha)/2}\right\}, \tag{B.4.5}$$

$$Q_\alpha\left(\rho_{ABC},\omega_C,\tau_{AC},\theta_{BC}\right) \equiv \operatorname{Tr}\left\{\rho_{ABC}^\alpha \omega_C^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\theta_{BC}^{1-\alpha}\tau_{AC}^{(1-\alpha)/2}\omega_C^{(\alpha-1)/2}\right\}, \tag{B.4.6}$$

$$Q_\alpha\left(\rho_{ABC},\omega_C,\theta_{BC},\tau_{AC}\right) \equiv \operatorname{Tr}\left\{\rho_{ABC}^\alpha \omega_C^{(\alpha-1)/2}\theta_{BC}^{(1-\alpha)/2}\tau_{AC}^{1-\alpha}\theta_{BC}^{(1-\alpha)/2}\omega_C^{(\alpha-1)/2}\right\}, \tag{B.4.7}$$

$$Q_\alpha\left(\rho_{ABC},\tau_{AC},\theta_{BC},\omega_C\right) \equiv \operatorname{Tr}\left\{\rho_{ABC}^\alpha \tau_{AC}^{(1-\alpha)/2}\theta_{BC}^{(1-\alpha)/2}\omega_C^{\alpha-1}\theta_{BC}^{(1-\alpha)/2}\tau_{AC}^{(1-\alpha)/2}\right\}, \tag{B.4.8}$$

$$Q_\alpha\left(\rho_{ABC},\theta_{BC},\tau_{AC},\omega_C\right) \equiv \operatorname{Tr}\left\{\rho_{ABC}^\alpha \theta_{BC}^{(1-\alpha)/2}\tau_{AC}^{(1-\alpha)/2}\omega_C^{\alpha-1}\tau_{AC}^{(1-\alpha)/2}\theta_{BC}^{(1-\alpha)/2}\right\}. \tag{B.4.9}$$

In the above, we are abusing notation by always having the power $(\alpha-1)/2$ associated with ω_C and the power $(1-\alpha)/2$ associated with τ_{AC} and θ_{BC}, but we take the convention that the different Q_α quantities are uniquely identified by the operator ordering of its last three arguments. These different Q_α functions lead to different Δ_α quantities, again uniquely identified by the operator ordering of the last three arguments.

We can then use the above observations, the observation in Proposition A.3, and the definition of the Rényi relative entropy to define Rényi generalizations of the QCMI. There are many definitions that we could take for a Rényi QCMI by using the different optimizations summarized in Proposition A.3 and the different orderings of operators as suggested above.

In spite of the many possibilities suggested above, we choose to define the *Rényi QCMI* as the following quantity because it obeys some additional properties (beyond those satisfied by many of the above generalizations) which we would expect to hold for a Rényi generalization of the QCMI.

Definition B.1. *Let $\rho_{ABC} \in \mathcal{S}\left(\mathcal{H}_{ABC}\right)$. The Rényi quantum conditional mutual information of ρ_{ABC} is defined for $\alpha \in [0,1) \cup (1,\infty)$ as*

$$I_\alpha\left(A;B|C\right)_\rho \equiv \inf_{\sigma_{BC}} \Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\sigma_{BC}\right), \tag{B.4.10}$$

where the optimization is over density operators σ_{BC} such that $\operatorname{supp}\left(\rho_{ABC}\right) \subseteq \operatorname{supp}\left(\sigma_{BC}\right)$.

Note that unlike the QCMI, this definition is not symmetric with respect to A and B. Thus one might also call it the Rényi information that B has about A from the perspective of C. Note also that, for trivial C, the definition reduces to the definition of Rényi mutual information in Section 2.2.2.

One advantage of the above definition is that we can identify an explicit form for the minimizing σ_{BC} and thus for $I_\alpha\left(A;B|C\right)_\rho$, as captured by the following proposition:

Proposition B.2. *Let $\rho_{ABC} \in \mathcal{S}\left(\mathcal{H}_{ABC}\right)$. The Rényi quantum conditional mutual information of ρ_{ABC} has the following explicit form for $\alpha \in (0,1) \cup (1,\infty)$:*

$$I_\alpha\left(A;B|C\right)_\rho = \frac{\alpha}{\alpha-1}\log \operatorname{Tr}\left\{\left(\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^\alpha\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2}\right)^{1/\alpha}\right\}. \tag{B.4.11}$$

This follows because the infimum in (B.4.10) *can be replaced by a minimum and the minimum* σ_{BC} *is unique with an explicit form.*

A proof of Proposition B.2 appears in Appendix D.2.1.

B.4.2 Rényi quantum conditional mutual informations based on the sandwiched Rényi relative entropy

As in the previous section, there are many ways in which we can define a sandwiched Rényi QCMI. Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)$. We define the following core quantities for $\alpha \in (0,1) \cup (1,\infty)$:

$$\widetilde{Q}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \equiv \operatorname{Tr}\left\{\left(\rho_{ABC}^{1/2}\tau_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\rho_{ABC}^{1/2}\right)^\alpha\right\}, \tag{B.4.12}$$

$$\widetilde{\Delta}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \equiv \frac{1}{\alpha-1}\log\widetilde{Q}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}). \tag{B.4.13}$$

We stress again that the formula above is to be interpreted in terms of generalized inverses. By employing (2.1.1) and (B.4.12), we can write

$$\widetilde{Q}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) = \left\|\rho_{ABC}^{1/2}\tau_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/2\alpha}\right\|_{2\alpha}^{2\alpha}, \tag{B.4.14}$$

and we see that $\widetilde{Q}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) = 0$ if and only if

$$\rho_{ABC}^{1/2}\tau_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/2\alpha} = 0. \tag{B.4.15}$$

So $\widetilde{Q}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) > 0$ if

$$\rho_{ABC}^{1/2} \not\perp \tau_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/2\alpha}. \tag{B.4.16}$$

The non-orthogonality condition in (B.4.16) is satisfied, e.g., if the support condition in (A.5.3) holds, so that (B.4.16) is satisfied when $\tau_{AC} = \rho_{AC}$, $\omega_C = \rho_C$, and $\theta_{BC} = \rho_{BC}$. It remains largely open to determine support conditions under which

$$\lim_{\xi\searrow 0}\widetilde{\Delta}_\alpha(\rho_{ABC}, \tau_{AC} + \xi I_{ABC}, \omega_C + \xi I_{ABC}, \theta_{BC} + \xi I_{ABC}) \tag{B.4.17}$$

is finite and equal to (B.4.13), with complications being due to the fact that (B.4.12) features the multiplication of several non-commuting operators which can interact in non-trivial ways. As before, we define five other different $\widetilde{Q}_\alpha$ quantities, again uniquely identified by the order of the last three arguments:

$$\widetilde{Q}_\alpha(\rho_{ABC}, \theta_{BC}, \omega_C, \tau_{AC}) \equiv \left\|\rho_{ABC}^{1/2}\theta_{BC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\right\|_{2\alpha}^{2\alpha}, \tag{B.4.18}$$

$$\widetilde{Q}_\alpha(\rho_{ABC}, \omega_C, \tau_{AC}, \theta_{BC}) \equiv \left\|\rho_{ABC}^{1/2}\omega_C^{(\alpha-1)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\theta_{BC}^{(1-\alpha)/2\alpha}\right\|_{2\alpha}^{2\alpha}, \tag{B.4.19}$$

$$\widetilde{Q}_\alpha(\rho_{ABC}, \omega_C, \theta_{BC}, \tau_{AC}) \equiv \left\|\rho_{ABC}^{1/2}\omega_C^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\right\|_{2\alpha}^{2\alpha}, \tag{B.4.20}$$

$$\widetilde{Q}_\alpha(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C) \equiv \left\|\rho_{ABC}^{1/2}\tau_{AC}^{(1-\alpha)/2\alpha}\theta_{BC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\right\|_{2\alpha}^{2\alpha}, \tag{B.4.21}$$

$$\widetilde{Q}_\alpha(\rho_{ABC}, \theta_{BC}, \tau_{AC}, \omega_C) \equiv \left\|\rho_{ABC}^{1/2}\theta_{BC}^{(1-\alpha)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\right\|_{2\alpha}^{2\alpha}. \tag{B.4.22}$$

These then lead to different $\widetilde{\Delta}_\alpha$ quantities. We call the quantities above "sandwiched" because they can be viewed as having their root in the sandwiched Rényi relative entropy, i.e., for $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$:

$$\widetilde{\Delta}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \\ = \widetilde{D}_\alpha\left(\rho_{ABC} \middle\| \left[\tau_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\right]^{\alpha/(1-\alpha)}\right). \quad \text{(B.4.23)}$$

Although there are many different possible sandwiched Rényi generalizations of the QCMI, found by combining the different $\widetilde{\Delta}_\alpha$ quantities discussed above with the different optimizations summarized in Proposition A.3, we choose the definition given below because it obeys many of the properties that the QCMI does.

Definition B.3. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$. The sandwiched Rényi quantum conditional mutual information is defined as*

$$\widetilde{I}_\alpha(A;B|C)_\rho \equiv \inf_{\sigma_{BC}} \sup_{\omega_C} \widetilde{\Delta}_\alpha(\rho_{ABC}, \rho_{AC}, \omega_C, \sigma_{BC}), \quad \text{(B.4.24)}$$

where the optimizations are over states obeying the support conditions in (A.5.3).

Again, unlike the QCMI, this definition is not symmetric with respect to A and B. Thus one might also call it the sandwiched Rényi information that B has about A from the perspective of C. Also, for trivial C, the definition reduces to the usual definition of sandwiched Rényi mutual information (see, e.g., [198, 76, 42]).

B.5 Properties of Rényi Quantum Conditional Mutual Informations

B.5.1 Limit of the Rényi quantum conditional mutual informations as $\alpha \to 1$

We now consider the limit of the Δ_α quantity as the Rényi parameter $\alpha \to 1$ and prove that some variations of the Rényi QCMI based on the Rényi relative entropy converge to the QCMI in the limit as $\alpha \to 1$.

Theorem B.4. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)$ and suppose that the support condition in* (A.5.3) *holds. Then*

$$\lim_{\alpha\to 1} \Delta_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) = \Delta(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}). \quad \text{(B.5.1)}$$

The same limiting relation holds for the other Δ_α quantities defined from (B.4.5)-(B.4.9).

Proof. We will consider L'Hôpital's rule in order to evaluate the limit of Δ_α as $\alpha \to 1$, due to the presence of the denominator term $\alpha - 1$ in Δ_α. To this end, we compute the following derivative with respect to α

$$\frac{d}{d\alpha}Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)=\operatorname{Tr}\left\{\left(\log\rho_{ABC}\right)\rho_{ABC}^{\alpha}\tau_{AC}^{(1-\alpha)/2}\omega_{C}^{(\alpha-1)/2}\theta_{BC}^{1-\alpha}\omega_{C}^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\right\}$$
$$-\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}^{\alpha}\left(\log\tau_{AC}\right)\tau_{AC}^{(1-\alpha)/2}\omega_{C}^{(\alpha-1)/2}\theta_{BC}^{1-\alpha}\omega_{C}^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\right\}$$
$$+\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}^{\alpha}\tau_{AC}^{(1-\alpha)/2}\left(\log\omega_{C}\right)\omega_{C}^{(\alpha-1)/2}\theta_{BC}^{1-\alpha}\omega_{C}^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\right\}$$
$$-\operatorname{Tr}\left\{\rho_{ABC}^{\alpha}\tau_{AC}^{(1-\alpha)/2}\omega_{C}^{(\alpha-1)/2}\left(\log\theta_{BC}\right)\theta_{BC}^{1-\alpha}\omega_{C}^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\right\}$$
$$+\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}^{\alpha}\tau_{AC}^{(1-\alpha)/2}\omega_{C}^{(\alpha-1)/2}\theta_{BC}^{1-\alpha}\left(\log\omega_{C}\right)\omega_{C}^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\right\}$$
$$-\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}^{\alpha}\tau_{AC}^{(1-\alpha)/2}\omega_{C}^{(\alpha-1)/2}\theta_{BC}^{1-\alpha}\omega_{C}^{(\alpha-1)/2}\left(\log\tau_{AC}\right)\tau_{AC}^{(1-\alpha)/2}\right\}. \quad \text{(B.5.2)}$$

Thus, the function $Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)$ is differentiable for $\alpha\in(0,\infty)$. Applying L'Hôpital's rule, we consider

$$\lim_{\alpha\to1}\Delta_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)=\lim_{\alpha\to1}\frac{1}{Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)}\frac{d}{d\alpha}Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right). \quad \text{(B.5.3)}$$

We can evaluate the limits separately to find that

$$\lim_{\alpha\to1}Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)=\operatorname{Tr}\left\{\rho_{ABC}\tau_{AC}^{0}\omega_{C}^{0}\theta_{BC}^{0}\omega_{C}^{0}\tau_{AC}^{0}\right\}, \quad \text{(B.5.4)}$$

$$\lim_{\alpha\to1}\frac{d}{d\alpha}Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)=\operatorname{Tr}\left\{\left(\log\rho_{ABC}\right)\rho_{ABC}\tau_{AC}^{0}\omega_{C}^{0}\theta_{BC}^{0}\omega_{C}^{0}\tau_{AC}^{0}\right\}$$
$$-\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}\left(\log\tau_{AC}\right)\tau_{AC}^{0}\omega_{C}^{0}\theta_{BC}^{0}\omega_{C}^{0}\tau_{AC}^{0}\right\}+\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}\tau_{AC}^{0}\left(\log\omega_{C}\right)\omega_{C}^{0}\theta_{BC}^{0}\omega_{C}^{0}\tau_{AC}^{0}\right\}$$
$$-\operatorname{Tr}\left\{\rho_{ABC}\tau_{AC}^{0}\omega_{C}^{0}\left(\log\theta_{BC}\right)\theta_{BC}^{0}\omega_{C}^{0}\tau_{AC}^{0}\right\}+\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}\tau_{AC}^{0}\omega_{C}^{0}\theta_{BC}\left(\log\omega_{C}\right)\omega_{C}^{0}\tau_{AC}^{0}\right\}$$
$$-\frac{1}{2}\operatorname{Tr}\left\{\rho_{ABC}\tau_{AC}^{0}\omega_{C}^{0}\theta_{BC}^{0}\omega_{C}^{0}\left(\log\tau_{AC}\right)\tau_{AC}^{0}\right\}. \quad \text{(B.5.5)}$$

Since by assumption $\operatorname{supp}(\rho_{ABC})$ is contained in each of $\operatorname{supp}(\tau_{AC})$, $\operatorname{supp}(\omega_C)$, and $\operatorname{supp}(\theta_{BC})$, we exploit the relations $\rho_{ABC}=\rho_{ABC}^{0}\rho_{ABC}\rho_{ABC}^{0}$, $\rho_{ABC}^{0}\tau_{AC}^{0}=\rho_{ABC}^{0}$, $\rho_{ABC}^{0}\theta_{BC}^{0}=\rho_{ABC}^{0}$, $\rho_{ABC}^{0}\omega_{C}^{0}=\rho_{ABC}^{0}$ and their Hermitian conjugates to find that

$$\lim_{\alpha\to1}Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)=1, \quad \text{(B.5.6)}$$
$$\lim_{\alpha\to1}\frac{d}{d\alpha}Q_{\alpha}\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right)=\Delta\left(\rho_{ABC},\tau_{AC},\omega_{C},\theta_{BC}\right), \quad \text{(B.5.7)}$$

which when combined with (B.5.3) leads to (B.5.1). Essentially the same proof establishes the limiting relation for the other Δ_{α} quantities defined from (B.4.5)-(B.4.9). ■

Corollary B.5. *Let $\rho_{ABC}\in\mathcal{S}\left(\mathcal{H}_{ABC}\right)$. Then the following limiting relation holds*

$$\lim_{\alpha\to1}\Delta_{\alpha}\left(\rho_{ABC},\rho_{AC},\rho_{C},\rho_{BC}\right)=I\left(A;B|C\right)_{\rho}. \quad \text{(B.5.8)}$$

Proof. This follows from the fact that $\text{supp}(\rho_{ABC}) \subseteq \text{supp}(\rho_{AC}), \text{supp}(\rho_C), \text{supp}(\rho_{BC})$ (see, e.g., [153, Lemma B.4.1]), from the above theorem, and by recalling that $\Delta(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC})$ equals $I(A;B|C)_\rho$. ■

Theorem B.6. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$. Then the Rényi quantum conditional mutual information converges to the quantum conditional mutual information in the limit as $\alpha \to 1$:*

$$\lim_{\alpha \to 1} I_\alpha(A;B|C)_\rho = I(A;B|C)_\rho . \tag{B.5.9}$$

Proof. The idea behind the proof of Theorem B.6 is the same as that behind the proof of Theorem B.4. However, we have the explicit form for $I_\alpha(A;B|C)_\rho$ from Proposition B.2, which allows us to evaluate the limit without needing uniform convergence of $\Delta_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ in τ_{AC}, ω_C, and θ_{BC} as $\alpha \to 1$. A proof of Theorem B.6 appears in Appendix D.2.2. ■

Remark B.7. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)$ and suppose that the support condition in* (A.5.3) *holds. If $\Delta_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ converges uniformly in τ_{AC}, ω_C, and θ_{BC} to $\Delta(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ as $\alpha \to 1$, then we could conclude that all Rényi generalizations of the QCMI (as proposed at the beginning of Section B.4) converge to it in the limit as $\alpha \to 1$.*

Similarly, consider the limit of the $\widetilde{\Delta}_\alpha$ quantities as $\alpha \to 1$. For technical reasons, we restrict the development to positive definite density operators. It remains open to determine whether the following theorems hold under less restrictive conditions.

Theorem B.8. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$. Then*

$$\lim_{\alpha \to 1} \widetilde{\Delta}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) = \Delta(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) . \tag{B.5.10}$$

The same limiting relation holds for the other $\widetilde{\Delta}_\alpha$ quantities defined from (B.4.18)-(B.4.22).

Proof. The proof of Theorem B.8 is very similar to the proof of Theorem B.4. ■

Corollary B.9. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$. The following limiting relation holds*

$$\lim_{\alpha \to 1} \widetilde{\Delta}_\alpha(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC}) = I(A;B|C)_\rho . \tag{B.5.11}$$

Proof. This follows from the fact that $\text{supp}(\rho_{ABC}) \subseteq \text{supp}(\rho_{AC}), \text{supp}(\rho_C), \text{supp}(\rho_{BC})$ (see, e.g., [153, Lemma B.4.1]), Theorem B.8, and by recalling that $\Delta(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC}) = I(A;B|C)_\rho$. ■

Remark B.10. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$. If $\widetilde{\Delta}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ converges uniformly to $\Delta(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ in τ_{AC}, ω_C, θ_{BC} as $\alpha \to 1$, then we could conclude that all sandwiched Rényi generalizations of the quantum conditional mutual information (as proposed at the beginning of Section B.4.2) converge to it in the limit as $\alpha \to 1$. In particular, uniform convergence implies that $\widetilde{I}_\alpha(A;B|C)_\rho$ converges to $I(A;B|C)_\rho$ as $\alpha \to 1$.*

B.5.2 Monotonicity under local quantum operations

The following lemma is the critical one which will allow us to conclude that the Rényi QCMI is monotone non-increasing with respect to local quantum operations acting on one system for $\alpha \in [0,1) \cup (1,2]$.

Lemma B.11. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$ and suppose that the non-orthogonality condition in (B.4.3) holds. Let $\mathcal{N}_{A\to A'}$ and $\mathcal{M}_{B\to B'}$ denote quantum operations acting on systems A and B, respectively. Then the following monotonicity inequalities hold for $\alpha \in [0,1) \cup (1,2]$:*

$$\Delta_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \geq \Delta_\alpha(\mathcal{M}_{B\to B'}(\rho_{ABC}), \tau_{AC}, \omega_C, \mathcal{M}_{B\to B'}(\theta_{BC})), \tag{B.5.12}$$

$$\Delta_\alpha(\rho_{ABC}, \omega_C, \tau_{AC}, \theta_{BC}) \geq \Delta_\alpha(\mathcal{M}_{B\to B'}(\rho_{ABC}), \omega_C, \tau_{AC}, \mathcal{M}_{B\to B'}(\theta_{BC})), \tag{B.5.13}$$

$$\Delta_\alpha(\rho_{ABC}, \omega_C, \theta_{BC}, \tau_{AC}) \geq \Delta_\alpha(\mathcal{N}_{A\to A'}(\rho_{ABC}), \omega_C, \theta_{BC}, \mathcal{N}_{A\to A'}(\tau_{AC})), \tag{B.5.14}$$

$$\Delta_\alpha(\rho_{ABC}, \theta_{BC}, \omega_C, \tau_{AC}) \geq \Delta_\alpha(\mathcal{N}_{A\to A'}(\rho_{ABC}), \theta_{BC}, \omega_C, \mathcal{N}_{A\to A'}(\tau_{AC})). \tag{B.5.15}$$

Proof. We begin by proving (B.5.12). Consider that $Q_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ is jointly concave in ρ_{ABC} and θ_{BC} when $\alpha \in [0,1)$. This is a result of Lieb's concavity theorem [121], a special case of which is the statement that the function

$$(S,R) \in \mathcal{B}(\mathcal{H})_+ \times \mathcal{B}(\mathcal{H})_+ \to \operatorname{Tr}\left\{S^\lambda X R^{1-\lambda} X^\dagger\right\} \tag{B.5.16}$$

is jointly concave in S and R when $\lambda \in [0,1]$. (We apply the theorem by choosing $S = \rho_{ABC}$, $R = \theta_{BC}$, and $X = \tau_{AC}^{(1-\alpha)/2}\omega_C^{(\alpha-1)/2}$.) Furthermore, by an application of Ando's convexity theorem [5], we know that $Q_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ is jointly convex in ρ_{ABC} and θ_{BC} when $\alpha \in (1,2]$.

By a standard (well known) argument due to Uhlmann [188], the monotonicity inequality in (B.5.12) holds. For completeness, we detail this standard argument here for the case when $\alpha \in [0,1)$. Note that it suffices to prove the following monotonicity under partial trace:

$$Q_\alpha(\rho_{AB_1B_2C}, \tau_{AC}, \omega_C, \theta_{B_1B_2C}) \leq Q_\alpha(\rho_{AB_1C}, \tau_{AC}, \omega_C, \theta_{B_1C}), \tag{B.5.17}$$

because the Q_α quantity is clearly invariant under isometries acting on system B and the Stinespring representation theorem [175] states that any quantum channel can be modeled as an isometry followed by a partial trace. To this end, let $\{U^i_{B_2}\}_{i=0}^{d^2_{B_2}-1}$ denote the set of Heisenberg-Weyl operators acting on the system B_2, with d_{B_2} the dimension of system B_2. Then

$$Q_\alpha(\rho_{AB_1B_2C}, \tau_{AC}, \omega_C, \theta_{B_1B_2C}) \\ = \frac{1}{d^2_{B_2}} \sum_{i=0}^{d^2_{B_2}-1} Q_\alpha\left(U^i_{B_2}\rho_{AB_1B_2C}\left(U^i_{B_2}\right)^\dagger, \tau_{AC}, \omega_C, U^i_{B_2}\theta_{B_1B_2C}\left(U^i_{B_2}\right)^\dagger\right). \tag{B.5.18}$$

We can then invoke the Lieb concavity theorem to conclude that

$$\begin{aligned}
&Q_\alpha\left(\rho_{AB_1B_2C},\tau_{AC},\omega_C,\theta_{B_1B_2C}\right)\\
&\leq Q_\alpha\left(\frac{1}{d_{B_2}^2}\sum_i U_{B_2}^i\rho_{AB_1B_2C}\left(U_{B_2}^i\right)^\dagger,\tau_{AC},\omega_C,\frac{1}{d_{B_2}^2}\sum_i U_{B_2}^i\theta_{B_1B_2C}\left(U_{B_2}^i\right)^\dagger\right) &\text{(B.5.19)}\\
&= Q_\alpha\left(\rho_{AB_1C}\otimes\pi_{B_2},\tau_{AC},\omega_C,\theta_{B_1C}\otimes\pi_{B_2}\right) &\text{(B.5.20)}\\
&= Q_\alpha\left(\rho_{AB_1C},\tau_{AC},\omega_C,\theta_{B_1C}\right), &\text{(B.5.21)}
\end{aligned}$$

where π is the maximally mixed state. After taking logarithms and dividing by $\alpha-1$, we can conclude the monotonicity for $\alpha\in[0,1)$. A similar development with Ando's convexity theorem gets the monotonicity for $\alpha\in(1,2]$. The inequalities in (B.5.13)-(B.5.15) follow from a similar line of reasoning. ■

Remark B.12. *Let $\rho_{ABC}\in\mathcal{S}\left(\mathcal{H}_{ABC}\right)$, $\tau_{AC}\in\mathcal{S}\left(\mathcal{H}_{AC}\right)$, $\theta_{BC}\in\mathcal{S}\left(\mathcal{H}_{BC}\right)$, and $\omega_C\in\mathcal{S}\left(\mathcal{H}_C\right)$ and suppose that the non-orthogonality condition in* (B.4.3) *holds. It is an open question to determine whether the Δ_α quantities defined from* (B.4.1), (B.4.5)-(B.4.9) *are monotone non-increasing with respect to quantum operations acting on either systems A or B for $\alpha\in[0,1)\cup(1,2]$. In particular, it is an open question to determine whether $\Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\rho_{BC}\right)$ and $\inf_{\theta_{BC}}\Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\theta_{BC}\right)$ are monotone non-increasing with respect to quantum operations acting on system A for $\alpha\in[0,1)\cup(1,2]$.*

Corollary B.13. *Let $\rho_{ABC}\in\mathcal{S}\left(\mathcal{H}_{ABC}\right)$, $\tau_{AC}\in\mathcal{S}\left(\mathcal{H}_{AC}\right)$, $\theta_{BC}\in\mathcal{S}\left(\mathcal{H}_{BC}\right)$, and $\omega_C\in\mathcal{S}\left(\mathcal{H}_C\right)$. All Rényi generalizations of the conditional mutual information derived from*

$$\Delta_\alpha\left(\rho_{ABC},\tau_{AC},\omega_C,\theta_{BC}\right),\qquad\Delta_\alpha\left(\rho_{ABC},\omega_C,\tau_{AC},\theta_{BC}\right),\tag{B.5.22}$$

are monotone non-increasing with respect to quantum operations acting on system B, for $\alpha\in[0,1)\cup(1,2]$. All Rényi generalizations of the quantum conditional mutual information derived from

$$\Delta_\alpha\left(\rho_{ABC},\omega_C,\theta_{BC},\tau_{AC}\right),\qquad\Delta_\alpha\left(\rho_{ABC},\theta_{BC},\omega_C,\tau_{AC}\right),\tag{B.5.23}$$

are monotone non-increasing with respect to quantum operations acting on system A, for $\alpha\in[0,1)\cup(1,2]$. The derived Rényi generalizations are optimized with respect to τ_{AC}, ω_C, and θ_{BC} satisfying the support condition in (A.5.3) *(which implies the non-orthogonality condition in* (B.4.3)*).*

Proof. We prove that a variation derived from (A.5.18) obeys the monotonicity (with the others mentioned above following from similar ideas). Beginning with the inequality in Lemma B.11, we find that

$$\begin{aligned}
\sup_{\omega_C}\Delta_\alpha\left(\rho_{ABC},\tau_{AC},\omega_C,\theta_{BC}\right)&\geq\sup_{\omega_C}\Delta_\alpha\left(\mathcal{M}_{B\to B'}\left(\rho_{ABC}\right),\tau_{AC},\omega_C,\mathcal{M}_{B\to B'}\left(\theta_{BC}\right)\right), &\text{(B.5.24)}\\
&\geq\inf_{\tau'_{AC},\theta'_{BC}}\sup_{\omega_C}\Delta_\alpha\left(\mathcal{M}_{B\to B'}\left(\rho_{ABC}\right),\tau'_{AC},\omega_C,\theta'_{BC}\right). &\text{(B.5.25)}
\end{aligned}$$

Since this inequality holds for all τ_{AC} and θ_{BC}, it holds in particular for the infimum of the first line over all such states, establishing monotonicity for the Rényi generalization of the QCMI derived from (A.5.18). ■

Corollary B.14. *We can employ the monotonicity inequalities from Lemma B.11 to conclude that some Rényi generalizations of the quantum conditional mutual information derived from* (B.5.22)-(B.5.23) *and Proposition A.3 are non-negative for all* $\alpha \in [0,1) \cup (1,2]$. *This includes* $\Delta_\alpha(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC})$ *and the one from Definition B.1.*

Proof. Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$ and suppose that the support condition in (A.5.3) holds. A common proof technique applies to reach the conclusions stated above. We illustrate with an example for

$$\inf_{\theta_{BC}} \sup_{\omega_C} \Delta_\alpha(\rho_{ABC}, \rho_{AC}, \omega_C, \theta_{BC}). \tag{B.5.26}$$

We apply Lemma B.11, choosing the local map on system B to be a trace-out map, to conclude that

$$\Delta_\alpha(\rho_{ABC}, \rho_{AC}, \omega_C, \theta_{BC}) \geq \Delta_\alpha(\rho_{AC}, \rho_{AC}, \omega_C, \theta_C). \tag{B.5.27}$$

Then, we can conclude that

$$\sup_{\omega_C} \Delta_\alpha(\rho_{ABC}, \rho_{AC}, \omega_C, \theta_{BC}) \geq \sup_{\omega_C} \Delta_\alpha(\rho_{AC}, \rho_{AC}, \omega_C, \theta_C) \tag{B.5.28}$$

$$\geq \Delta_\alpha(\rho_{AC}, \rho_{AC}, \theta_C, \theta_C) \tag{B.5.29}$$

$$= \frac{1}{\alpha-1} \log \operatorname{Tr}\left\{\rho_{AC}^{\alpha} \rho_{AC}^{(1-\alpha)/2} \theta_C^{(\alpha-1)/2} \theta_C^{1-\alpha} \theta_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2}\right\} \tag{B.5.30}$$

$$= \frac{1}{\alpha-1} \log \operatorname{Tr}\left\{\rho_{AC} \theta_C^0\right\} \tag{B.5.31}$$

$$= 0, \tag{B.5.32}$$

with the last inequality following from the support condition $\operatorname{supp}(\rho_{ABC}) \subseteq \operatorname{supp}(\theta_{BC})$ implying the support condition $\operatorname{supp}(\rho_{AC}) \subseteq \operatorname{supp}(\theta_C)$ [153, Lemma B.4.2]. Since the inequality holds for all θ_{BC} satisfying the support condition, we can conclude that the quantity in (B.5.26) is non-negative. A similar technique can be used to conclude that other Rényi generalizations of the QCMI are non-negative (including the one in Definition B.1). ■

Remark B.15. *If the system C is classical, then the Rényi quantum conditional mutual information given in Definition B.1 is monotone with respect to local operations on both A and B. This is because the optimizing state is classical on system C and then we have the commutation*

$$\rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2} \sigma_{BC}^{1-\alpha} \rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} = \sigma_{BC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2} \rho_{AC}^{1-\alpha} \rho_C^{(\alpha-1)/2} \sigma_{BC}^{(1-\alpha)/2}. \tag{B.5.33}$$

Remark B.16. *It is an open question to determine whether all Rényi generalizations of the quantum conditional mutual information designed from the different optimizations in Proposition A.3 and the different orderings in* (B.4.1), (B.4.5)-(B.4.9) *are non-negative for* $\alpha \in [0,1) \cup (1,2]$.

We now consider monotonicity of the $\widetilde{\Delta}_\alpha$ quantities under local quantum operations. For technical reasons, we restrict the development to positive definite density operators. It remains open to determine whether the following theorems hold under less restrictive conditions.

Lemma B.17. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$. Let $\mathcal{N}_{A\to A'}$ and $\mathcal{M}_{B\to B'}$ denote quantum operations acting on systems A and B, respectively. Then the following monotonicity inequalities hold for all $\alpha \in [1/2, 1) \cup (1, \infty)$:*

$$\widetilde{\Delta}_\alpha (\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}) \geq \widetilde{\Delta}_\alpha (\mathcal{M}_{B\to B'} (\rho_{ABC}), \tau_{AC}, \omega_C, \mathcal{M}_{B\to B'} (\theta_{BC})), \tag{B.5.34}$$

$$\widetilde{\Delta}_\alpha (\rho_{ABC}, \omega_C, \tau_{AC}, \theta_{BC}) \geq \widetilde{\Delta}_\alpha (\mathcal{M}_{B\to B'} (\rho_{ABC}), \omega_C, \tau_{AC}, \mathcal{M}_{B\to B'} (\theta_{BC})), \tag{B.5.35}$$

$$\widetilde{\Delta}_\alpha (\rho_{ABC}, \omega_C, \theta_{BC}, \tau_{AC}) \geq \widetilde{\Delta}_\alpha (\mathcal{N}_{A\to A'} (\rho_{ABC}), \omega_C, \theta_{BC}, \mathcal{N}_{A\to A'} (\tau_{AC})), \tag{B.5.36}$$

$$\widetilde{\Delta}_\alpha (\rho_{ABC}, \theta_{BC}, \omega_C, \tau_{AC}) \geq \widetilde{\Delta}_\alpha (\mathcal{N}_{A\to A'} (\rho_{ABC}), \theta_{BC}, \omega_C, \mathcal{N}_{A\to A'} (\tau_{AC})). \tag{B.5.37}$$

Proof. We first focus on establishing the inequality in (B.5.34) for $\alpha \in [1/2, 1)$. From part 1) of [85, Theorem 1.1], we know that the following function is jointly concave in S and T:

$$(S, T) \in \mathcal{B}(\mathcal{H})_{++} \times \mathcal{B}(\mathcal{H})_{++} \mapsto \text{Tr}\left\{\left[\Phi (S^p)^{1/2} \Psi (T^q) \Phi (S^p)^{1/2}\right]^s\right\}, \tag{B.5.38}$$

for strictly positive maps $\Phi(\cdot)$ and $\Psi(\cdot)$, $0 < p, q \leq 1$, and $1/2 \leq s \leq 1/(p+q)$. We can then see that $\widetilde{Q}_\alpha (\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ is of this form, with

$$\Psi = \tau_{AC}^{(1-\alpha)/2\alpha} \omega_C^{(\alpha-1)/2\alpha} (\cdot) \, \omega_C^{(\alpha-1)/2\alpha} \tau_{AC}^{(1-\alpha)/2\alpha}, \tag{B.5.39}$$

$$q = \frac{1-\alpha}{\alpha}, \tag{B.5.40}$$

$$\Phi(\cdot) = \text{id}, \tag{B.5.41}$$

$$p = 1, \tag{B.5.42}$$

$$s = \alpha. \tag{B.5.43}$$

For the range $\alpha \in [1/2, 1)$, we have that $p \in (0, 1]$ and $1/(p+q) = \alpha$, so that the conditions of part 1) of [85, Theorem 1.1] are satisfied. We conclude that $\widetilde{Q}_\alpha (\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ is jointly concave in θ_{BC} and ρ_{ABC}. From this, we can conclude the monotonicity in (B.5.34) for $\alpha \in [1/2, 1)$. A similar proof establishes the inequalities in (B.5.35)-(B.5.37) for $\alpha \in [1/2, 1)$.

The proof of (B.5.34) for $\alpha \in (1, \infty)$ is a straightforward generalization of the technique used for [65, Proposition 3]. To prove (B.5.34), it suffices to prove that the following function

$$(\rho_{ABC}, \theta_{BC}) \in \mathcal{S}(\mathcal{H}_{ABC})_{++} \times \mathcal{S}(\mathcal{H}_{ABC})_{++} \mapsto \text{Tr}\left\{\left[\rho_{ABC}^{1/2} K(\alpha) \, \rho_{ABC}^{1/2}\right]^\alpha\right\} \tag{B.5.44}$$

is jointly convex for $\alpha \in (1, \infty)$, where

$$K(\alpha) \equiv \tau_{AC}^{(1-\alpha)/2\alpha} \omega_C^{(\alpha-1)/2\alpha} \theta_{BC}^{(1-\alpha)/\alpha} \omega_C^{(\alpha-1)/2\alpha} \tau_{AC}^{(1-\alpha)/2\alpha}. \tag{B.5.45}$$

To this end, consider that we can write the trace function in (B.5.44) as

$$\text{Tr}\left\{\left[\rho_{ABC}^{1/2} K(\alpha) \, \rho_{ABC}^{1/2}\right]^\alpha\right\} = \sup_{H \geq 0} \alpha \text{Tr}\{H \rho_{ABC}\} - (\alpha - 1) \text{Tr}\left\{\left[H^{1/2} L(\alpha) \, H^{1/2}\right]^{\alpha/(\alpha-1)}\right\}, \tag{B.5.46}$$

where

$$L(\alpha) \equiv \tau_{AC}^{(\alpha-1)/2\alpha} \omega_C^{(1-\alpha)/2\alpha} \theta_{BC}^{(\alpha-1)/\alpha} \omega_C^{(1-\alpha)/2\alpha} \tau_{AC}^{(\alpha-1)/2\alpha}, \tag{B.5.47}$$

so that $[L(\alpha)]^{-1} = K(\alpha)$. From the fact that the following map

$$S \in \mathcal{B}(\mathcal{H})_+ \mapsto \operatorname{Tr}\left\{ \left[T^\dagger S^p T \right]^{1/p} \right\} \tag{B.5.48}$$

is concave in S for a fixed $T \in \mathcal{B}(\mathcal{H})$ and for $-1 \leq p \leq 1$ [65, Lemma 5] and the representation formula given in (B.5.46), we can then conclude that the function in (B.5.44) is jointly convex in ρ_{ABC} and θ_{BC} for $\alpha \in (1, \infty)$.

So it remains to prove the representation formula in (B.5.46). Recall from the alternative proof of [65, Lemma 4] that for positive semi-definite operators X and Y and $1 < p, q < \infty$ with $1/p + 1/q = 1$, the following inequality holds

$$\operatorname{Tr}\{XY\} \leq \frac{1}{p} \operatorname{Tr}\{X^p\} + \frac{1}{q} \operatorname{Tr}\{Y^q\}, \tag{B.5.49}$$

with equality holding if $X^p = Y^q$. To apply the inequality in (B.5.49), we set

$$X = K(\alpha)^{1/2} \rho_{ABC} K(\alpha)^{1/2}, \tag{B.5.50}$$

$$Y = L(\alpha)^{1/2} H L(\alpha)^{1/2}, \tag{B.5.51}$$

$$p = \alpha, \tag{B.5.52}$$

$$q = \frac{\alpha}{\alpha - 1}. \tag{B.5.53}$$

Applying (B.5.49), we find that

$$\operatorname{Tr}\{H\rho_{ABC}\} \leq \frac{1}{\alpha} \operatorname{Tr}\left\{ \left[\rho_{ABC}^{1/2} K(\alpha) \rho_{ABC}^{1/2} \right]^\alpha \right\} + \frac{\alpha - 1}{\alpha} \operatorname{Tr}\left\{ \left[H^{1/2} L(\alpha) H^{1/2} \right]^{\alpha/(\alpha-1)} \right\}, \tag{B.5.54}$$

which can be rewritten as

$$\alpha \operatorname{Tr}\{H\rho_{ABC}\} - (\alpha - 1) \operatorname{Tr}\left\{ \left[H^{1/2} L(\alpha) H^{1/2} \right]^{\alpha/(\alpha-1)} \right\} \leq \operatorname{Tr}\left\{ \left[\rho_{ABC}^{1/2} K(\alpha) \rho_{ABC}^{1/2} \right]^\alpha \right\}. \tag{B.5.55}$$

From the equality condition $X^p = Y^q$, we can see that the optimal H attaining equality is

$$L(\alpha)^{-1/2} \left[K(\alpha)^{1/2} \ \rho_{ABC} \ K(\alpha)^{1/2} \right]^{\alpha-1} L(\alpha)^{-1/2}. \tag{B.5.56}$$

This proves the representation formula in (B.5.46). A proof similar to the above one demonstrates (B.5.35)-(B.5.37) for $\alpha \in (1, \infty)$. ■

Remark B.18. *It is open to determine whether Lemma B.17 applies to* $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})$, *and* $\omega_C \in \mathcal{S}(\mathcal{H}_C)$. *That is, it is not clear to us whether Lemma B.17 can be extended by a straightforward continuity argument as was the case in [65, Proposition 3], due to the fact that* $\widetilde{\Delta}_\alpha$ *features many non-commutative matrix multiplications which can interact in non-trivial ways.*

Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$*,* $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$*,* $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$*, and* $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$*. It is an open question to determine whether the* $\widetilde{\Delta}_\alpha$ *quantities defined from* (B.4.12)*,* (B.4.18)*-*(B.4.22) *are monotone non-increasing with respect to quantum operations acting on either systems* A *or* B *for* $\alpha \in [1/2, 1) \cup (1, \infty)$*. It is also an open question to determine whether* $\widetilde{I}_\alpha(A; B|C)_\rho$ *is monotone non-increasing with respect to local quantum operations acting on the system* A *for* $\alpha \in [1/2, 1) \cup (1, \infty)$*.*

Corollary B.19. *Let* $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$*,* $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$*,* $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$*, and* $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$*. All sandwiched Rényi generalizations of the quantum conditional mutual information derived from*

$$\widetilde{\Delta}_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}), \qquad \widetilde{\Delta}_\alpha(\rho_{ABC}, \omega_C, \tau_{AC}, \theta_{BC}), \tag{B.5.57}$$

are monotone non-increasing with respect to quantum operations on system B*, for* $\alpha \in [1/2, 1) \cup (1, \infty)$*. All sandwiched Rényi generalizations of the quantum conditional mutual information derived from*

$$\widetilde{\Delta}_\alpha(\rho_{ABC}, \omega_C, \theta_{BC}, \tau_{AC}), \quad \widetilde{\Delta}_\alpha(\rho_{ABC}, \theta_{BC}, \omega_C, \tau_{AC}), \tag{B.5.58}$$

are monotone non-increasing with respect to quantum operations on system A*, for* $\alpha \in [1/2, 1) \cup (1, \infty)$*.*

Proof. The argument is exactly the same as that in the proof of Corollary B.13. ■

Corollary B.20. *We can employ the monotonicity inequalities from Lemma B.11 to conclude that some Rényi generalizations of the quantum conditional mutual information derived from* (B.5.57)*-*(B.5.58) *and Proposition A.3 are non-negative for all* $\alpha \in [1/2, 1) \cup (1, \infty)$*. This includes* $\widetilde{\Delta}_\alpha(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC})$ *and the one from* (B.4.24)*.*

Proof. The argument proceeds similarly to that in the proof of Corollary B.14. ■

Remark B.21. *It is an open question to determine whether all sandwiched Rényi generalizations of the conditional mutual information designed from the different optimizations in Proposition A.3 and the different orderings in* (B.4.12)*,* (B.4.18)*-*(B.4.22) *are non-negative for* $\alpha \in [1/2, 1) \cup (1, \infty)$*.*

B.5.3 Duality

A fundamental property of the QCMI is a duality relation: For a four-party pure state ψ_{ABCD}, the following equality holds

$$I(A; B|C)_\psi = I(A; B|D)_\psi . \tag{B.5.59}$$

This can easily be verified by considering Schmidt decompositions of ψ_{ABCD} for the different possible bipartite cuts of $ABCD$ (see [49, 203] for an operational interpretation of this duality in terms of the state redistribution protocol). Furthermore, since the QCMI is symmetric under the exchange of A and B, we have the following equalities:

$$I(B; A|C)_\psi = I(A; B|C)_\psi = I(A; B|D)_\psi = I(B; A|D)_\psi . \tag{B.5.60}$$

In this section, we prove that the Rényi QCMI in Definition B.1 and the sandwiched quantity in Definition B.3 obey a duality relation of the above form. However, note that other (but not all) variations satisfy duality as well. In order to prove these results, we make use of the following standard lemma:

Lemma B.22. *For any bipartite pure state ψ_{AB}, any Hermitian operator M_A acting on system A, and the maximally entangled vector $|\Gamma\rangle_{AB} \equiv \sum_j |j\rangle_A |j\rangle_B$ (with $\{|j\rangle_A\}$ and $\{|j\rangle_B\}$ orthonormal bases), we have that*

$$(M_A \otimes I_B)\,|\Gamma\rangle_{AB} = \left(I_A \otimes M_B^T\right)|\Gamma\rangle_{AB}\,, \tag{B.5.61}$$

$$\psi_A\,|\psi\rangle_{AB} = \psi_B\,|\psi\rangle_{AB}\,, \tag{B.5.62}$$

$$\langle\psi|M_A \otimes I_B|\psi\rangle_{AB} = \langle\psi|I_A \otimes M_B^T|\psi\rangle_{AB}, \tag{B.5.63}$$

where the transpose is with respect to the Schmidt basis.

Theorem B.23. *The following duality relation holds for all $\alpha \in (0,1)\cup(1,\infty)$ for a pure four-party state ψ_{ABCD}:*

$$I_\alpha\,(A;B|C)_\psi = I_\alpha\,(B;A|D)_\psi\,. \tag{B.5.64}$$

Proof. Our proof exploits ideas used in the proof of [183, Lemma 6] and [182, Theorem 2]. We know from Proposition B.2 that

$$I_\alpha\,(A;B|C)_\psi = \frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABC}^{\alpha}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}, \tag{B.5.65}$$

$$I_\alpha\,(B;A|D)_\psi = \frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\left(\operatorname{Tr}_B\left\{\psi_D^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{ABD}^{\alpha}\psi_{BD}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}. \tag{B.5.66}$$

Thus, we will have proved the theorem if we can show that the eigenvalues of

$$\operatorname{Tr}_A\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABC}^{\alpha}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\} \tag{B.5.67}$$

and

$$\operatorname{Tr}_B\left\{\psi_D^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{ABD}^{\alpha}\psi_{BD}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\} \tag{B.5.68}$$

are the same. To show this, consider that

$$\begin{aligned}
&\operatorname{Tr}_A\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABC}^{\alpha}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\} \\
&= \operatorname{Tr}_A\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABC}^{(\alpha-1)/2}\psi_{ABC}\psi_{ABC}^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\} && \text{(B.5.69)} \\
&= \operatorname{Tr}_{AD}\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABC}^{(\alpha-1)/2}\psi_{ABCD}\psi_{ABC}^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\}. && \text{(B.5.70)}
\end{aligned}$$

The eigenvalues of the operator in the last line are the same as those of the operator in the first line of what follows (from the Schmidt decomposition):

$$
\begin{aligned}
&\operatorname{Tr}_{BC}\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABC}^{(\alpha-1)/2}\psi_{ABCD}\psi_{ABC}^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\}\\
&=\operatorname{Tr}_{BC}\left\{\psi_C^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{D}^{(\alpha-1)/2}\psi_{ABCD}\psi_{D}^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_C^{(\alpha-1)/2}\right\} &\text{(B.5.71)}\\
&=\operatorname{Tr}_{BC}\left\{\psi_D^{(\alpha-1)/2}\psi_{C}^{(\alpha-1)/2}\psi_{AC}^{(\alpha-1)/2}\psi_{ABCD}\psi_{AC}^{(\alpha-1)/2}\psi_{C}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\} &\text{(B.5.72)}\\
&=\operatorname{Tr}_{BC}\left\{\psi_D^{(\alpha-1)/2}\psi_{C}^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{ABCD}\psi_{BD}^{(\alpha-1)/2}\psi_{C}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\} &\text{(B.5.73)}\\
&=\operatorname{Tr}_{BC}\left\{\psi_D^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{C}^{(\alpha-1)/2}\psi_{ABCD}\psi_{C}^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\} &\text{(B.5.74)}\\
&=\operatorname{Tr}_{BC}\left\{\psi_D^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{ABD}^{(\alpha-1)/2}\psi_{ABCD}\psi_{ABD}^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\} &\text{(B.5.75)}\\
&=\operatorname{Tr}_{B}\left\{\psi_D^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{ABD}^{(\alpha-1)/2}\psi_{ABD}\psi_{ABD}^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\} &\text{(B.5.76)}\\
&=\operatorname{Tr}_{B}\left\{\psi_D^{(\alpha-1)/2}\psi_{BD}^{(\alpha-1)/2}\psi_{ABD}^{\alpha}\psi_{BD}^{(\alpha-1)/2}\psi_D^{(\alpha-1)/2}\right\}. &\text{(B.5.77)}
\end{aligned}
$$

In the above, we have applied (B.5.62) several times. ■

Theorem B.24. *The following duality relation holds for all $\alpha \in (0,1) \cup (1,\infty)$ for a pure four-party state ψ_{ABCD}:*

$$\widetilde{I}_\alpha(A;B|C)_\psi = \widetilde{I}_\alpha(B;A|D)_\psi . \tag{B.5.78}$$

Proof. Our proof uses ideas similar to those in the proof of [132, Theorem 10]. We start by considering the case $\alpha > 1$. We recall that it is possible to express the α-norm with its dual norm (see, e.g., [132, Lemma 12]):

$$
\begin{aligned}
&\inf_{\sigma_{BC}}\sup_{\omega_C}\left\|\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\right\|_\alpha =\\
&\inf_{\sigma_{BC}}\sup_{\omega_C}\sup_{\tau_{ABC}}\operatorname{Tr}\left\{\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\tau_{ABC}^{(\alpha-1)/\alpha}\right\}. \qquad \text{(B.5.79)}
\end{aligned}
$$

So it suffices to prove the following relation:

$$
\begin{aligned}
&\inf_{\sigma_{BC}}\sup_{\omega_C}\sup_{\tau_{ABC}}\operatorname{Tr}\left\{\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\tau_{ABC}^{(\alpha-1)/\alpha}\right\} =\\
&\qquad\inf_{\sigma_{AD}}\sup_{\tau_D}\sup_{\omega_{ABD}}\operatorname{Tr}\left\{\psi_{ABD}^{1/2}\psi_{BD}^{(1-\alpha)/2\alpha}\tau_D^{(\alpha-1)/2\alpha}\sigma_{AD}^{(1-\alpha)/\alpha}\tau_D^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABD}^{1/2}\omega_{ABD}^{(\alpha-1)/\alpha}\right\},
\end{aligned}
\tag{B.5.80}
$$

because

$$
\begin{aligned}
\widetilde{I}_\alpha(B;A|D)_\psi = \inf_{\sigma_{AD}}\sup_{\tau_D}\sup_{\omega_{ABD}}\frac{\alpha}{\alpha-1}\log\operatorname{Tr}\Big\{&\psi_{ABD}^{1/2}\psi_{BD}^{(1-\alpha)/2\alpha}\tau_D^{(\alpha-1)/2\alpha}\sigma_{AD}^{(1-\alpha)/\alpha}\tau_D^{(\alpha-1)/2\alpha}\\
&\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABD}^{1/2}\omega_{ABD}^{(\alpha-1)/\alpha}\Big\}.
\end{aligned}
\tag{B.5.81}
$$

Indeed, we will prove that

$$\operatorname{Tr}\left\{\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\tau_{ABC}^{(\alpha-1)/\alpha}\right\} = \operatorname{Tr}\Big\{\psi_{ABD}^{1/2}\psi_{BD}^{(1-\alpha)/2\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\left(\sigma_{AD}^T\right)^{(1-\alpha)/\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\psi_{BD}^{(1-\alpha)/2\alpha} \psi_{ABD}^{1/2}\left(\omega_{ABD}^T\right)^{(\alpha-1)/\alpha}\Big\}, \quad \text{(B.5.82)}$$

from which one can conclude (B.5.80), which has the optimizations.

Proceeding, we observe that

$$\operatorname{Tr}\left\{\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\tau_{ABC}^{(\alpha-1)/\alpha}\right\}$$

$$= \langle\Gamma|\,\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\tau_{ABC}^{(\alpha-1)/\alpha}\,|\Gamma\rangle_{ABC|D} \quad \text{(B.5.83)}$$

$$= \langle\Gamma|\,\psi_{ABC}^{1/2}\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}\psi_{ABC}^{1/2}\left(\tau_D^T\right)^{(\alpha-1)/\alpha}|\Gamma\rangle_{ABC|D} \quad \text{(B.5.84)}$$

$$= \langle\psi|\,\psi_{AC}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{AC}^{(1-\alpha)/2\alpha}|\psi\rangle_{ABCD} \quad \text{(B.5.85)}$$

$$= \langle\psi|\,\psi_{BD}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}\psi_{BD}^{(1-\alpha)/2\alpha}|\psi\rangle_{ABCD} \quad \text{(B.5.86)}$$

$$= \langle\psi|\,\omega_C^{(\alpha-1)/2\alpha}\psi_{BD}^{(1-\alpha)/2\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\sigma_{BC}^{(1-\alpha)/\alpha}\left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\psi_{BD}^{(1-\alpha)/2\alpha}\omega_C^{(\alpha-1)/2\alpha}|\psi\rangle_{ABCD} \quad \text{(B.5.87)}$$

$$= \langle\Gamma|\,\psi_{ABD}^{1/2}\omega_C^{(\alpha-1)/2\alpha}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\sigma_{BC}^{\frac{1-\alpha}{\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\omega_C^{(\alpha-1)/2\alpha}\psi_{ABD}^{1/2}|\Gamma\rangle_{ABD|C} \quad \text{(B.5.88)}$$

$$= \langle\Gamma|\,\omega_C^{(\alpha-1)/2\alpha}\psi_{ABD}^{1/2}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\sigma_{BC}^{\frac{1-\alpha}{\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\psi_{ABD}^{1/2}\omega_C^{(\alpha-1)/2\alpha}|\Gamma\rangle_{ABD|C} \quad \text{(B.5.89)}$$

$$= \langle\Gamma|\left(\omega_{ABD}^T\right)^{\frac{\alpha-1}{2\alpha}}\psi_{ABD}^{1/2}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\sigma_{BC}^{\frac{1-\alpha}{\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\psi_{ABD}^{1/2}\left(\omega_{ABD}^T\right)^{\frac{\alpha-1}{2\alpha}}|\Gamma\rangle_{ABD|C}, \quad \text{(B.5.90)}$$

where we used the standard transpose trick (B.5.61) for the maximally entangled vector $|\Gamma\rangle_{ABD|C}$ and the first identity from Lemma B.22. For the vector

$$|\varphi\rangle_{ABCD} \equiv \left(\tau_D^T\right)^{(\alpha-1)/2\alpha}\psi_{BD}^{(1-\alpha)/2\alpha}\psi_{ABD}^{1/2}\left(\omega_{ABD}^T\right)^{(\alpha-1)/2\alpha}|\Gamma\rangle_{ABD|C}, \quad \text{(B.5.91)}$$

we get from the second identity in Lemma B.22 that

$$\langle\Gamma|\left(\omega_{ABD}^T\right)^{\frac{\alpha-1}{2\alpha}}\psi_{ABD}^{1/2}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\sigma_{BC}^{\frac{1-\alpha}{\alpha}}\left(\tau_D^T\right)^{\frac{\alpha-1}{2\alpha}}\psi_{BD}^{\frac{1-\alpha}{2\alpha}}\psi_{ABD}^{1/2}\left(\omega_{ABD}^T\right)^{\frac{\alpha-1}{2\alpha}}|\Gamma\rangle_{ABD|C} = \langle\varphi|\,\sigma_{BC}^{\frac{1-\alpha}{\alpha}}|\varphi\rangle_{ABCD} \quad \text{(B.5.92)}$$

$$= \langle\varphi| \left(\sigma_{AD}^{T}\right)^{\frac{1-\alpha}{\alpha}} |\varphi\rangle_{ABCD} \tag{B.5.93}$$

$$= \langle\Gamma| \left(\omega_{ABD}^{T}\right)^{\frac{\alpha-1}{2\alpha}} \psi_{ABD}^{1/2}\psi_{BD}^{\frac{1-\alpha}{2\alpha}} \left(\tau_{D}^{T}\right)^{\frac{\alpha-1}{2\alpha}} \left(\sigma_{AD}^{T}\right)^{\frac{1-\alpha}{\alpha}} \left(\tau_{D}^{T}\right)^{\frac{\alpha-1}{2\alpha}} \psi_{BD}^{\frac{1-\alpha}{2\alpha}}\psi_{ABD}^{1/2} \left(\omega_{ABD}^{T}\right)^{\frac{\alpha-1}{2\alpha}} |\Gamma\rangle_{ABD|C} \tag{B.5.94}$$

$$= \operatorname{Tr}\left\{\left(\omega_{ABD}^{T}\right)^{\frac{\alpha-1}{2\alpha}} \psi_{ABD}^{1/2}\psi_{BD}^{\frac{1-\alpha}{2\alpha}} \left(\tau_{D}^{T}\right)^{\frac{\alpha-1}{2\alpha}} \left(\sigma_{AD}^{T}\right)^{(1-\alpha)/\alpha} \left(\tau_{D}^{T}\right)^{\frac{\alpha-1}{2\alpha}} \psi_{BD}^{\frac{1-\alpha}{2\alpha}}\psi_{ABD}^{1/2} \left(\omega_{ABD}^{T}\right)^{\frac{\alpha-1}{2\alpha}}\right\} \tag{B.5.95}$$

$$= \operatorname{Tr}\left\{\psi_{ABD}^{1/2}\psi_{BD}^{(1-\alpha)/2\alpha} \left(\tau_{D}^{T}\right)^{(\alpha-1)/2\alpha} \left(\sigma_{AD}^{T}\right)^{(1-\alpha)/\alpha} \left(\tau_{D}^{T}\right)^{(\alpha-1)/2\alpha} \psi_{BD}^{(1-\alpha)/2\alpha}\psi_{ABD}^{1/2} \left(\omega_{ABD}^{T}\right)^{(\alpha-1)/\alpha}\right\}. \tag{B.5.96}$$

For the case $\alpha \in (0,1)$ the proof is similar, where we also use [132, Lemma 12]. We omit the details for this case. ■

B.6 Conjectured Monotonicity in α

From numerical evidence and proofs for some special cases, we think it is natural to put forward the following conjecture:

Conjecture B.25. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$. Then all of the Rényi core quantities Δ_α and $\widetilde{\Delta}_\alpha$ derived from* (B.4.1), (B.4.5)-(B.4.9) *and* (B.4.12), (B.4.18)-(B.4.22)*, respectively, are monotone non-decreasing in α. That is, for $0 \le \alpha \le \beta$, the following inequalities hold*

$$\Delta_\alpha\left(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}\right) \le \Delta_\beta\left(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}\right), \tag{B.6.1}$$

$$\widetilde{\Delta}_\alpha\left(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}\right) \le \widetilde{\Delta}_\beta\left(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}\right), \tag{B.6.2}$$

and similar inequalities hold for all orderings of the last three arguments of Δ_α and $\widetilde{\Delta}_\alpha$.

If Conjecture B.25 is true, we could conclude that all non-sandwiched and sandwiched Rényi generalizations of the QCMI are monotone non-decreasing in α for positive definite operators. Another implication of monotonicity in $\alpha \ge 1/2$ for $\widetilde{\Delta}_\alpha\left(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC}\right)$ would be that a tripartite quantum state ρ_{ABC} is a quantum Markov state if and only if

$$\widetilde{\Delta}_\alpha\left(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC}\right) = 0 \tag{B.6.3}$$

(with $\alpha \ge 1/2$). This would generalize the results from [80] to the case $\alpha \ne 1$. However, note that (B.6.3) has now been proven for $\alpha \in (0,1) \cup (1,2)$ in [47].

Note that this conjecture does not follow straightforwardly from the following monotonicity

$$D_\alpha\left(\rho\|\sigma\right) \le D_\beta\left(\rho\|\sigma\right), \tag{B.6.4}$$

$$\widetilde{D}_\alpha\left(\rho\|\sigma\right) \le \widetilde{D}_\beta\left(\rho\|\sigma\right), \tag{B.6.5}$$

which holds for $0 \le \alpha \le \beta$ [183, 132]. However, for classical states ρ_{ABC}, the conjecture is clearly true for $\Delta_\alpha\left(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC}\right)$ and $\widetilde{\Delta}_\alpha\left(\rho_{ABC}, \rho_{AC}, \rho_C, \rho_{BC}\right)$ by appealing to the above known inequalities.

Observe that some of the conjectured inequalities are redundant. For example, if

$$\Delta_\alpha\left(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C\right) \leq \Delta_\beta\left(\rho_{ABC}, \tau_{AC}, \theta_{BC}, \omega_C\right) \tag{B.6.6}$$

holds for all $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$, then the following monotonicity holds as well

$$\Delta_\alpha\left(\rho_{ABC}, \theta_{BC}, \tau_{AC}, \omega_C\right) \leq \Delta_\beta\left(\rho_{ABC}, \theta_{BC}, \tau_{AC}, \omega_C\right), \tag{B.6.7}$$

due to a symmetry under the exchange of systems A and B. Similar statements apply to other pairs of inequalities, so that it suffices to prove only six of the 12 monotonicities discussed above in order to establish the other six. However, as we will see below, a single proof of the monotonicity for each kind of Rényi QCMI (non-sandwiched and sandwiched) should suffice because we think one could easily generalize such a proof to the other cases.

B.6.1 Approaches for proving the conjecture

We briefly outline some approaches for proving the conjecture. One idea is to follow a proof technique from [183, Lemma 3] and [132, Theorem 7]. If the derivative of $\Delta_\alpha(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC})$ and $\widetilde{\Delta}_\alpha\left(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}\right)$ with respect to α is non-negative, then we can conclude that these functions are monotone increasing with α. It is possible to prove that the derivatives are non-negative when α is in a neighborhood of one, by computing Taylor expansions of these functions. We explore this approach further in Appendix D.2.3.

B.6.2 Numerical evidence

To test the conjecture in (B.6.1) and its variations, we conducted several numerical experiments. First, we selected states ρ_{ABC}, τ_{AC}, ω_C, θ_{BC} at random [44], with the dimensions of the local systems never exceeding six. We then computed the numerator in (D.2.44) for values of γ ranging from -0.99 to 10 with a step size of 0.05 (so that $\alpha = \gamma + 1$ goes from 0.01 to 11). For each value of γ, we conducted 1000 numerical experiments. The result was that the numerator in (D.2.44) was always non-negative. We then conducted the same set of experiments for the various operator orderings and always found the numerator to be non-negative.

To test the conjecture in (B.6.2) and its variations, we conducted similar numerical experiments. First, we selected states ρ_{ABC}, τ_{AC}, ω_C, θ_{BC}, μ_{ABC} at random [44], with the dimensions of the local systems never exceeding six. We then computed the numerator in (D.2.53) for values of γ ranging from -10 to 0.99 with a step size of 0.05 (so that $\alpha = 1/\left(1-\gamma\right)$ goes from ≈ 0.091 to ≈ 100). For each value of γ, we conducted 1000 numerical experiments. The result was that the numerator in (D.2.53) was always non-negative. We then conducted the same set of experiments for the various operator orderings and always found the numerator to be non-negative.

B.6.3 Special cases of the conjecture

We can prove that the conjecture is true in a number of cases, due to the special form that the Rényi QCMI takes in these cases. Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$. Consider the Rényi and sandwiched Rényi QCMI of Definitions B.1 and B.3, respectively:

$$I_\alpha(A;B|C)_{\rho|\rho} \equiv \frac{1}{\alpha-1}\log\operatorname{Tr}\left\{\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_{C}^{(\alpha-1)/2}\rho_{BC}^{1-\alpha}\rho_{C}^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\right\}, \tag{B.6.8}$$

$$\widetilde{I}_\alpha(A;B|C)_{\rho|\rho} \equiv \frac{\alpha}{\alpha-1}\log\left\|\rho_{ABC}^{1/2}\rho_{AC}^{(1-\alpha)/2\alpha}\rho_{C}^{(\alpha-1)/2\alpha}\rho_{BC}^{(1-\alpha)/\alpha}\rho_{C}^{(\alpha-1)/2\alpha}\rho_{AC}^{(1-\alpha)/2\alpha}\rho_{ABC}^{1/2}\right\|_\alpha, \tag{B.6.9}$$

so that

$$I_0(A;B|C)_{\rho|\rho} = -\log\operatorname{Tr}\left\{\rho_{ABC}^{0}\rho_{AC}^{1/2}\rho_{C}^{-1/2}\rho_{BC}\rho_{C}^{-1/2}\rho_{AC}^{1/2}\right\}, \tag{B.6.10}$$

$$I_2(A;B|C)_{\rho|\rho} = \log\operatorname{Tr}\left\{\rho_{ABC}^{2}\left(\rho_{AC}^{1/2}\rho_{C}^{-1/2}\rho_{BC}\rho_{C}^{-1/2}\rho_{AC}^{1/2}\right)^{-1}\right\}. \tag{B.6.11}$$

Recall that the following inequality holds for all $\alpha \in (0,1)\cup(1,\infty)$ [46]:

$$\widetilde{D}_\alpha(\rho\|\sigma) \le D_\alpha(\rho\|\sigma). \tag{B.6.12}$$

Using the monotonicity given in (B.6.5) and the above inequality, we can conclude that

$$I_0(A;B|C)_{\rho|\rho} \le I_2(A;B|C)_{\rho|\rho}. \tag{B.6.13}$$

However, we cannot relate to the von Neumann entropy-based QCMI because its representation in terms of the relative entropy does not feature the operator $\rho_{AC}^{1/2}\rho_{C}^{-1/2}\rho_{BC}\rho_{C}^{-1/2}\rho_{AC}^{1/2}$ as its second argument but instead has $\exp\{\log\rho_{BC}+\log\rho_{AC}-\log\rho_C\}$.

Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC} \in \mathcal{S}(\mathcal{H}_{AC})_{++}$, $\omega_C \in \mathcal{S}(\mathcal{H}_C)_{++}$, and $\theta_{BC} \in \mathcal{S}(\mathcal{H}_{BC})_{++}$. Tomamichel has communicated that the inequality in (B.6.2) and its variations are true for $0 \le \alpha \le \beta$ and such that $1/\alpha + 1/\beta = 2$ [181]. This is because in such a case, we have that $\alpha/(1-\alpha) = -\beta(1-\beta)$, so that

$$\begin{aligned}&\left[\tau_{AC}^{(1-\alpha)/2\alpha}\omega_{C}^{(\alpha-1)/2\alpha}\theta_{BC}^{(1-\alpha)/\alpha}\omega_{C}^{(\alpha-1)/2\alpha}\tau_{AC}^{(1-\alpha)/2\alpha}\right]^{\alpha/(1-\alpha)}\\&\qquad= \left[\tau_{AC}^{(1-\beta)/2\beta}\omega_{C}^{(\beta-1)/2\beta}\theta_{BC}^{(1-\beta)/\beta}\omega_{C}^{(\beta-1)/2\beta}\tau_{AC}^{(1-\beta)/2\beta}\right]^{\beta/(1-\beta)},\end{aligned} \tag{B.6.14}$$

and similar equalities hold for the five other operator orderings. Since this is the case, the monotonicity follows directly from the ordinary monotonicity of the sandwiched Rényi relative entropy. By a similar line of reasoning, the inequality in (B.6.1) and its variations are true for $0 \le \alpha \le \beta$ and such that $\alpha + \beta = 2$. Similarly, in such a case, we have that $1-\alpha = -(1-\beta)$, so that

$$\begin{aligned}&\left[\tau_{AC}^{(1-\alpha)/2}\omega_{C}^{(\alpha-1)/2}\theta_{BC}^{1-\alpha}\omega_{C}^{(\alpha-1)/2}\tau_{AC}^{(1-\alpha)/2}\right]^{1/(1-\alpha)}\\&\qquad= \left[\tau_{AC}^{(1-\beta)/2}\omega_{C}^{(\beta-1)/2}\theta_{BC}^{1-\beta}\omega_{C}^{(\beta-1)/2}\tau_{AC}^{(1-\beta)/2}\right]^{1/(1-\beta)},\end{aligned} \tag{B.6.15}$$

and similar equalities hold for the five other operator orderings. Then the monotonicity again follows from the ordinary monotonicity of the Rényi relative entropy. The observation in (B.6.13) is then a special case of the above observation.

B.6.4 Implications for tripartite states with small conditional mutual information

It has been an open question since the work in [80] to characterize tripartite quantum states ρ_{ABC} with small conditional mutual information $I(A;B|C)_{\rho}$. That is, given that the various quantum Markov state conditions in (A.4.2) and (A.4.3)-(A.4.5) are equivalent to $I(A;B|C)_{\rho}$ being equal to zero, we would like to understand what happens when we perturb these various conditions. In this section, we pursue this direction and explicitly show how Conjecture B.25 could be used to address this important question.

Several researchers have already considered what happens when perturbing the quantum Markov state condition in (A.4.2), but we include a discussion here for completeness. To begin with, we know that if there exists a quantum Markov state $\mu_{ABC} \in \mathcal{M}_{A-C-B}$ such that

$$\left\|\rho_{ABC} - \mu_{ABC}\right\|_1 \leq \varepsilon \tag{B.6.16}$$

then

$$I(A;B|C)_{\mu} = 0, \tag{B.6.17}$$

$$I(A;B|C)_{\rho} \leq 8\varepsilon \log \min\{d_A, d_B\} + 4h_2(\varepsilon), \tag{B.6.18}$$

where

$$h_2(x) \equiv -x\log x - (1-x)\log(1-x) \tag{B.6.19}$$

is the binary entropy, which obeys

$$\lim_{\varepsilon \searrow 0} h_2(\varepsilon) = 0. \tag{B.6.20}$$

The first line is by definition and the second follows from an application of the Alicki-Fannes inequality [4]. However, the example in [39] and the subsequent development in [58] exclude a particular converse of the above bound. That is, by [39, Lemma 6], there exists a sequence of states ρ^d_{ABC} such that

$$I(A;B|C)_{\rho^d} = 2\log((d+2)/d), \tag{B.6.21}$$

which goes to zero as $d \to \infty$. However, for this same sequence of states, the following constant lower bound is known

$$\min_{\mu_{ABC} \in \mathcal{M}_{A-C-B}} D_0\left(\rho^d_{ABC} \middle\| \mu_{ABC}\right) \geq \log\sqrt{4/3}, \tag{B.6.22}$$

by [58, Theorem 1]. By employing monotonicity of the Rényi relative entropy with respect to the Rényi parameter, so that $D_{1/2} \geq D_0$, and the well-known relation $1 - \left\|\omega - \tau\right\|_1/2 \leq \text{Tr}\{\sqrt{\omega}\sqrt{\tau}\}$ for $\omega, \tau \in \mathcal{S}(\mathcal{H})$ (see, e.g., [32, Equation (22)]), we can readily translate the bound in (B.6.22) to a constant lower bound on the trace distance of ρ^d_{ABC} to the set of quantum Markov states:

$$\left\|\rho^d_{ABC} - \mathcal{M}_{A-C-B}\right\|_1 \equiv \min_{\mu_{ABC} \in \mathcal{M}_{A-C-B}} \left\|\rho^d_{ABC} - \mu_{ABC}\right\|_1 \geq 2\left(1 - (3/4)^{1/4}\right) \approx 0.139. \tag{B.6.23}$$

So (B.6.21) and (B.6.23) imply that a Pinsker-like bound of the form

$$I(A;B|C)_{\rho} \geq K \left\| \rho_{ABC} - \mathcal{M}_{A-C-B} \right\|_1^2 \tag{B.6.24}$$

cannot hold in general, with K a dimension-independent constant.

We now focus on a perturbation of the conditions in (A.4.3)-(A.4.4). It appears that these cases will be promising for applications if Conjecture B.25 is true. The following proposition states that the conditional mutual information is small if it is possible to recover the system A from system C alone (or by symmetry, if one can get B from C alone). We note that (B.6.27) was proven independently in [62, Eq. (8)].

Proposition B.26. *Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$, $\mathcal{R}_{C\to AC}$ be a CPTP "recovery" map, and $\varepsilon \in [0,1]$. Suppose that it is possible to recover the system A from system C alone, in the following sense*

$$\left\| \rho_{ABC} - \omega_{ABC} \right\|_1 \leq \varepsilon, \tag{B.6.25}$$

where

$$\omega_{ABC} \equiv \mathcal{R}_{C\to AC}(\rho_{BC}). \tag{B.6.26}$$

Then the conditional mutual informations $I(A;B|C)_{\rho}$ and $I(A;B|C)_{\omega}$ obey the following bounds:

$$I(A;B|C)_{\rho} \leq 4\varepsilon \log d_B + 2h_2(\varepsilon), \tag{B.6.27}$$

$$I(A;B|C)_{\omega} \leq 4\varepsilon \log d_B + 2h_2(\varepsilon), \tag{B.6.28}$$

where d_B is the dimension of the B system and $h_2(\varepsilon)$ is defined in (B.6.19). *By symmetry, a related bound holds if one can recover system B from system C alone.*

Proof. Consider that

$$\begin{aligned}
I(A;B|C)_{\rho} &= H(B|C)_{\rho} - H(B|AC)_{\rho} &\text{(B.6.29)}\\
&\leq H(B|AC)_{\omega} - H(B|AC)_{\rho} &\text{(B.6.30)}\\
&\leq H(B|AC)_{\omega} - H(B|AC)_{\omega} + 4\varepsilon \log d_B + 2h_2(\varepsilon) &\text{(B.6.31)}\\
&= 4\varepsilon \log d_B + 2h_2(\varepsilon). &\text{(B.6.32)}
\end{aligned}$$

The first inequality follows because the conditional entropy is monotone increasing under quantum operations on the conditioning system (the map $\mathcal{R}_{C\to AC}$ is applied to the system C of state ρ_{ABC} to produce ω_{ABC} and the conditional entropy only increases under such processing). The second inequality is a result of (B.6.25) and the Alicki-Fannes inequality [4] (continuity of conditional entropy). Similarly, consider that

$$\begin{aligned}
I(A;B|C)_{\omega} &= H(B|C)_{\omega} - H(B|AC)_{\omega} &\text{(B.6.33)}\\
&\leq H(B|C)_{\rho} - H(B|AC)_{\omega} + 4\varepsilon \log d_B + 2h_2(\varepsilon) &\text{(B.6.34)}\\
&\leq H(B|AC)_{\omega} - H(B|AC)_{\omega} + 4\varepsilon \log d_B + 2h_2(\varepsilon) &\text{(B.6.35)}\\
&= 4\varepsilon \log d_B + 2h_2(\varepsilon). &\text{(B.6.36)}
\end{aligned}$$

The first inequality is from the fact that (B.6.25) implies that

$$\left\|\rho_{BC}-\omega_{BC}\right\|_1 \leq \varepsilon \tag{B.6.37}$$

and the Alicki-Fannes' inequality. The second is again from monotonicity of conditional entropy. ■

The implications of Conjecture B.25 are nontrivial. For example, if it were true, then we could conclude a converse of Proposition B.26, that if the conditional mutual information is small, then it is possible to recover the system A from system C alone (or by symmetry, that one can get B from C alone). That is, the following relation would hold for $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})_{++}$:

$$\begin{aligned}
I\left(A;B|C\right)_\rho &\geq I_{\min}\left(A;B|C\right)_{\rho|\rho} && \text{(B.6.38)}\\
&= -\log F\left(\rho_{ABC}, \rho_{AC}^{1/2}\rho_C^{-1/2}\rho_{BC}\rho_C^{-1/2}\rho_{AC}^{1/2}\right) && \text{(B.6.39)}\\
&= -\log F\left(\rho_{ABC}, \mathcal{R}^P_{C\to AC}\left(\rho_{BC}\right)\right) && \text{(B.6.40)}\\
&\geq -\log\left[1-\left(\frac{1}{2}\left\|\rho_{ABC}-\mathcal{R}^P_{C\to AC}\left(\rho_{BC}\right)\right\|_1\right)^2\right] && \text{(B.6.41)}\\
&\geq \frac{1}{4}\left\|\rho_{ABC}-\mathcal{R}^P_{C\to AC}\left(\rho_{BC}\right)\right\|_1^2, && \text{(B.6.42)}
\end{aligned}$$

where $\mathcal{R}^P_{C\to AC}$ is Petz's transpose map discussed in [80]

$$\mathcal{R}^P_{C\to AC}(\cdot) \equiv \rho_{AC}^{1/2}\rho_C^{-1/2}(\cdot)\rho_C^{-1/2}\rho_{AC}^{1/2}. \tag{B.6.43}$$

In the above, the first inequality would follow from Conjecture B.25, the second is a result of well known relations between trace distance and fidelity [66], and the last is a consequence of the inequality $-\log(1-x) \geq x$, valid for $x \leq 1$. Thus, the truth of Conjecture B.25 would establish the truth of an open conjecture from [109] (up to a constant). As pointed out in [109], this would then imply that for tripartite states ρ_{ABC} with conditional mutual information $I(A;B|C)_\rho$ small (i.e., states that fulfill strong subadditivity with near equality), Petz's transpose map for the partial trace over A is good for recovering ρ_{ABC} from ρ_{BC}. Hence, even though ρ_{ABC} does not have to be close to a quantum Markov state if $I(A;B|C)_\rho$ is small (as discussed above), A would still be nearly independent of B from the perspective of C in the sense that ρ_{ABC} could be approximately recovered from ρ_{BC} alone. This would give an operationally useful characterization of states that fulfill strong subadditivity with near equality and would be helpful for answering some open questions concerning squashed entanglement, as discussed in [199].

For the quantum Markov state condition in (A.4.5), for simplicity we consider instead the "relative entropy distance" between ρ_{ABC} and ς_{ABC}, where

$$\varsigma_{ABC} \equiv \exp\left\{\log\rho_{AC}+\log\rho_{BC}-\log\rho_C\right\}. \tag{B.6.44}$$

So if

$$D\left(\rho_{ABC}\|\varsigma_{ABC}\right) \leq \varepsilon, \tag{B.6.45}$$

then we can conclude that

$$I(A;B|C)_\rho = D(\rho_{ABC} \| \varsigma_{ABC}) \leq \varepsilon. \tag{B.6.46}$$

If desired, one can also obtain an ε-dependent upper bound on $I(A;B|C)_{\varsigma'}$, where

$$\varsigma'_{ABC} \equiv \varsigma_{ABC} / \operatorname{Tr}\{\varsigma_{ABC}\}, \tag{B.6.47}$$

which vanishes in the limit as ε goes to zero. This can be accomplished by employing the bound in Corollary A.5 and by bounding $\operatorname{Tr}\{\varsigma_{ABC}\}$ from below by $1 - \|\rho_{ABC} - \varsigma_{ABC}\|_1$. The bound in Corollary A.5 also serves as a converse of these bounds: if the conditional mutual information is small, then the trace distance between ρ_{ABC} and ς_{ABC} is small. However, it is not clear that a perturbation of the quantum Markov state condition in (A.4.5) will be as useful in applications as a perturbation of (A.4.3)-(A.4.4) would be, mainly because the map $\rho_{ABC} \to \exp\{\log \rho_{AC} + \log \rho_{BC} - \log \rho_C\}$ is non-linear (as discussed in [108]).

B.7 Discussion

To summarize, in this appendix we defined several Rényi generalizations of the QCMI that satisfy the properties desired of such a generalization of the QCMI. Namely, we showed that these generalizations are non-negative and are monotone under local quantum operations on one of the systems A or B. An important open question is to prove that they are monotone under local quantum operations on both systems. Some of the Rényi generalizations satisfy a generalization of the duality relation $I(A;B|C) = I(A;B|D)$, which holds for a four-party pure state ψ_{ABCD}. We conjecture that these Rényi generalizations of the QCMI are monotone non-decreasing in the Rényi parameter α, and we have proved that this conjecture is true when α is in a neighborhood of one and in some other special cases. The truth of this conjecture in general would have implications in condensed matter physics, as detailed in [109], and quantum communication complexity, as mentioned in [186]. A summary of the properties of the proposed Rényi generalizations of the QCMI is given in Table B.1.

Table B.1: Rényi generalizations of the conditional quantum mutual information (QCMI). The Rényi generalizations prescribed in this work are applicable to the QCMI. The leftmost column of the table lists some desired properties of a Rényi QCMI. These properties are satisfied by the original von Neumann QCMI $I(A;B|C)_\rho$ in (B.2.4) as shown in Column 2. The Rényi QCMI in (B.2.6) obtained by simply replacing the linear sum of von Neumann entropies with the corresponding linear sum of Rényi entropies, in Column 3, is compared with the Rényi generalizations obtained through the formula prescribed in this work, in Columns 4 and 5. The question marks indicate open questions, with numerical evidence supporting a positive answer. The quantity in Column 3 does not retain many of the desired properties. On the contrary, the quantities in Columns 4 and 5 retain some of these desired properties. The table suggests that the latter are more useful Rényi generalizations of the QCMI.

Formula	QCMI in (B.2.4)	Rényi QCMI in (B.2.6)	Rényi QCMI in (B.4.11)	Rényi QCMI in (B.4.24)
Non-negative	✓	✗	✓	✓
Monotone under local op.'s on A	✓	✗	?	?
Monotone under local op.'s on B	✓	✗	✓	✓
Duality	✓	✓	✓	✓
Converges to (B.2.4) as $\alpha \to 1$	N/A	✓	✓	?
Monotone in α	N/A	✗	?	?

Based on the fact that the QCMI can be written as

$$I\left(A;B|C\right)_{\rho}=D\left(\rho_{ABC}\|\exp\left\{\log\rho_{AC}+\log\rho_{BC}-\log\rho_{C}\right\}\right), \tag{B.7.1}$$

one could consider another Rényi generalization of the QCMI, such as

$$D_{\alpha}\left(\rho_{ABC}\|\exp\left\{\log\rho_{AC}+\log\rho_{BC}-\log\rho_{C}\right\}\right), \tag{B.7.2}$$

or with the sandwiched variant. However, it is unclear to us whether (B.7.2) is monotone under local operations, which we have argued is an important property for a Rényi generalization of the QCMI.

There are many directions to consider going forward on the proposed Rényi QCMI. First, one could improve many of the results here on a technical level. It would be interesting to understand in depth the limits in (A.5.5), (B.4.4), and (B.4.17) in order to establish the most general support conditions for the Δ, Δ_{α}, and $\widetilde{\Delta}_{\alpha}$ quantities, respectively, as has been done for the quantum and Rényi relative entropies, as recalled in (2.2.33), (2.2.39), and (2.2.41). Next, if one could establish uniform convergence of the Δ_{α} and $\widetilde{\Delta}_{\alpha}$ quantities as α goes to one, then we could conclude that the optimized versions of these quantities converge to the QCMI in this limit. One might also attempt to extend Theorem B.6, Theorem B.8, and Lemma B.17 to hold for positive semi-definite density operators.

As far as applications are concerned, we explored a Rényi squashed entanglement in Chapter 3 and showed that several properties hold for the quantity which are analogous to the squashed entanglement [40]. Such a quantity might be helpful in strengthening [40, Proposition 10], so that the squashed entanglement could be interpreted as a strong converse upper bound on distillable entanglement. More generally, it might be helpful in strengthening the main result of [178], so that the upper bound established on the two-way assisted quantum capacity could be interpreted as a strong converse rate. We also explored a Rényi quantum discord in Chapter 3. Such a quantity could be used to study phase transitions in condensed matter systems [128]. More generally, the quantities defined here might be useful in the context of one-shot information theory, for example, to establish a one-shot state redistribution protocol as an extension of the main result of [49]. One could also explore applications of the Rényi QCMIs in the context of condensed matter physics or high energy physics, as the Rényi entropy has been employed extensively in these contexts [31].

Finally, these potential applications in information theory and physics should help in singling out some of our many possible definitions for Rényi QCMI.

Appendix C
Quantum Optical Metrology[1]

C.1 Introduction

Metrology is the science of precision measurements. It is fundamentally based on information acquisition and processing by physical systems. Thus, quantum mechanics has been considered to uncover the ultimate possibilities in metrology. *Quantum metrology* [74] is the field of research that concerns with this pursuit. Strategies suggested in quantum metrology have been found to enable measurements with precisions that surpass what is possible using classical strategies. Potential applications of this exciting field of research include gravitational wave detection [147], quantum positioning and clock synchronization [73], quantum frequency standards [97], quantum sensing [201, 43], quantum radar and LIDAR [106, 68], quantum imaging [170, 126] and quantum lithography [114, 113, 22].

Quantum metrology offers a theoretical framework to analyze the precision performance of measurement devices that employ quantum mechanical probes containing nonclassical effects such as entanglement or squeezing. The framework consists of the theory of quantum parameter estimation (discussed earlier in Section 2.5) [84, 26, 27].

Consider the typical scenario of parameter estimation described in Fig. C.1, where we want to estimate an unknown parameter associated with the unitary dynamics generated by a known physical process. We prepare probes in suitable quantum states, evolve them through the process, and measure the probes at the output using a suitable detection strategy. We then compare the input and output probe states, which allows us to estimate the unknown parameter of the physical process. Let us suppose that the generating Hamiltonian is linear in the number of probes. (For example, in the case of two-mode interferometry discussed later in the appendix, we suppose that the generator of phase evolution is the photon-number difference between the two modes $\hat{a}^\dagger\hat{a} - \hat{b}^\dagger\hat{b}$.) When N classical probes (probes with no quantum effects) are used, the precision is limited by a scaling given by $1/\sqrt{N}$; known as the shot noise limit. This scaling arises from the central limit theorem of statistics. On the other hand, probes with quantum entanglement can reach below the shot noise limit and determine the unknown parameter with a precision that can scale as $1/N$; known as the Heisenberg limit [93].

C.2 Quantum Optical Interferometry

Optical metrology uses light interferometry as a tool to perform precision measurements. The most basic optical interferometer is a two-mode device with an unknown relative phase

[1]This appendix is reproduced by updating and adapting the contents of J.P. Dowling and K.P. Seshadreesan, Journal of Lightwave Technology, 33(12):2359-2370, June 2015, with the permission of IEEE. See Appendix E for the copyright permission from the publishers.

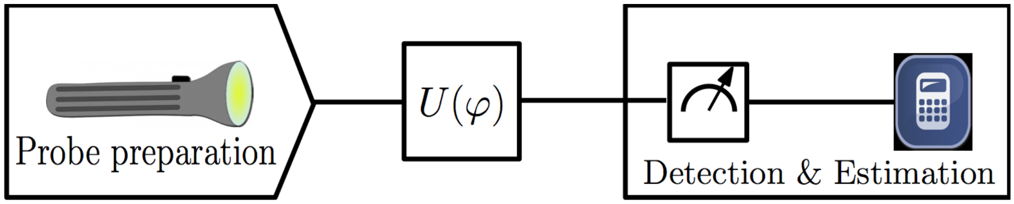

Figure C.1: A schematic of a typical quantum parameter estimation setup. Probes prepared in suitable quantum states are made to evolve through a unitary process $U(\varphi)$, which is an optical interferometer in our case. The process imparts information about the unknown parameter of interest on to the probes. The probes are then detected at the output, and the measurement outcomes used to estimate the unknown value of the parameter.

(between the two modes). This unknown phase can be engineered to carry information about different quantities of interest in different contexts, e.g., it is related to the strength of a magnetic field in an optical magnetometer, a gravitational wave at LIGO (light interferometer gravitational wave observation), etc.

Fig. C.2 shows a conventional optical interferometer in the Mach Zehnder configuration. The input to the classical interferometer is a coherent laser source, and the detection is based on intensity difference measurement. When a coherent light of average photon number $\overline{n}$ is used, the precision of phase estimation is limited by the shot noise of $1/\sqrt{\overline{n}}$ associated with intensity fluctuations at the output, which have their origin in the vacuum fluctuations of the quantized electromagnetic field that enter the device through the unused input port b_0.

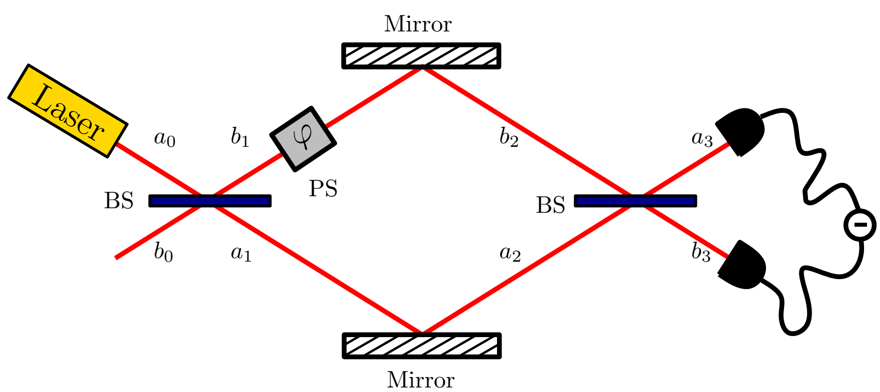

Figure C.2: A schematic of the conventional Mach-Zehnder interferometry based on coherent light input and intensity difference detection. The BS and PS denote beam splitters and phase shifters.

However, quantum optical metrology enables sub-shot noise phase estimation. In a seminal work in the field, Caves [34] showed that when the nonclassical squeezed vacuum state is mixed instead of the vacuum state in the unused port of the same interferometer, sub-shot noise precision that scales as $1/\overline{n}^{2/3}$ can be attained. Subsequently, two-mode squeezed states were shown to enable phase estimation at a precision of $1/\overline{n}$ [21]. With the advancement in single-photon technology, finite photon-number states containing quantum entanglement were also proposed and studied in quantum optical metrology. This includes the $N00N$

states [51], which are Schrdinger cat-like, maximally mode-entangled states of two modes, where the N photons are in superposition of all N photons being in one mode or the other; the Holland-Burnett states [93] and the Berry-Wiseman states [16], to name a few. All these states were found to be capable of attaining the Heisenberg limit $1/N$. The above theoretical results have led to many experimental demonstrations of sub-shot noise metrology with finite photon-number states [193, 202, 3, 86, 133, 23].

Along with the different quantum states of light, a plethora of detection strategies have also been investigated. This includes homodyne and heterodyne detection [204], the canonical phase measurement [139] (which can be mimicked by an adaptive measurement [200]), photon-number counting [155, 107], and photon-number parity measurement [72]. These measurement schemes have been shown to be capable of attaining the optimal precisions of different quantum states of light.

More recently, numerous studies have been devoted to investigating the effects of photon loss, dephasing noise and other decoherence phenomena, on the precision of phase estimation in quantum optical metrology. Useful lower bounds on precision, and optimal quantum states that attain those bounds, have been identified in some such scenarios both numerically and analytically [111, 48, 59, 110, 118, 50].

C.3 Tools to Study Quantum Optical Metrology

In this section, we describe the basic tools that get used in quantum optical metrology. (Note that we restrict ourselves to pure states.)

C.3.1 Two-mode interferometry in the Fock basis

In the quantum description of the Mach-Zehnder interferometer (MZI), we associate creation and annihilation operators with each of the two modes. Here, we call them $\hat{a}_i^\dagger$, $\hat{a}_i$ and $\hat{b}_i^\dagger$, $\hat{b}_i$, $i \in \{0, 1, 2\}$, where the different values of i refer to the modes at the input, inside, and output of the interferometer. The two modes of an MZI could be spatial modes or polarization modes.

Consider the propagation of the input quantum states of the two modes through the different linear optical elements present in the MZI. In the so-called Heisenberg picture, the propagation can be viewed as a transformation of the mode operators via a scattering matrix M_i:

$$\begin{bmatrix} \hat{a}_0 \\ \hat{b}_0 \end{bmatrix} = \hat{M}_i^{-1} \begin{bmatrix} \hat{a}_1 \\ \hat{b}_1 \end{bmatrix}. \tag{C.3.1}$$

The scattering matrices corresponding to a 50:50 beam splitter and a phase shifter are given by

$$\hat{M}_{\text{BS}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \tag{C.3.2}$$

$$\hat{M}_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\varphi} \end{bmatrix}, \tag{C.3.3}$$

respectively. (Note that this form for $\hat{M}_{\text{BS}}$ holds for beam splitters that are constructed as a single dielectric layer, in which case the reflected and the transmitted beams gather a relative phase of $\pi/2$.) The two-mode quantum state at the output of a MZI in the Fock basis, can be therefore obtained by replacing the mode operators in the input state in terms of the output mode operators, where the overall scattering matrix is given by: $\hat{M}_{\rm MZI} = \hat{M}_{\rm BS}\hat{M}_{\varphi}\hat{M}_{\rm BS}$ and is found to be:

$$\hat{M}_{\rm MZI} = ie^{-i\frac{\varphi}{2}} \begin{bmatrix} \sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \\ \cos\frac{\varphi}{2} & -\sin\frac{\varphi}{2} \end{bmatrix}. \tag{C.3.4}$$

(Note that the overall scattering matrix has been suitably renormalized.)

C.3.2 Two-mode interferometry in terms of phase space representations

In terms of phase space quasi-probability distributions such as the Wigner distribution function, the propagation through the Mach-Zehnder interferometer can be similarly described by relating the initial complex variables in the Wigner function to their final expressions as:

$$W_{\rm out}(\alpha_1, \beta_1) = W_{\rm in}\left[\alpha_0(\alpha_1, \beta_1), \beta_0(\alpha_1, \beta_1)\right]. \tag{C.3.5}$$

The relation between the complex variables is similarly given in terms of the two-by-two scattering matrices $\hat{M}$:

$$\begin{bmatrix} \alpha_0 \\ \beta_0 \end{bmatrix} = \hat{M}^{-1} \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}, \tag{C.3.6}$$

α_0, β_0, α_1, and β_1 being the complex amplitudes of the field in the modes $\hat{a}_0$, $\hat{b}_0$, $\hat{a}_1$, and $\hat{b}_1$, respectively. The approach based on phase space probability distributions is particularly convenient and powerful when dealing with Gaussian states, namely, states that have a Gaussian Wigner distribution, and Gaussian operations [194]. Examples include the coherent state, the squeezed vacuum state and the thermal state [69]. This is due to the fact that a Gaussian distribution is completely described by its first and second moments, and there exist tools based on the algebra of the symplectic group that can be used to propagate the mean and covariances of Gaussian states of any number of independent photonic modes.

C.3.3 Two-mode interferometry in the Schwinger basis

The Schwinger model presents an alternative way to describe quantum states and their dynamics in a MZI [205]. The model is based on an interesting relationship between the algebra of the mode operators of two independent photonic modes and the algebra of angular momentum.

Consider the following functions of the mode operators of a pair of independent photonic modes, say, the modes inside the MZI of Fig. C.2, $\hat{a}_1$, $\hat{a}_1^\dagger$, $\hat{b}_1$, and $\hat{b}_1^\dagger$:

$$\hat{J}_x = \frac{1}{2}(\hat{a}_1^\dagger\hat{b}_1 + \hat{b}_1^\dagger\hat{a}_1),\ \hat{J}_y = \frac{1}{2i}(\hat{a}_1^\dagger\hat{b}_1 - \hat{b}_1^\dagger\hat{a}_1),\ \hat{J}_z = \frac{1}{2}(\hat{a}_1^\dagger\hat{a}_1 - \hat{b}_1^\dagger\hat{b}_1), \tag{C.3.7}$$

and $\hat{N} = \hat{a}_1^\dagger\hat{a}_1 + \hat{b}_1^\dagger\hat{b}_1$. The operators in $(C.3.7)$ obey the SU(2) algebra of angular momentum operators, namely, $\left[\hat{J}_q, \hat{J}_r\right] = i\hbar\epsilon_{q,r,s}\hat{J}_s$, where ϵ is the antisymmetric tensor and where $q, r, s \in \{x, y, z\}$. Further, $J^2 = \hat{N}/2\left(\hat{N}/2 + 1\right)$ is the Casimir invariant of the group, which commutes with the operators in (C.3.7). (In fact, $\hat{N}$ itself commutes with the operators in (C.3.7).)

In the Schwinger representation, a two-mode N-photon pure state gets uniquely mapped on to a pure state in the spin-$N/2$ subspace of the angular momentum Hilbert space, i.e.,

$$|n_a, n_b\rangle \rightarrow \left| j = \frac{n_a + n_b}{2}, m = \frac{n_a - n_b}{2} \right\rangle, \tag{C.3.8}$$

where $n_a + n_b = N$. The propagation of the state of the quantized single-mode field is realized by a SU(2)-group transformation generated by the angular momentum operators $\hat{J}_x$, $\hat{J}_y$ and $\hat{J}_z$. For example, the beam splitter transformation of (C.3.2) can be written as:

$$\begin{bmatrix} \hat{a}_0 \\ \hat{b}_0 \end{bmatrix} = U_{\mathrm{BS}} \begin{bmatrix} \hat{a}_1 \\ \hat{b}_1 \end{bmatrix} U_{\mathrm{BS}}^{\dagger}, \tag{C.3.9}$$

where $U_{\mathrm{BS}} = \exp(i\,(\pi/2)\,\hat{J}_y)$, and likewise, the transformation due to the phase shifter inside the interferometer can be described as

$$\begin{bmatrix} \hat{a}_2 \\ \hat{b}_2 \end{bmatrix} = U_{\varphi}^{\dagger} \begin{bmatrix} \hat{a}_1 \\ \hat{b}_1 \end{bmatrix} U_{\varphi}. \tag{C.3.10}$$

Using the SU(2) algebra of the angular momentum operators and the Baker-Hausdorff lemma (See [160]), the overall unitary transformation corresponding to the MZI of Fig. C.2 can be expressed as $\hat{U}_{MZI} = \exp(-i\varphi\hat{J}_x)$. Operationally, for any given two-mode state inside the interferometer, the operator $\hat{J}_z$ tracks the photon-number difference between the two modes inside the interferometer (which is $\propto \hat{a}_1^{\dagger}\hat{a}_1 - \hat{b}_1^{\dagger}\hat{b}_1$). Similarly, when the beam-splitter transformation is chosen to be $U_{\mathrm{BS}} = \exp(i\,(\pi/2)\,\hat{J}_y)$, it can be shown using the SU(2) commutation relations that the operators $\hat{J}_y$ and $\hat{J}_x$ track the photon-number differences at the input (which is $\propto \hat{a}_0^{\dagger}\hat{a}_0 - \hat{b}_0^{\dagger}\hat{b}_0$) and the output (which is $\propto \hat{a}_3^{\dagger}\hat{a}_3 - \hat{b}_3^{\dagger}\hat{b}_3$), respectively.

Alternatively, the propagation through the MZI can be viewed as an SO(3) rotation of the abstract angular momentum vector $\mathbf{J} = \left\{\hat{J}_x, \hat{J}_y, \hat{J}_z\right\}$, while the state remains as it is at the input modes $\hat{a}_0$ and $\hat{b}_0$. For example, the MZI transformation on the angular momentum vector can be captured as follows

$$\begin{pmatrix} \hat{J}'_x \\ \hat{J}'_y \\ \hat{J}'_z \end{pmatrix} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \hat{J}_x \\ \hat{J}_y \\ \hat{J}_z \end{pmatrix}, \tag{C.3.11}$$

which can be simplified as

$$\begin{pmatrix} \hat{J}'_x \\ \hat{J}'_y \\ \hat{J}'_z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & \sin\varphi \\ 0 & -\sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} \hat{J}_x \\ \hat{J}_y \\ \hat{J}_z \end{pmatrix}. \tag{C.3.12}$$

C.3.4 Measurement and phase estimation

After propagating the two-mode quantum state through the MZI, we measure the output state (most generally a density operator $\hat{\rho}$) using a suitable Hermitian operator $\hat{O}$ as the measurement observable. For example, the measurement observable corresponding to the intensity difference detection of the conventional MZI described in Fig. C.2 is the photon-number difference operator $\hat{O} = \hat{b}_3^\dagger \hat{b}_3 - \hat{a}_3^\dagger \hat{a}_3$. Another interesting detection scheme that has been found to be optimal for many input states is the photon-number parity operator [166, 165, 6, 72] of one of the two output modes, e.g., the parity operator of mode $\hat{a}_3$ is given by $\hat{\Pi} = (-1)^{\hat{a}_3^\dagger \hat{a}_3}$. The measured signal corresponding to any observable $\hat{O}$ is given by $\langle \hat{O} \rangle = \mathrm{Tr}\{\hat{O}\hat{\rho}\}$. Further, the precision with which the unknown phase φ can be estimated using the chosen detection scheme, to a good approximation, is given using the error propagation formula as [27]

$$\Delta\varphi = \frac{\Delta O}{\left| d\langle \hat{O} \rangle / d\varphi \right|}, \tag{C.3.13}$$

where

$$\Delta O = \sqrt{\langle \hat{O}^2 \rangle - \langle \hat{O} \rangle^2}. \tag{C.3.14}$$

C.3.5 An example

As an example, consider the coherent light interferometer of Fig. C.2. We will use the Fock state representation for this example. The output state is determined using the scattering matrix of (C.3.4) as

$$|\alpha\rangle \otimes |0\rangle \to \left| i\alpha \sin(\varphi/2) e^{-i\varphi/2} \right\rangle \otimes \left| i\alpha \cos(\varphi/2) e^{-i\varphi/2} \right\rangle. \tag{C.3.15}$$

The output signal for the measurement operator $\hat{O} = \hat{b}_3^\dagger \hat{b}_3 - \hat{a}_3^\dagger \hat{a}_3$ corresponding to intensity difference detection is

$$\langle \hat{O} \rangle = |\alpha|^2 (\cos^2(\varphi/2) - \sin^2(\varphi/2)) = |\alpha|^2 \cos\varphi, \tag{C.3.16}$$

which matches the classical result. The second moment $\langle \hat{O}^2 \rangle$ for the output state is $|\alpha|^4 \cos^2\varphi + |\alpha|^2$, with which we can then ascertain the precision of phase estimation possible with the coherent light interferometer and intensity difference measurement to be

$$\Delta\varphi = \frac{\sqrt{|\alpha|^4 \cos^2\varphi + |\alpha|^2 - |\alpha|^4 \cos^2\varphi}}{|\alpha|^2 \sin\varphi} \tag{C.3.17}$$

$$= \frac{1}{|\alpha| |\sin\varphi|} = \frac{1}{\sqrt{\overline{n}} |\sin\varphi|}, \tag{C.3.18}$$

where $\overline{n}$ is the average photon number of the coherent state. Say the unknown phase φ is such that $\varphi - \theta$ is a small real number, where θ is a control phase. Then, the precision is optimal when θ is an odd multiple of $\pi/2$, attaining $\Delta\varphi = 1/\sqrt{\overline{n}}$, which is the quantum shot noise limit. Unlike classical interferometry based on intensity difference detection, it is possible to get rid of the dependence on the actual value of phase by considering the fringe visibility observable [57]. The visibility observable accomplishes this by keeping track of not only the photon-number difference, but also the total photon number observed.

The above fully quantum result about coherent light interferometry being shot noise limited can also be arrived at using a semi-classical treatment. In the latter, light is considered to be classical, but the detection process to be quantum. However, this result cannot be captured by a fully classical treatment as we show below. In the classical picture, the input laser beam to the interferometer of Fig. C.2 is split into two beams of equal intensities by the first 50:50 beam splitter. These beams then gather an unknown relative phase as they pass through the device. They are then recombined on the final beam splitter, and the average intensity difference between the two output beams is measured. A simple classical optics calculation tells us that the intensities at the output ports may be written in terms of the input intensity I_{a_0} and the relative phase φ as

$$I_{a_2} = I_{a_0} \sin^2(\varphi/2), \tag{C.3.19}$$

$$I_{b_2} = I_{a_0} \cos^2(\varphi/2). \tag{C.3.20}$$

This implies the intensity difference between the two output ports is $M(\varphi) \equiv I_{b_3} - I_{a_3} = I_{a_0} \cos\varphi$—sinusoidal fringes that can be observed when the relative phase is varied.

The precision with which one can estimate an unknown relative phase based on the measurement of M, in terms of the phase error, or the minimum detectable phase, $\Delta\varphi$, may be determined to a good approximation using the following linear error-propagation formula:

$$\Delta\varphi = \frac{\Delta M}{|dM/d\varphi|} = \frac{\Delta M}{I_{a_0} \sin\varphi}. \tag{C.3.21}$$

The above equation suggests that at a local value of phase $\varphi = \pi/2$, the precision of phase estimation can be made arbitrarily small by measuring the intensity difference M with infinite precision, and further by making the input intensity I_a arbitrarily large.

However, quantum mechanics rules out the possibility of measuring intensities with infinite precision, i.e., with $\Delta M = 0$. This is because photon detection is intrinsically a quantum phenomenon, where the measured quantity is not a continuously varying intensity signal, but rather the discrete number of quanta of energy, or photons, that are absorbed by the detector. This absorption process is inherently stochastic due to the vacuum fluctuations of the quantized electromagnetic field, and in the case of coherent laser light the photon numbers detected obey a Poisson distribution. Hence, in such a semi-classical treatment of coherent light interferometry, the precision of phase estimation is limited by $\Delta\varphi = 1/\sqrt{\overline{n}}$, $\overline{n}$ being the intensity of the input laser beam, which is consistent with the fully quantum treatment.

C.4 Entanglement and Squeezing

Like in many other quantum information applications, entanglement is thought to be the driving force behind the enhancements possible in quantum metrology over classical approaches. The quantum Fisher information of N independent probes in a separable state, i.e., without quantum entanglement, cannot exceed N. Since this value of the quantum Fisher information corresponds to precision at the shot noise limit based on (2.5.6), thus, separable states cannot beat the shot noise limit. On the other hand, the quantum Fisher information of entangled states can exceed this bound. In fact it has been shown that the Fisher information of a N-particle state being greater than N is a sufficient condition for multipartite entanglement [144, 74]. Entangled states are therefore capable of achieving sub-shot noise precision. However, it is important to note that the presence of entanglement is necessary, but not a sufficient condition for achieving sub-shot noise precisions. In other words, not all entangled states offer a quantum enhancement to precision metrology [99]. When the generator of parameter evolution $\hat{H}$ is linear in the number of probes, according to (2.5.8), the quantum Fisher information of a state containing N probes can at best attain a value of N^2, which corresponds to the Heisenberg limit in the precision of parameter estimation.

In two-mode optical interferometry, e.g., of the type in Fig. C.2, the relevant type of entanglement to consider is entanglement between the two modes past the first beam splitter, namely a_1 and b_1. The most well-known mode entangled states are the $N00N$ states [161, 51], where are defined as

$$|N :: 0\rangle_{a_1,b_1} = \frac{1}{\sqrt{2}}(|N\rangle_{a_1} \otimes |0\rangle_{b_1} + |0\rangle_{a_1} \otimes |N\rangle_{b_1}), \tag{C.4.1}$$

where a_1 and b_1 denote the two modes past the first beam splitter. The $N00N$ state has a quantum Fisher information of N^2 [2] and hence is capable of achieving the Heisenberg limit in phase estimation. It is known that both the photon-number difference operator and the photon-number parity operator are optimal for Heisenberg-limited phase estimation with the $N00N$ states [19, 51]. Another example of finite photon-number states that are known to be capable of Heisenberg-limited precision are the Holland-Burnett states $|N\rangle_{a_0}|N\rangle_{b_0}$, which result in a mode-entangled state inside the interferometer.

In the indefinite photon-number (continuous variable) regime, entanglement is intimately connected to another nonclassical effect—squeezing. The connection between squeezing and entanglement is unveiled when two single-mode squeezed vacuum beams are mixed on a beam splitter of the type described in (C.3.2). The state that results past the beam splitter is given by the two-mode squeezed vacuum state

$$\begin{aligned} |\xi\rangle &= \hat{S}_2(\xi)|0\rangle_{a_1} \otimes |0\rangle_{b_1} \ (\xi = re^{i(\theta+\pi/2)}) \\ &= \frac{1}{\cosh r}\sum_{0}^{\infty}(-1)^n e^{in(\theta+\pi/2)}(\tanh r)^n |n\rangle_a \otimes |n\rangle_b, \end{aligned} \tag{C.4.2}$$

where $\hat{S}_2(\xi) = \exp\left(\xi \hat{a}_1^\dagger \hat{b}_1^\dagger - \xi^* \hat{a}_1 \hat{b}_1\right)$ is the two-mode squeezing operator. This state is mode-entangled as the state of the two modes cannot be written in a separable form. The two-mode squeezing operator can itself also be implemented using a non-degenerate parametric conversion process, where once again a strong pump emitting photons at frequency ω_p interacts with a nonlinear crystal containing a second order nonlinearity, generating pairs of photons at frequencies ω_{a_1} and ω_{b_1}, such that $\omega_{a_1} + \omega_{b_1} = \omega_p$.

[2] The quantum Fisher information (QFI) of a pure state is $4\,(\Delta H)^2$, where H is the generating Hamiltonian. For $H = \hat{n}_{a_1} - \hat{n}_{b_1}$, the QFI of the $N00N$ state evaluates to be N^2.

C.5 Quantum Technologies with Entangled Photons

In this section, we review some recent experiments that have demonstrated the enhanced sensing and imaging capabilities of entangled photons in interferometry with the $N00N$ states. In particular, these experiments focus on the small photon-number regime, which is relevant for sensing and imaging delicate material systems such as biological specimen, single molecules, cold quantum gases and atomic ensembles. We also discuss a recent experiment based on the $N00N$ state for enhanced spatial resolution for applications in quantum lithography.

C.5.1 Quantum metrology and sensing

Several experiments based on the $N00N$ states have demonstrated phase estimation beyond the shot noise limit, and achieving the Heisenberg limit. Here, we briefly mention two experiments, which have used $N00N$ states to measure useful quantities mapped on to the optical phase under realistic conditions of photon loss and other decoherence. The first one is by Crespi et al. [43], where $N = 2$ $N00N$ states were used to measure the concentration of a blood protein in an aqueous buffer solution. The experiment used an opto-fluidic device, which consists of a waveguide interferometer whose one arm passes through a microfluidic channel containing the solution. The concentration-dependent refractive index of the solution causes a relative phase shift between the two arms of the interferometer, which is then detected using coincidence photon-number detection. The $N = 2$ $N00N$ states were generated using Hong-Ou-Mandel interference [69] with entangled photon pairs from a parametric down conversion source. At the output, an array of telecommunication optical fibers were used to collect the photons, which were then detected with coincidence detection using four single-photon avalanche photo-diodes. The photons were detected with a fringe visibility of about 87% in the case where the micro channel had a transmissivity of only about 61% due to photon loss. The experiment achieved a sensitivity below the shot noise limit.

In another experiment, Wolfgramm et al. [201] used $N = 2$ polarization $N00N$ states and Faraday rotation to probe a Rubidium atomic spin ensemble in a non-destructive manner. Atomic spins ensembles find application in optical quantum memory, quantum-enhanced atom interferometry, etc. Such atomic spin ensembles, when interacted with via optical measurements, e.g., to store or readout quantum information in a quantum memory or to produce spin-squeezing in atom interferometry, inherently suffer from scattering induced depolarization noise. Also, there is photon loss due to the scattering of the optical probes off the ensemble. In order to minimize loss, the experiment generated narrowband $N00N$ states of about 90% fidelity and purity, at a frequency detuned four Doppler widths from the nearest Rb-85 resonance containing matter-resonant indistinguishable photons. The photons at the output were detected using condense photon-number detection with a fringe visibility of $> 90\%$. The experiment achieved a sensitivity that was five standard deviations better than the shot noise limit.

C.5.2 Quantum imaging

Another important application of optical phase measurement is that of microscopy and imaging. In biology, the technique of differential interference contrast microscopy is widely used to image biological samples. The depth resolution of the images produced by this technique is related to the signal-to-noise ratio (SNR) of the measurement. In the case of classical laser-light-based imaging, for a given light intensity, this is limited by the shot noise limit in phase precision. While one way to enhance the SNR is to raise the illumination power, this might have undesirable effects on delicate, photosensitive samples such as biological tissues, ice crystals, etc. Quantum metrology, however, can provide an enhancement to the SNR without having to increase the illumination power, and therefore could be of significant help in this scenario. In one of the first works on the use of quantum metrology for phase imaging, Brida et al. [29] showed that entangled photon pairs can provide sub-shot noise imaging of absorbing samples. Later, Taylor et al. [179] showed that squeezed light could be used to achieve sub-shot noise sensitivities in micro-particle tracking, with applications in tracking diffusive biological specimen in realtime.

We describe two recent experiments that have used entangled photons for phase super-sensitive imaging. The first one is by Ono et al. [138], where $N = 2$ $N00N$ states were used in a laser confocal microscope in conjunction with a differential interference contrast microscope (LCM-DIM) to demonstrate quantum-enhanced microscopy. The LCM-DIM works based on polarization interferometry, where the H and V modes are separated using a polarization beam splitter or a Nomarski prism, and made to pass through different spatial parts of the sample. These modes, depending on the local refractive index and the structure of the sample, experience different phase shifts, whose difference is then measured at the output. The experiment used $N = 2$ polarization $N00N$ states generated via Hong-Ou-Mandel interference with about 98% fidelity, and the photons were detected at the output using photon-number parity measurement with a fringe visibility of about 95%. The microscope attained an SNR 1.35-times better than the shot noise limit.

In another experiment, Israel et al. [102] used $N = 2$ and $N = 3$ $N00N$ states in quantum polarization light microscopy (QPLM) to image a quartz crystal. In QPLM, a birefringent sample causes the H and V modes to experience a differential phase shift, which is then measured at the output to image the sample. The $N00N$ states for the experiment were generated from the mixing of coherent light and squeezed vacuum light in equal intensities (discussed later in Section 5.5), and the photons were detected using an array of single photon counting modules. The experiment achieved quantum-enhanced imaging with sensitivities close to the Heisenberg limit.

C.5.3 Quantum lithography

Lithography relies on the creation and detection of spatial interference fringes to etch ultra fine features on a chip. While classical light lithography is limited by the Rayleigh diffraction limit, as mentioned before, the $N00N$ states can beat this limit—a result known as super-resolution [114, 113, 22]. A few independent experiments with $N = 2$ $N00N$ states had earlier demonstrated this result. However, it was realized that the $N00N$ state lithography suffers from the problem that the efficiency of detecting N photons in the same spatial location decreases exponentially in N.

In a new theoretical development, a counter-measure was suggested based on the optical centroid measurement [187], which does not require all the photons to arrive at the same spatial point. The optical centroid measurement is based on an array of detectors that keep track of every N photon detection event irrespective of which detectors fired. Then the average position of the photons is obtained via post-processing. In a recent experiment, using $N = 2,\ 3,\ 4$ $N00N$ states and the optical centroid measurement, Rozema et al. [158] for the first time demonstrated a scalable implementation of quantum super-resolving interferometry with a visibility of interference fringes nearly independent of N.

C.6 Discussion

In this appendix, we presented a brief overview of quantum optical metrology, with an emphasis on quantum technologies that have been demonstrated with entangled photons. We presented some state-of-the-art experiments for technological applications such as quantum-enhanced biosensing, imaging, and spatial resolution lithography.

This review is by no means representative of everything there is to quantum optical metrology. For a comprehensive review of the field, please refer [151, 115]. We did not discuss the approach to quantum metrology via the Bayesian method [90], where the unknown parameter is assumed to be inherently random, and thus distributed according to an unknown probability distribution. Optimal states in this paradigm have also been identified, and adaptive protocols have been designed, which implement the optimal measurements for such states based on measurement settings that continually changed based on the results previously obtained [202, 86, 16, 200]. Also, we did not go into the details of how the effects of photon loss and decoherence such as collective dephasing noise due to the thermal motion of optical components or laser noise, etc, are handled in optical metrology. A large body of work in the recent literature has dealt with identifying useful lower bounds on phase precision in the presence of such decoherence [48, 59]. Further, optimal quantum states of light that attain these bounds in the presence of decoherence have been identified in the asymptotic limit of a large number of photons [111].

It must be mentioned here that the $N00N$ states are highly susceptible to photon loss, or other types of decoherence in the limit of a large photon number N. Nevertheless, the use of the $N00N$ state in the experiments discussed here is justified, since the $N00N$ states still remain optimal for relatively small photon numbers. In fact, in noisy, decoherence-ridden interferometry, given a large finite photon-number constraint, it has been recently shown that the best strategy for phase estimation is to divide the total number of photons into smaller independent packets or "clusters", where each cluster is prepared in a $N00N$ state [111]. These clusters are then to be sent through the interferometer one at a time. (The optimal size of the clusters will depend on the decoherence strength inside the interferometer.) In addition, alternatives to the $N00N$ states, of the form

$$(|M\rangle|N-M\rangle + |N-M\rangle|M\rangle)/2,\ M \leq N \tag{C.6.1}$$

have been proposed for interferometry in the presence of photon loss [105, 98]. Such states, when suitably chosen, offer the same benefits as the $N00N$ states, while being more robust against photon loss than the latter. Both the $N00N$ states and the states of the form in (C.6.1) of a moderate number of photons, have been shown to perform optimally in the presence of collective dephasing noise [156]. Therefore, the states of the form in (C.6.1) may provide a way to perform quantum metrology in the presence of both photon loss and collective dephasing noise in suitable regimes of photon numbers and the decoherence parameters.

Appendix D
Useful Lemmata

D.1 Generalized Lie-Trotter Product Formula

Proposition D.1. *For invertible operators A, B and C, the following equivalence holds*

$$\exp\{A+B-C\}$$
$$= \lim_{N\to\infty}\left[\exp\left\{\frac{B}{2N}\right\}\exp\left\{\frac{-C}{2N}\right\}\exp\left\{\frac{A}{N}\right\}\exp\left\{\frac{-C}{2N}\right\}\exp\left\{\frac{B}{2N}\right\}\right]^N.$$
$$= \lim_{N\to\infty}\left[\exp\left\{\frac{A}{N}\right\}\exp\left\{\frac{B}{N}\right\}\exp\left\{\frac{-C}{N}\right\}\right]^N. \quad \text{(D.1.1)}$$

Proof. We shall prove $(D.1.1)$. The other equality can be proved essentially identically. Let us first compare the following two operators:

$$X_N = \exp\{(A+B-C)/N\}, \quad \text{(D.1.2)}$$
$$Y_N = \exp\left\{\frac{B}{2N}\right\}\exp\left\{\frac{-C}{2N}\right\}\exp\left\{\frac{A}{N}\right\}\exp\left\{\frac{-C}{2N}\right\}\exp\left\{\frac{B}{2N}\right\}. \quad \text{(D.1.3)}$$

Consider the Taylor expansions of X_N and Y_N up to first order in N^{-1}.

$$X_N = I + \frac{A+B-C}{N} + O(N^{-2}), \quad \text{(D.1.4)}$$
$$Y_N = (I + \frac{B}{2N} + O(N^{-2}))(I - \frac{C}{2N} + O(N^{-2}))(I + \frac{A}{N} + O(N^{-2}))$$
$$\times (I - \frac{C}{2N} + O(N^{-2}))(I + \frac{B}{2N} + O(N^{-2})) \quad \text{(D.1.5)}$$
$$= I + \frac{A+B-C}{N} + O(N^{-2}). \quad \text{(D.1.6)}$$

Therefore, clearly, $X_N - Y_N = O(N^{-2})$.

Now, consider $X_N^N - Y_N^N$. For arbitrary matrices X and Y, it can be shown that

$$\left\|X^N - Y^N\right\| \le NM^{N-1}\|X - Y\|, \quad \text{(D.1.7)}$$

where $M = \max(\|X\|, \|Y\|)$. For the case $X = X_N$ and $Y = Y_N$, we have

$$\left\|X_N^N - Y_N^N\right\| \le NM^{N-1}\|X_N - Y_N\|. \quad \text{(D.1.8)}$$

Given that

$$\|X_N\| \le \|\exp\{(A+B-C)/N\}\| \le \exp\{(\|A\|+\|B\|+\|C\|)/N\}, \quad \text{(D.1.9)}$$
$$\|Y_N\| \le \left\|\exp\left\{\frac{B}{2N}\right\}\exp\left\{\frac{-C}{2N}\right\}\exp\left\{\frac{A}{N}\right\}\exp\left\{\frac{-C}{2N}\right\}\exp\left\{\frac{B}{2N}\right\}\right\| \quad \text{(D.1.10)}$$
$$\le \exp\{\|A\|+\|B\|+\|C\|)/N\}, \quad \text{(D.1.11)}$$

we have $M^N \leq \exp\{\|A\| + \|B\| + \|C\|\}$. Therefore,

$$\left\|X_N^N - Y_N^N\right\| \leq N \exp\{\|A\| + \|B\| + \|C\|\} O(N^{-2}) = O(N^{-1}). \tag{D.1.12}$$

That is, in the limit $N \to \infty$, $\left\|X_N^N - Y_N^N\right\| = 0$. The proof for the limit when $\alpha \to +1$ is similar, so that we can conclude the statement of the proposition. ■

Corollary D.2. *For invertible operators σ_{AC},σ_{BC} and σ_C, the following equivalence holds*

$$\exp\{\log \sigma_{AC} + \log \sigma_{BC} - \log \sigma_C\} = \lim_{\alpha \to 1} \left[\sigma_{BC}^{(1-\alpha)/2} \sigma_C^{(\alpha-1)/2} \sigma_{AC}^{1-\alpha} \sigma_C^{(\alpha-1)/2} \sigma_{BC}^{(1-\alpha)/2}\right]^{1/(1-\alpha)}. \tag{D.1.13}$$

D.2 Rényi Quantum Conditional Mutual Information

D.2.1 A Sibson identity for the Rényi quantum conditional mutual information

The Rényi QCMI in Definition B.1 has an explicit form, much like other Rényi information quantities [116, 169, 76, 182]. We prove this in two steps, first by proving the following Sibson identity [172].

Lemma D.3. *The following quantum Sibson identity holds when* $\operatorname{supp}(\rho_{ABC}) \subseteq \operatorname{supp}(\sigma_{BC})$ *and for $\alpha \in (0,1) \cup (1,\infty)$:*

$$\Delta_\alpha(\rho_{ABC}, \rho_{AC}, \rho_C, \sigma_{BC}) = \Delta_\alpha(\rho_{ABC}, \rho_{AC}, \rho_C, \sigma_{BC}^*) + D_\alpha(\sigma_{BC}^* \| \sigma_{BC}), \tag{D.2.1}$$

with the state σ_{BC}^* having the form

$$\sigma_{BC}^* \equiv \frac{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}}{\operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}}. \tag{D.2.2}$$

Proof. The relation for σ_{BC}^* implies that

$$\begin{aligned}
&\left[\sigma_{BC}^* \operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}\right]^\alpha \\
&\qquad = \operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2}\right\}.
\end{aligned} \tag{D.2.3}$$

Then consider that

$$\Delta_\alpha(\rho_{ABC}, \rho_{AC}, \rho_C, \sigma_{BC})$$

$$= \frac{1}{\alpha-1} \log \operatorname{Tr}\left\{\rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2} \sigma_{BC}^{1-\alpha} \rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2}\right\} \tag{D.2.4}$$

$$= \frac{1}{\alpha-1} \log \operatorname{Tr}\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2} \sigma_{BC}^{1-\alpha}\right\} \tag{D.2.5}$$

$$= \frac{1}{\alpha-1} \log \operatorname{Tr}\left\{\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2}\right\} \sigma_{BC}^{1-\alpha}\right\} \tag{D.2.6}$$

$$= \frac{1}{\alpha-1} \log \operatorname{Tr}\left\{[\sigma_{BC}^*]^\alpha \sigma_{BC}^{1-\alpha}\right\} \tag{D.2.7}$$

$$+ \frac{\alpha}{\alpha-1} \log \operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2} \rho_{AC}^{(1-\alpha)/2} \rho_{ABC}^\alpha \rho_{AC}^{(1-\alpha)/2} \rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}. \tag{D.2.8}$$

Now consider expanding the following:

$$\Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\sigma^*_{BC}\right)$$
$$=\frac{1}{\alpha-1}\log\operatorname{Tr}\left\{\rho_C^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_C^{(\alpha-1)/2}\left[\sigma^*_{BC}\right]^{1-\alpha}\right\} \tag{D.2.9}$$
$$=\frac{1}{\alpha-1}\log\operatorname{Tr}\left\{\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_C^{(\alpha-1)/2}\right\}\left[\sigma^*_{BC}\right]^{1-\alpha}\right\} \tag{D.2.10}$$
$$=\frac{1}{\alpha-1}\log\operatorname{Tr}\left\{\left[\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_C^{(\alpha-1)/2}\right\}\right]^{1/\alpha}\right\} \tag{D.2.11}$$
$$+\log\operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\} \tag{D.2.12}$$
$$=\frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}. \tag{D.2.13}$$

Putting everything together, we can conclude the statement of the lemma. ■

Corollary D.4. *The Rényi quantum conditional mutual information has the following explicit form for $\alpha \in (0,1)\cup(1,\infty)$:*

$$I_\alpha\left(A;B|C\right)_\rho=\frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\left(\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2}\right)^{1/\alpha}\right\}. \tag{D.2.14}$$

The infimum in $I_\alpha\left(A;B|C\right)_\rho$ is achieved uniquely by the state in (D.2.2)*, so that it can be replaced by a minimum.*

Proof. This follows from the previous lemma:

$$I_\alpha\left(A;B|C\right)_\rho=\inf_{\sigma_{BC}}\Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\sigma_{BC}\right) \tag{D.2.15}$$
$$=\inf_{\sigma_{BC}}\left[\Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\sigma^*_{BC}\right)+D_\alpha\left(\sigma^*_{BC}\|\sigma_{BC}\right)\right] \tag{D.2.16}$$
$$=\Delta_\alpha\left(\rho_{ABC},\rho_{AC},\rho_C,\sigma^*_{BC}\right) \tag{D.2.17}$$
$$=\frac{\alpha}{\alpha-1}\log\operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_C^{(\alpha-1)/2}\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\rho_C^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}. \tag{D.2.18}$$

That proves the statement of the corollary. ■

Other Sibson identities hold for other variations of the Rényi QCMI (whenever the innermost operator is optimized over and the others are the marginals of ρ_{ABC}). The proof for this is the same as given above.

D.2.2 Convergence of the Rényi quantum conditional mutual information

Before giving a proof of Theorem B.6, we first establish the following lemma, which is a slight extension of [132, Proposition 15].

Lemma D.5. *Let $Z(\alpha) \in \mathcal{B}(\mathcal{H})_{++}$ be an operator-valued function and let $f(\alpha)$ be a function, both continuously differentiable in α for all $\alpha \in (0,\infty)$. Then the derivative $\frac{d}{d\alpha}\operatorname{Tr}\{Z(\alpha)^{f(\alpha)}\}$ exists and is equal to*

$$\frac{d}{d\alpha}\operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)}\right\} = \left(\frac{d}{d\alpha}f(\alpha)\right)\operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)}\log Z(\alpha)\right\} + f(\alpha)\operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)-1}\frac{d}{d\alpha}Z(\alpha)\right\}. \tag{D.2.19}$$

Proof. We proceed as in [135] or [132]. Consider that

$$\begin{aligned}
&Z(\alpha+h)^{f(\alpha+h)} - Z(\alpha)^{f(\alpha)} \\
&= \int_0^1 ds \frac{d}{ds}\left[Z(\alpha+h)^{sf(\alpha+h)} Z(\alpha)^{(1-s)f(\alpha)}\right] &\text{(D.2.20)}\\
&= \int_0^1 ds\ Z(\alpha+h)^{sf(\alpha+h)}\left[\log Z(\alpha+h)^{f(\alpha+h)} - \log Z(\alpha)^{f(\alpha)}\right] Z(\alpha)^{(1-s)f(\alpha)}. &\text{(D.2.21)}
\end{aligned}$$

Taking the trace, we get

$$\begin{aligned}
&\operatorname{Tr}\left\{Z(\alpha+h)^{f(\alpha+h)}\right\} - \operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)}\right\} \\
&\quad = f(\alpha+h)\int_0^1 ds\ \operatorname{Tr}\left\{Z(\alpha)^{(1-s)f(\alpha)} Z(\alpha+h)^{sf(\alpha+h)}\left[\log Z(\alpha+h) - \log Z(\alpha)\right]\right\} \\
&\qquad (f(\alpha+h) - f(\alpha))\int_0^1 ds\ \operatorname{Tr}\left\{Z(\alpha)^{(1-s)f(\alpha)} Z(\alpha+h)^{sf(\alpha+h)}\log Z(\alpha)\right\}. &\text{(D.2.22)}
\end{aligned}$$

Dividing by h and taking the limit as $h \to 0$, we find

$$\begin{aligned}
&\lim_{h\to 0}\frac{1}{h}\left[\operatorname{Tr}\left\{Z(\alpha+h)^{f(\alpha+h)}\right\} - \operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)}\right\}\right] \\
&\quad = f(\alpha)\int_0^1 ds\ \operatorname{Tr}\left\{Z(\alpha)^{(1-s)f(\alpha)} Z(\alpha)^{sf(\alpha)}\lim_{h\to 0}\frac{1}{h}\left[\log Z(\alpha+h) - \log Z(\alpha)\right]\right\} \\
&\qquad + \lim_{h\to 0}\frac{f(\alpha+h) - f(\alpha)}{h}\int_0^1 ds\ \operatorname{Tr}\left\{Z(\alpha)^{(1-s)f(\alpha)} Z(\alpha)^{sf(\alpha)}\log Z(\alpha)\right\}, &\text{(D.2.23)}
\end{aligned}$$

which is equal to

$$f(\alpha)\operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)}\frac{d}{d\alpha}\left[\log Z(\alpha)\right]\right\} + \left(\frac{d}{d\alpha}f(\alpha)\right)\operatorname{Tr}\left\{Z(\alpha)^{f(\alpha)}\log Z(\alpha)\right\}. \tag{D.2.24}$$

Carrying out the same arguments as in [135, Theorem 2.7] or [132, Proposition 15] in order to compute $\frac{d}{d\alpha}[\log Z(\alpha)]$, we recover the formula in the statement of the lemma. ■

We now provide a proof of Theorem B.6. The idea is similar to that in the proof of Theorem B.4. To this end, we again invoke L'Hôpital's rule. We begin by defining

$$G(\alpha) \equiv \rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2}, \tag{D.2.25}$$

which implies that

$$I_\alpha (A;B|C)_\rho = \frac{1}{1-\frac{1}{\alpha}} \log \operatorname{Tr}\left\{ G(\alpha)^{1/\alpha} \right\}. \tag{D.2.26}$$

Applying Lemma D.5 to $G(\alpha)$ and the function $1/\alpha$, we find that

$$\frac{d}{d\alpha}\operatorname{Tr}\left\{G(\alpha)^{1/\alpha}\right\} = -\frac{1}{\alpha^2}\operatorname{Tr}\left\{G(\alpha)^{1/\alpha}\log G(\alpha)\right\} + \frac{1}{\alpha}\operatorname{Tr}\left\{G(\alpha)^{(1-\alpha)/\alpha}\frac{d}{d\alpha}G(\alpha)\right\}. \tag{D.2.27}$$

Also, we have that

$$\begin{aligned}
\frac{d}{d\alpha}G(\alpha) = \frac{d}{d\alpha}&\left[\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2}\right] \\
&= \frac{1}{2}(\log\rho_C)\,\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2} \\
&- \frac{1}{2}\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{(\log\rho_{AC})\,\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2} \\
&+ \rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}(\log\rho_{ABC})\,\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2} \\
&- \frac{1}{2}\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}(\log\rho_{AC})\,\rho_{AC}^{(1-\alpha)/2}\right\}\rho_C^{(\alpha-1)/2} \\
&\qquad + \frac{1}{2}\rho_C^{(\alpha-1)/2}\operatorname{Tr}_A\left\{\rho_{AC}^{(1-\alpha)/2}\rho_{ABC}^{\alpha}\rho_{AC}^{(1-\alpha)/2}\right\}(\log\rho_C)\,\rho_C^{(\alpha-1)/2}.
\end{aligned} \tag{D.2.28}$$

Applying L'Hôpital's rule gives

$$\lim_{\alpha\to1} I_\alpha(A;B|C)_\rho = \lim_{\alpha\to1}\frac{-\operatorname{Tr}\left\{G(\alpha)^{1/\alpha}\log G(\alpha)\right\} + \alpha\operatorname{Tr}\left\{G(\alpha)^{(1-\alpha)/\alpha}\frac{d}{d\alpha}G(\alpha)\right\}}{\operatorname{Tr}\left\{G(\alpha)^{1/\alpha}\right\}}. \tag{D.2.29}$$

Consider that

$$\lim_{\alpha\to1} G(\alpha)^{(1-\alpha)/\alpha} = \left[\rho_C^0\operatorname{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0\right]^0 \tag{D.2.30}$$

$$= \rho_{BC}^0. \tag{D.2.31}$$

Evaluating the limits above one at a time and using that $\operatorname{supp}(\rho_{ABC}) \subseteq \operatorname{supp}(\rho_{AC}) \subseteq \operatorname{supp}(\rho_C)$ (see, e.g., [153, Lemma B.4.1]), we find that

$$\lim_{\alpha\to1}\frac{1}{\operatorname{Tr}\left\{G(\alpha)^{1/\alpha}\right\}} = \frac{1}{\operatorname{Tr}\left\{\rho_C^0\operatorname{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0\right\}} \tag{D.2.32}$$

$$= 1, \tag{D.2.33}$$

$$\lim_{\alpha\to1} -\operatorname{Tr}\left\{G(\alpha)^{1/\alpha}\log G(\alpha)\right\}$$

$$= -\operatorname{Tr}\left\{\left[\rho_C^0\operatorname{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0\right]\log\left[\rho_C^0\operatorname{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0\right]\right\} \tag{D.2.34}$$

$$= -\operatorname{Tr}\left\{\rho_{BC}\log\rho_{BC}\right\} \tag{D.2.35}$$

$$\lim_{\alpha\to 1}\frac{d}{d\alpha}G(\alpha)=\frac{1}{2}(\log\rho_C)\rho_C^0\mathrm{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0-\frac{1}{2}\rho_C^0\mathrm{Tr}_A\left\{(\log\rho_{AC})\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0$$
$$+\rho_C^0\mathrm{Tr}_A\left\{\rho_{AC}^0(\log\rho_{ABC})\rho_{ABC}\rho_{AC}^0\right\}\rho_C^0-\frac{1}{2}\rho_C^0\mathrm{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}(\log\rho_{AC})\rho_{AC}^0\right\}\rho_C^0$$
$$+\frac{1}{2}\rho_C^0\mathrm{Tr}_A\left\{\rho_{AC}^0\rho_{ABC}\rho_{AC}^0\right\}(\log\rho_C)\rho_C^0.\quad\text{(D.2.36)}$$

Putting all of this together, we can see that the limit in (D.2.29) evaluates to

$$\lim_{\alpha\to 1}I_\alpha(A;B|C)_\rho=\Delta(\rho_{ABC},\rho_{AC},\rho_C,\rho_{BC})\quad\text{(D.2.37)}$$
$$=I(A;B|C)_\rho.\quad\text{(D.2.38)}$$

D.2.3 Approaches for proving Conjecture B.25 and proof for a special case

This section gives more details regarding the approach outlined in Section B.6.1 for proving Conjecture B.25. Let $\rho_{ABC}\in\mathcal{S}(\mathcal{H}_{ABC})_{++}$, $\tau_{AC}\in\mathcal{S}(\mathcal{H}_{AC})_{++}$, $\theta_{BC}\in\mathcal{S}(\mathcal{H}_{BC})_{++}$, and $\omega_C\in\mathcal{S}(\mathcal{H}_C)_{++}$. We begin by introducing a variable

$$\gamma=\alpha-1,\quad\text{(D.2.39)}$$

and with

$$Y(\gamma)\equiv\rho_{ABC}^{1+\gamma}\tau_{AC}^{\frac{-\gamma}{2}}\omega_C^{\frac{\gamma}{2}}\theta_{BC}^{-\gamma}\omega_C^{\frac{\gamma}{2}}\tau_{AC}^{\frac{-\gamma}{2}},\quad\text{(D.2.40)}$$

it follows that $\Delta_\alpha(\rho_{ABC},\tau_{AC},\omega_C,\theta_{BC})$ is equal to

$$\frac{1}{\alpha-1}\log\mathrm{Tr}\left\{\rho_{ABC}^{\alpha}\tau_{AC}^{\frac{1-\alpha}{2}}\omega_C^{\frac{\alpha-1}{2}}\theta_{BC}^{1-\alpha}\omega_C^{\frac{\alpha-1}{2}}\tau_{AC}^{\frac{1-\alpha}{2}}\right\}=\frac{1}{\gamma}\log\mathrm{Tr}\left\{Y(\gamma)\right\}.\quad\text{(D.2.41)}$$

Since $d\gamma/d\alpha=1$,

$$\frac{d}{d\alpha}\left[\frac{1}{\alpha-1}\log\mathrm{Tr}\left\{\rho_{ABC}^{\alpha}\tau_{AC}^{\frac{1-\alpha}{2}}\omega_C^{\frac{\alpha-1}{2}}\theta_{BC}^{1-\alpha}\omega_C^{\frac{\alpha-1}{2}}\tau_{AC}^{\frac{1-\alpha}{2}}\right\}\right]=\frac{d}{d\gamma}\left[\frac{1}{\gamma}\log\mathrm{Tr}\left\{Y(\gamma)\right\}\right].\quad\text{(D.2.42)}$$

We can then explicitly compute the derivative:

$$\frac{d}{d\gamma}\left[\frac{1}{\gamma}\log\mathrm{Tr}\left\{Y(\gamma)\right\}\right]=-\frac{1}{\gamma^2}\log\mathrm{Tr}\left\{Y(\gamma)\right\}+\frac{\mathrm{Tr}\left\{\frac{d}{d\gamma}Y(\gamma)\right\}}{\gamma\mathrm{Tr}\left\{Y(\gamma)\right\}}\quad\text{(D.2.43)}$$
$$=\frac{\gamma\mathrm{Tr}\left\{\frac{d}{d\gamma}Y(\gamma)\right\}-\mathrm{Tr}\left\{Y(\gamma)\right\}\log\mathrm{Tr}\left\{Y(\gamma)\right\}}{\gamma^2\mathrm{Tr}\left\{Y(\gamma)\right\}}.\quad\text{(D.2.44)}$$

So

$$\gamma\frac{d}{d\gamma}Y(\gamma)=\log\rho_{ABC}^{\gamma}Y(\gamma)+\rho_{ABC}^{1+\gamma}\left[\log\tau_{AC}^{-\gamma/2}\right]\tau_{AC}^{\frac{-\gamma}{2}}\omega_C^{\frac{\gamma}{2}}\theta_{BC}^{-\gamma}\omega_C^{\frac{\gamma}{2}}\tau_{AC}^{\frac{-\gamma}{2}}$$
$$+\rho_{ABC}^{1+\gamma}\tau_{AC}^{\frac{-\gamma}{2}}\left[\log\omega_C^{\gamma/2}\right]\omega_C^{\frac{\gamma}{2}}\theta_{BC}^{-\gamma}\omega_C^{\frac{\gamma}{2}}\tau_{AC}^{\frac{-\gamma}{2}}+\rho_{ABC}^{1+\gamma}\tau_{AC}^{\frac{-\gamma}{2}}\omega_C^{\frac{\gamma}{2}}\left[\log\theta_{BC}^{-\gamma}\right]\theta_{BC}^{-\gamma}\omega_C^{\frac{\gamma}{2}}\tau_{AC}^{\frac{-\gamma}{2}}$$
$$+\rho_{ABC}^{1+\gamma}\tau_{AC}^{\frac{-\gamma}{2}}\omega_C^{\frac{\gamma}{2}}\theta_{BC}^{-\gamma}\omega_C^{\frac{\gamma}{2}}\left[\log\omega_C^{\gamma/2}\right]\tau_{AC}^{\frac{-\gamma}{2}}+Y(\gamma)\log\tau_{AC}^{-\gamma/2}.\quad\text{(D.2.45)}$$

If it is true that the numerator in (D.2.44) is non-negative for all ρ_{ABC}, then we can conclude the monotonicity in α.

A potential path for proving the conjecture for the sandwiched version is to follow a similar approach developed by Tomamichel *et al.* (see the proof of [132, Theorem 7]). Since we can write

$$\widetilde{\Delta}_\alpha\left(\rho_{ABC}, \tau_{AC}, \omega_C, \theta_{BC}\right) = \max_{\gamma_{ABC}} \widetilde{D}_\alpha\left(\rho, \tau, \omega, \theta, \gamma\right), \tag{D.2.46}$$

where

$$\widetilde{D}_\alpha\left(\rho, \tau, \omega, \theta, \mu\right) \equiv \frac{\alpha}{\alpha-1} \log \operatorname{Tr}\left\{\rho_{ABC}^{1/2} \tau_{AC}^{(1-\alpha)/2\alpha} \omega_C^{(\alpha-1)/2\alpha} \theta_{BC}^{(1-\alpha)/\alpha} \omega_C^{(\alpha-1)/2\alpha} \tau_{AC}^{(1-\alpha)/2\alpha} \rho_{ABC}^{1/2} \mu_{ABC}^{(\alpha-1)/\alpha}\right\}, \tag{D.2.47}$$

it suffices to prove that $\widetilde{D}_\alpha\left(\rho, \tau, \omega, \theta, \mu\right)$ is monotone in α. For this purpose, the idea is similar to the above (i.e., try to show that the derivative of $\widetilde{D}_\alpha\left(\rho, \tau, \omega, \theta, \mu\right)$ with respect to α is non-negative). To this end, now let

$$\gamma = \frac{\alpha-1}{\alpha}, \tag{D.2.48}$$

and with

$$Z\left(\gamma\right) \equiv \rho_{ABC}^{1/2} \tau_{AC}^{\frac{-\gamma}{2}} \omega_C^{\frac{\gamma}{2}} \theta_{BC}^{-\gamma} \omega_C^{\frac{\gamma}{2}} \tau_{AC}^{\frac{-\gamma}{2}} \rho_{ABC}^{1/2} \mu_{ABC}^{\gamma}, \tag{D.2.49}$$

it follows that (D.2.47) is equal to

$$\widetilde{D}_\alpha\left(\rho, \tau, \omega, \theta, \mu\right) = \frac{1}{\gamma} \log \operatorname{Tr}\left\{Z\left(\gamma\right)\right\}. \tag{D.2.50}$$

Then since $d\gamma/d\alpha = 1/\alpha^2$,

$$\frac{d}{d\alpha}\left[\widetilde{D}_\alpha\left(\rho, \tau, \omega, \theta, \mu\right)\right] = \frac{1}{\alpha^2}\frac{d}{d\gamma}\left[\frac{1}{\gamma} \log \operatorname{Tr}\left\{Z\left(\gamma\right)\right\}\right]. \tag{D.2.51}$$

Computing the derivative then results in

$$\frac{d}{d\gamma}\left[\frac{1}{\gamma} \log \operatorname{Tr}\left\{Z\left(\gamma\right)\right\}\right] = -\frac{1}{\gamma^2} \log \operatorname{Tr}\left\{Z\left(\gamma\right)\right\} + \frac{\operatorname{Tr}\left\{\frac{d}{d\gamma} Z\left(\gamma\right)\right\}}{\gamma \operatorname{Tr}\left\{Z\left(\gamma\right)\right\}} \tag{D.2.52}$$

$$= \frac{\gamma \operatorname{Tr}\left\{\frac{d}{d\gamma} Z\left(\gamma\right)\right\} - \operatorname{Tr}\left\{Z\left(\gamma\right)\right\} \log \operatorname{Tr}\left\{Z\left(\gamma\right)\right\}}{\gamma^2 \operatorname{Tr}\left\{Z\left(\gamma\right)\right\}}. \tag{D.2.53}$$

The calculation of the derivative $\gamma \operatorname{Tr}\left\{\frac{d}{d\gamma} Z\left(\gamma\right)\right\}$ is very similar to what we have shown above. So, in order to prove the conjecture, it suffices to prove that the numerator of the last line above is non-negative.

If the above approach is successful, one could take essentially the same approach to prove all of the other conjectured monotonicities detailed in Conjecture B.25.

D.2.4 Conditioning on classical information

Lemma D.6. *Let ρ_{XABC} be a classical-quantum state of the following form:*

$$\rho_{XABC} = \sum_x p_X(x) |x\rangle \langle x|_X \otimes \rho^x_{ABC}. \tag{D.2.54}$$

Then the following identity holds for $\alpha \geq 0$:

$$I_\alpha(A;B|CX)_\rho = \frac{\alpha}{\alpha-1} \log \sum_x p_X(x) \exp^{\left(\frac{\alpha-1}{\alpha}\right) I_\alpha(A;B|C)_{\rho^x}}. \tag{D.2.55}$$

Proof. Recalling the formula in (B.4.11), we have

$$I_\alpha(A;B|CX)_\rho = \frac{\alpha}{\alpha-1} \log \operatorname{Tr}\left\{\left(\operatorname{Tr}_A\left\{\rho_{CX}^{(\alpha-1)/2} \rho_{ACX}^{(1-\alpha)/2} \rho^\alpha_{ABCX} \rho_{ACX}^{(1-\alpha)/2} \rho_{CX}^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\}. \tag{D.2.56}$$

So

$$\begin{aligned}
&\rho_{CX}^{(\alpha-1)/2} \rho_{ACX}^{(1-\alpha)/2} \rho^\alpha_{ABCX} \rho_{ACX}^{(1-\alpha)/2} \rho_{CX}^{(\alpha-1)/2} \\
&\quad = \left[\sum_x p_X(x) \rho^x_C \otimes |x\rangle \langle x|_X\right]^{(\alpha-1)/2} \left[\sum_x p_X(x) \rho^x_{AC} \otimes |x\rangle \langle x|_X\right]^{(1-\alpha)/2} \times \\
&\qquad \left[\sum_x p_X(x) \rho^x_{ABC} \otimes |x\rangle \langle x|_X\right]^{\alpha} \left[\sum_x p_X(x) \rho^x_{AC} \otimes |x\rangle \langle x|_X\right]^{(1-\alpha)/2} \times \\
&\qquad \left[\sum_x p_X(x) \rho^x_C \otimes |x\rangle \langle x|_X\right]^{(\alpha-1)/2}
\end{aligned} \tag{D.2.57}$$

$$= \sum_x p^\alpha_X(x) \left[\rho^x_C\right]^{(\alpha-1)/2} \left[\rho^x_{AC}\right]^{(1-\alpha)/2} \left[\rho^x_{ABC}\right]^\alpha \left[\rho^x_{AC}\right]^{(1-\alpha)/2} \left[\rho^x_C\right]^{(\alpha-1)/2} \otimes |x\rangle \langle x|_X. \tag{D.2.58}$$

From the fact that

$$\begin{aligned}
&\mathrm{Tr}\Big\{\big(\mathrm{Tr}_A\{\sum_x p_X^\alpha(x)\,[\rho_C^x]^{(\alpha-1)/2}\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_{ABC}^x]^\alpha\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_C^x]^{(\alpha-1)/2} \\
&\otimes |x\rangle\langle x|_X\}\big)^{1/\alpha}\Big\} \\
&= \mathrm{Tr}\Big\{\big(\sum_x p_X^\alpha(x)\,\mathrm{Tr}_A\left\{[\rho_C^x]^{(\alpha-1)/2}\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_{ABC}^x]^\alpha\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_C^x]^{(\alpha-1)/2}\right\} \\
&\otimes |x\rangle\langle x|_X\big)^{1/\alpha}\Big\} && \text{(D.2.59)} \\
&= \mathrm{Tr}\Big\{\sum_x p_X(x)\left(\mathrm{Tr}_A\left\{[\rho_C^x]^{(\alpha-1)/2}\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_{ABC}^x]^\alpha\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_C^x]^{(\alpha-1)/2}\right\}\right)^{1/\alpha} \\
&\otimes |x\rangle\langle x|_X\Big\} && \text{(D.2.60)} \\
&= \sum_x p_X(x)\,\mathrm{Tr}\left\{\left(\mathrm{Tr}_A\left\{[\rho_C^x]^{(\alpha-1)/2}\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_{ABC}^x]^\alpha\,[\rho_{AC}^x]^{(1-\alpha)/2}\,[\rho_C^x]^{(\alpha-1)/2}\right\}\right)^{1/\alpha}\right\} \\
& && \text{(D.2.61)} \\
&= \sum_x p_X(x)\exp^{\left(\frac{\alpha-1}{\alpha}\right)I_\alpha(A;B|C)_{\rho^x}}, && \text{(D.2.62)}
\end{aligned}$$

it follows that

$$I_\alpha(A;B|CX)_\rho = \frac{\alpha}{\alpha-1}\log\sum_x p_X(x)\exp^{\left(\frac{\alpha-1}{\alpha}\right)I_\alpha(A;B|C)_{\rho^x}}. \tag{D.2.63}$$

■

D.2.5 Invariance under tensoring with product states

Lemma D.7. *Let* $\rho_{AA_1BB_1EE_1} \equiv \omega_{ABE} \otimes \sigma_{A_1} \otimes \tau_{B_1} \otimes \gamma_{E_1}$. *Then*

$$I_\alpha(AA_1;BB_1|EE_1)_\rho = I_\alpha(A;B|E)_\omega. \tag{D.2.64}$$

Proof. This follows from a direct calculation. Consider that

$$\begin{aligned}
&\mathrm{Tr}_{AA_1}\left\{\rho_{AA_1EE_1}^{(1-\alpha)/2}\rho_{AA_1BB_1EE_1}^{\alpha}\rho_{AA_1EE_1}^{(1-\alpha)/2}\right\} \\
&= \mathrm{Tr}_{AA_1}\left\{(\omega_{AE}\otimes\sigma_{A_1}\otimes\gamma_{E_1})^{(1-\alpha)/2}(\omega_{ABE}\otimes\sigma_{A_1}\otimes\tau_{B_1}\otimes\gamma_{E_1})^{\alpha}(\omega_{AE}\otimes\sigma_{A_1}\otimes\gamma_{E_1})^{(1-\alpha)/2}\right\} \\
& && \text{(D.2.65)}
\end{aligned}$$

$$= \mathrm{Tr}_{AA_1}\Big\{ \left(\omega_{AE}^{(1-\alpha)/2} \otimes \sigma_{A_1}^{(1-\alpha)/2} \otimes \gamma_{E_1}^{(1-\alpha)/2}\right) \left(\omega_{ABE}^{\alpha} \otimes \sigma_{A_1}^{\alpha} \otimes \tau_{B_1}^{\alpha} \otimes \gamma_{E_1}^{\alpha}\right) \left(\omega_{AE}^{(1-\alpha)/2} \otimes \sigma_{A_1}^{(1-\alpha)/2} \otimes \gamma_{E_1}^{(1-\alpha)/2}\right) \Big\} \tag{D.2.66}$$

$$= \mathrm{Tr}_{AA_1} \left\{\omega_{AE}^{(1-\alpha)/2} \left(\omega_{ABE}^{\alpha} \otimes \tau_{B_1}^{\alpha}\right) \omega_{AE}^{(1-\alpha)/2} \otimes \sigma_{A_1} \otimes \gamma_{E_1}\right\} \tag{D.2.67}$$

$$= \mathrm{Tr}_{A} \left\{\omega_{AE}^{(1-\alpha)/2} \omega_{ABE}^{\alpha} \omega_{AE}^{(1-\alpha)/2}\right\} \otimes \tau_{B_1}^{\alpha} \otimes \gamma_{E_1}. \tag{D.2.68}$$

From the fact that

$$\mathrm{Tr}\left\{ \left(\rho_{EE_1}^{(\alpha-1)/2} \mathrm{Tr}_{AA_1}\left\{\rho_{AA_1EE_1}^{(1-\alpha)/2} \rho_{AA_1BB_1EE_1}^{\alpha} \rho_{AA_1EE_1}^{(1-\alpha)/2}\right\} \rho_{EE_1}^{(\alpha-1)/2}\right)^{1/\alpha} \right\}$$

$$= \mathrm{Tr}\Big\{ \Big(\left(\omega_{E}^{(\alpha-1)/2} \otimes \gamma_{E_1}^{(\alpha-1)/2}\right) \left(\mathrm{Tr}_{A} \left\{\omega_{AEE_1}^{(1-\alpha)/2} \omega_{ABEE_1}^{\alpha} \omega_{AEE_1}^{(1-\alpha)/2}\right\} \otimes \gamma_{E_1}\right) \left(\omega_{E}^{(\alpha-1)/2} \otimes \gamma_{E_1}^{(\alpha-1)/2}\right) \otimes \tau_{B_1}^{\alpha} \Big)^{1/\alpha} \Big\} \tag{D.2.69}$$

$$= \mathrm{Tr}\left\{ \left(\omega_{E}^{(\alpha-1)/2} \left(\mathrm{Tr}_{A}\left\{\omega_{AEE_1}^{(1-\alpha)/2} \omega_{ABEE_1}^{\alpha} \omega_{AEE_1}^{(1-\alpha)/2}\right\}\right) \omega_{E}^{(\alpha-1)/2} \otimes \tau_{B_1}^{\alpha} \otimes \gamma_{E_1}^{\alpha}\right)^{1/\alpha} \right\} \tag{D.2.70}$$

$$= \mathrm{Tr}\left\{ \left(\omega_{E}^{(\alpha-1)/2} \mathrm{Tr}_{A}\left\{\omega_{AE}^{(1-\alpha)/2} \omega_{ABE}^{\alpha} \omega_{AE}^{(1-\alpha)/2}\right\} \omega_{E}^{(\alpha-1)/2}\right)^{1/\alpha} \otimes \tau_{B_1} \otimes \gamma_{E_1} \right\} \tag{D.2.71}$$

$$= \mathrm{Tr}\left\{ \left(\omega_{E}^{(\alpha-1)/2} \mathrm{Tr}_{A}\left\{\omega_{AE}^{(1-\alpha)/2} \omega_{ABE}^{\alpha} \omega_{AE}^{(1-\alpha)/2}\right\} \omega_{E}^{(\alpha-1)/2}\right)^{1/\alpha} \right\}, \tag{D.2.72}$$

it follows that

$$I_{\alpha}\left(AA_1; BB_1|EE_1\right)_{\rho} = I_{\alpha}\left(A; B|E\right)_{\omega}. \tag{D.2.73}$$

■

D.3 Rényi Conditional Entropy

Lemma D.8. *Let ρ_{XB} be a classical-quantum state, i.e., such that*

$$\rho_{XB} \equiv \sum_{x} p\left(x\right) |x\rangle \langle x|_{X} \otimes \rho_{B}^{x}, \tag{D.3.1}$$

where $p\left(x\right)$ is a probability distribution and $\{\rho_{B}^{x}\}$ is a set of quantum states. For $\alpha \in [0,1) \cup (1,2]$,

$$H_{\alpha}\left(X|B\right) \geq 0. \tag{D.3.2}$$

Proof. This follows because it is possible to copy classical information, and conditional entropy increases under the loss of a classical copy. Consider the following extension of ρ_{XB}:

$$\rho_{X\hat{X}B} \equiv \sum_{x} p\left(x\right) |x\rangle \langle x|_{X} \otimes |x\rangle \langle x|_{\hat{X}} \otimes \rho_{B}^{x}. \tag{D.3.3}$$

Then we show that $H_\alpha(X|\hat{X}B) = 0$ for all $\alpha \in [0,1) \cup (1,\infty)$. Indeed, consider that

$$\begin{aligned}
& H_\alpha(X|\hat{X}B) \\
&= \frac{1}{1-\alpha} \log \operatorname{Tr}\Bigg\{ \left(\sum_x p(x) |x\rangle\langle x|_X \otimes |x\rangle\langle x|_{\hat{X}} \otimes \rho_B^x \right)^\alpha \\
&\qquad \left[I_X \otimes \left(\sum_{x'} p(x') |x'\rangle\langle x'|_{\hat{X}} \otimes \rho_B^{x'} \right)^{1-\alpha} \right] \Bigg\} \quad \text{(D.3.4)} \\
&= \frac{1}{1-\alpha} \log \operatorname{Tr}\Bigg\{ \sum_x p^\alpha(x) |x\rangle\langle x|_X \otimes |x\rangle\langle x|_{\hat{X}} \otimes (\rho_B^x)^\alpha \\
&\qquad \sum_{x'} p^{1-\alpha}(x') I_X \otimes |x'\rangle\langle x'|_{\hat{X}} \otimes \left(\rho_B^{x'}\right)^{1-\alpha} \Bigg\} \quad \text{(D.3.5)} \\
&= \frac{1}{1-\alpha} \log \operatorname{Tr}\left\{ \sum_x p(x) |x\rangle\langle x|_X \otimes |x\rangle\langle x|_{\hat{X}} \otimes \rho_B^x \right\} \quad \text{(D.3.6)} \\
&= 0. \quad \text{(D.3.7)}
\end{aligned}$$

Then for $\alpha \in [0,1) \cup (1,2]$, the desired inequality is a consequence of quantum data processing [183, Lemma 5]:

$$H_\alpha(X|B) \geq H_\alpha(X|\hat{X}B) = 0. \quad \text{(D.3.8)}$$

■

Appendix E
Reuse and Permissions

http://journals.aps.org/copyrightFAQ.html

As the author of an APS-published article, may I include my article or a portion of my article in my thesis or dissertation?

Yes, the author has the right to use the article or a portion of the article in a thesis or dissertation without requesting permission from APS, provided the bibliographic citation and the APS copyright credit line are given on the appropriate pages.

http://authors.iop.org/atom/help.nsf/LookupJournalSpecific/WebPermissionsFAQ~**

Author's rights after publication by IOP

After the copyright in my article has transferred to IOP, may I still use the article for teaching or in a thesis or dissertation?

Yes - upon transfer of copyright, IOP and/or the copyright owner grants back to authors a number of rights. These include the right to copy the article for teaching purposes, and to include the article in research theses or dissertations. Please include citation details and for online use, a link to the Version of Record. IOP's permission will be required for commercial use of an article published as part of your thesis.

AIP PUBLISHING LLC LICENSE
TERMS AND CONDITIONS

Jun 28, 2015

All payments must be made in full to CCC. For payment instructions, please see information listed at the bottom of this form.

License Number	3657591068995
Order Date	Jun 28, 2015
Publisher	AIP Publishing LLC
Publication	Journal of Mathematical Physics
Article Title	Rényi generalizations of the conditional quantum mutual information
Author	Mario Berta,Kaushik P. Seshadreesan,Mark M. Wilde
Online Publication Date	Feb 23, 2015
Volume number	56
Issue number	2
Type of Use	Thesis/Dissertation
Requestor type	Author (original article)
Format	Electronic
Portion	Excerpt (> 800 words)
Will you be translating?	No
Title of your thesis / dissertation	Renyi quantum conditional mutual information and parity quantum optical metrology
Expected completion date	Aug 2015
Estimated size (number of pages)	231
Total	0.00 USD

Terms and Conditions

AIP Publishing LLC -- Terms and Conditions: Permissions Uses

AIP Publishing LLC ("AIPP"") hereby grants to you the non-exclusive right and license to use and/or distribute the Material according to the use specified in your order, on a one-time basis, for the specified term, with a maximum distribution equal to the number that you have ordered. Any links or other content accompanying the Material are not the subject of this license.

1. You agree to include the following copyright and permission notice with the reproduction of the Material:"Reprinted with permission from [FULL CITATION]. Copyright [PUBLICATION YEAR], AIP Publishing LLC." For an article, the copyright and permission notice must be printed on the first page of the article or book chapter. For photographs, covers, or tables, the copyright and permission notice may appear with the Material, in a footnote, or in the reference list.
2. If you have licensed reuse of a figure, photograph, cover, or table, it is your responsibility to ensure that the material is original to AIPP and does not contain the copyright of another entity, and that the copyright notice of the figure, photograph, cover, or table does not indicate that it was reprinted by AIPP, with permission, from another source. Under no circumstances does AIPP, purport or intend to grant permission to reuse material to which it does not hold copyright.
3. You may not alter or modify the Material in any manner. You may translate the Material into another language only if you have licensed translation rights. You may not use the Material for promotional purposes. AIPP reserves all rights not specifically granted herein.
4. The foregoing license shall not take effect unless and until AIPP or its agent, Copyright Clearance Center, receives the Payment in accordance with Copyright Clearance Center Billing and Payment Terms and Conditions, which are incorporated herein by reference.
5. AIPP or the Copyright Clearance Center may, within two business days of granting this

Copyright Clearance Center RightsLink®

Home | Account Info | Help | Live Chat

IEEE Requesting permission to reuse content from an IEEE publication

Title: Quantum Optical Technologies for Metrology, Sensing, and Imaging
Author: Dowling, J.P.; Seshadreesan, K.P.
Publication: Lightwave Technology, IEEE/OSA Journal of
Publisher: IEEE
Date: June15, 15 2015

Logged in as:
Kaushik Seshadreesan
Account #:
3000849309
LOGOUT

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK | CLOSE WINDOW

Vita

Kaushik is a native of Kalpakkam, Tamilnadu, India. He received his bachelor's and master's degrees from Birla Institute of Technology and Science Pilani in 2009. During his master's, Kaushik spent an year visiting the Institute of Mathematical Sciences at Chennai grooming his interest in quantum information science. He then made the decision to enter graduate school in the Department of Physics and Astronomy at Louisiana State University. Kaushik has since been pursuing research in quantum optics and quantum information theory at the Quantum Science and Technologies Group. He will receive his doctorate in August 2015. Kaushik will start as a postdoctoral researcher at the Max Planck Institute for the Science of Light in Erlangen, Germany, in August 2015.