LIMITS ON SECURE COMMUNICATION OVER QUANTUM NETWORKS VIA EXTENDIBILITY

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Vishal Singh

August 2025

LIMITS ON SECURE COMMUNICATION OVER QUANTUM NETWORKS VIA EXTENDIBILITY

Vishal Singh, Ph.D.

Cornell University 2025

A quantum network promises unconditionally secure transmission of data between its nodes by utilizing its ability to distribute entanglement across distant nodes. However, for most practical purposes, the distribution of entanglement is affected by environmental noise. We study the limits of secure communication between two parties sharing an arbitrary bipartite state or an arbitrary quantum channel under the one-way local operations and classical communication (one-way LOCC) setting, particularly for the non-asymptotic case. We use the ideas of unextendibility of entanglement to quantify the resourcefulness of a bipartite state or a quantum channel for forward-assisted private communication between its bearers, which we use to establish limits on the number of secret bits that can be established between the two parties either exactly, or probabilistically, or approximately. Our results surpass several previously known limits on secure communication under the considered setting. Additionally, several bounds presented in our work are efficiently computable, including the bounds on the one-shot private capacity of a channel, which are the first efficiently computable bounds on these quantities to the best of our knowledge.

BIOGRAPHICAL SKETCH

Vishal Singh was born in the city of Lucknow in India, where he completed his high school education. He obtained an Integrated Master of Science degree from the Department of Physics at Indian Institute of Technology, Roorkee in 2019. He joined a Ph.D. program at Louisiana State University in Spring 2021 and transferred to Cornell University to continue his Ph.D. studies with Prof. Mark M. Wilde in Fall 2022.

ACKNOWLEDGEMENTS

I am immensely thankful to my supervisor, Prof. Mark M. Wilde, for his guidance and support throughout my time as a Ph.D. student. My interactions with him have not only fueled scientific and professional development but also personal development. The motivation and encouragement I received from him were pivotal for navigating through the difficult times of my graduate studies and setting a higher ceiling for myself.

I also thank Prof. Jayadev Acharya and Prof. Peter McMahon for their valuable advice as members of my select committee. Their comments and suggestions helped me look at research from new perspectives.

I am especially thankful to my collaborators, Tharon Holdsworth and Theshani Nuradha, for sharing their insights and bringing our collaborative works to fruition. I am also thankful to Prof. Nilanjana Datta, Dr. Ludovico Lami, and Dr. Bartosz Regula for their comments that significantly improved the quality of the works discussed in this thesis.

Much of this work was funded by the National Science Foundation under Grant No. 2329662 and the School of Electrical and Computer Engineering at Cornell University.

I had the pleasure of sharing the workspace with a fantastic group of Ph.D. students at Cornell. Each of my colleagues, Kaiyuan Ji, Hami Mehrabi, Michele Minervini, Hemant Mishra, Theshani Nuradha, Dhrumil Patel, Aby Philip, Soorya Rethinasamy, and Aidan Sims, demonstrated a unique approach to research, and they have greatly enriched my interest in quantum information theory and mathematics. I carry fond memories and incredible experiences from my short but invaluable time with them.

My time at Louisiana State University was also spent with great friends. I did not feel far from home despite being on the opposite side of the globe thanks to Prerna Agarwal, Pratik Barge, Anshumitra Baul, Akhil Bhardwaj, Stav Haldar, Lauren Hingle, Tharon Holdsworth, Vishal Katariya, Sumeet Khatri, Kunal Sharma, Karunya Shirali, and Sid-

dharth Soni.

My career as a researcher would not have transpired without the inspiring discussions I had with my peers at IIT Roorkee. I am immensely thankful to my friends Aemon, Apoorva, Gargi, Gola, Kalaks, Kedarsh, Lien, Pallod, Sanket, Sid, and Sinha, who have been an absolute joy to share my journey with.

Lastly, I thank my family for their unconditional love and support. I am grateful to my parents for their encouragement and values that I shall carry with me forever, my brother for being a pillar of support and inspiration for personal and professional development, my sister for being the best of friends, and my nieces, Akshita and Avya, whose smiles are the most precious gifts I have received.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Ensuring the secrecy of a message transmitted over a network shared by multiple parties is of utmost importance in the information age. Several public key cryptographic schemes have been developed in the last few decades, facilitating secure communication over large-scale networks. However, the security of the current cryptographic schemes can only be guaranteed in the presence of a computationally restricted eavesdropper. The advancements towards a fault-tolerant quantum computer perhaps pose the most serious threat to information security as they can break the most widely used cryptographic schemes, including RSA [Sho97, MNM+16, ST21]. The lack of unconditional security guarantees of such cryptographic schemes also leaves them susceptible to attacks based on classical algorithms that may be developed in the near future.

Remarkably, several cryptographic schemes have been developed that exploit the laws of quantum mechanics to ensure unconditional security against an eavesdropper that is bound by the laws of quantum mechanics [BB84, Eke91, BBM92] (see [PAB+20] for a review). The theoretical guarantees of these schemes have been a major stimulus for the development of large-scale quantum networks [Kim08, WEH18]. As technology advances to implement quantum cryptographic schemes over a quantum network, the necessity to understand the rate of communication over such networks from an information-theoretic perspective grows ever so relevant.

In this thesis, we present three papers that significantly advance our understanding of the limitations on secure communication, also called private communication, between two parties in a quantum network. Entanglement is the primary resource that facilitates the distribution of an unconditionally secure key over a quantum network, in the sense

argued in [CLL04]. We study the task of establishing a secret key between two parties that either hold one share each of an entangled quantum state, or they have access to a one-way quantum channel. We assume that the parties can perform any quantum operations on the system in their possession, and one party can send an arbitrary amount of public classical data to the other. This setting is commonly called secret-key distillation assisted by one-way local operations and classical communication (one-way LOCC), and it has been a subject of several studies due to its practical significance [DW05, RR12, KKGW21].

The primary tool used in our investigation is the unextendibility of entanglement. Unextendibility has been of fundamental interest in quantum information theory since the seminal works of [Wer89, Wer90]. More recently, it has been studied from a resource-theoretic perspective, which has led to efficiently computable bounds on quantities of interest in quantum Shannon theory, such as the one-shot, forward-assisted quantum capacity of a channel [KDWW19, KDWW21], one-way distillable key of a state [WWW24], and the maximum probability with which a message can be sent over a channel with one-way LOCC assistance [BBFS21, HSW23]. We use the resource theory of unextendibility to study the task of key distillation and private communication in the probabilistic, zero-error, and approximate settings, obtaining several efficiently computable bounds on the relevant quantities of interest in each of these settings.

The contents of the thesis are organized as follows: In Chapter 2, we study the probabilistic distillation of secret keys from a bipartite state using a one-way LOCC channel. We identify a large class of quantum states that are useless for this task, essentially stating a no-go theorem for probabilistic key distillation with one-way LOCC. In Chapter 3, we develop tools to quantify the entanglement of a channel based on the ideas of unextendibility. We then use the thus-defined entanglement measure, dubbed the unextendible entanglement of channels, to obtain efficiently computable upper bounds on the

zero-error, forward-assisted quantum capacity and zero-error, forward-assisted private capacity of a channel. We also obtain efficiently computable upper bounds on the probabilistic one-way distillable key of a state assisted by one-way LOCC and a semicausal bipartite quantum channel. Finally, in Chapter 4, we obtain efficiently computable upper bounds on the one-shot, one-way distillable key of a state and the one-shot, forward-assisted private capacity of a channel using the unextendible entanglement of channels defined in the preceding chapter. These are the first efficiently computable bounds on these quantities to the best of our knowledge. We also find efficiently computable bounds on these quantities for some special cases in the independent and identically distributed (i. i. d.) setting.

BIBLIOGRAPHY

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984. doi:10.1016/j.tcs.2014.05.025.

[BBFS21] Mario Berta, Francesco Borderi, Omar Fawzi, and Volkher B. Scholz. Semidefinite programming hierarchies for constrained bilinear optimization. *Mathematical Programming*, 194(1-2):781–829, April 2021. arXiv:1810.12197, doi:10.1007/s10107-021-01650-1.

[BBM92] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, February 1992. doi:10.1103/PhysRevLett.68.557.

[CLL04] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Physical Review Letters*, 92:217903, May 2004. arXiv:quant-ph/0307151, doi:10.1103/PhysRevLett.92.217903.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, January 2005. doi:10.1098/rspa.2004.1372.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991. doi:10.1103/PhysRevLett.67.661.

[HSW23] Tharon Holdsworth, Vishal Singh, and Mark M. Wilde. Quantifying the performance of approximate teleportation and quantum error correction via symmetric 2-PPT-extendible channels. *Physical Review A*, 107(1):012428, Jan 2023. arXiv:2207.06931, doi:10.1103/PhysRevA.107.012428.

[KDWW19] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. *Physical Review Letters*, 123(7):070502, August 2019. arXiv:2108.03137, doi:10.1103/physrevlett.123.070502.

[KDWW21] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Resource theory of unextendibility and nonasymptotic quantum capacity. *Physical Review A*, 104(2):022401, August 2021. arXiv:1803.10710, doi:10.1103/physreva.104.022401.

[Kim08] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, June 2008. arXiv:0806.4195, doi:10.1038/nature07127.

[KKGW21] Sumeet Khatri, Eneet Kaur, Saikat Guha, and Mark M. Wilde. Second-order coding rates for key distillation in quantum key distribution, 2021. arXiv:1910.03883.

[MNM+16] Thomas Monz, Daniel Nigg, Esteban A. Martinez, Matthias F. Brandl, Philipp Schindler, Richard Rines, Shannon X. Wang, Isaac L. Chuang, and Rainer Blatt. Realization of a scalable Shor algorithm. *Science*, 351(6277):1068–1070, 2016. arXiv:1507.08852, doi:10.1126/science.aad9480.

[PAB+20] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, December 2020. URL: https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012, arXiv:1906.01645, doi:10.1364/AOP.361502.

[RR12] Joseph M. Renes and Renato Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Transactions on Information Theory*, 58(3):1985–1991, 2012. arXiv:1008.0452, doi:10.1109/TIT.2011.2177589.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. arXiv:quant-ph/9508027, doi:10.1137/S0097539795293172.

[ST21] Unathi Skosana and Mark Tame. Demonstration of Shor's factoring algorithm for $N = 21$ on IBM quantum processors. *Scientific Reports*, 11(1):16599, August 2021. arXiv:2103.13855, doi:10.1038/s41598-021-95973-w.

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018. doi:10.1126/science.aam9288.

[Wer89] Reinhard F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17(4):359–363, 1989. doi:10.1007/BF00399761.

[Wer90] Reinhard F. Werner. Remarks on a quantum state extension problem. *Letters in Mathematical Physics*, 19(4):319–326, 1990. doi:10.1007/BF00429951.

[WWW24] Kun Wang, Xin Wang, and Mark M. Wilde. Quantifying the unextendibility of entanglement. *New Journal of Physics*, 26(3):033013, March 2024. arXiv:1911.07433, doi:10.1088/1367-2630/ad264e.

CHAPTER 2

NO-GO THEOREM FOR PROBABILISTIC ONE-WAY SECRET-KEY DISTILLATION[1]

2.1 Abstract

The probabilistic one-way distillable secret key is equal to the largest expected rate at which perfect secret key bits can be probabilistically distilled from a bipartite state by means of local operations and one-way classical communication. Here we define the set of super two-extendible states and prove that an arbitrary state in this set cannot be used for probabilistic one-way secret-key distillation. This broad class of states includes both erased states and all full-rank states. Comparing the probabilistic one-way distillable secret key with the more commonly studied approximate one-way distillable secret key, our results demonstrate an extreme gap between them for many states of interest, with the approximate one-way distillable secret key being much larger. Our findings naturally extend to probabilistic one-way entanglement distillation, with similar conclusions.

2.2 Introduction

Quantum key distribution has emerged as one of the most promising applications of a quantum network, as it facilitates unconditionally secure communication between distant parties [XMZ+20, PR22, ZvLAF+23]. It allows the transmission of private data between multiple parties, such that the security is ensured by the laws of quantum mechan-

[1] V. Singh and M. M. Wilde, "No-go theorem for probabilistic one-way secret-key distillation", arXiv:2404.01392, under review in *Quantum*

ics [BB84, Eke91], instead of relying on computational assumptions about the eavesdropper [KL07]. The rapid development of quantum network technologies demands a strong understanding of our ability to distribute a secret key over a quantum network equipped with some available resources.

Entanglement is a major ingredient that ensures quantum mechanically secure communication [Eke91], and it is in fact necessary as well, in the sense argued in [CLL04]. However, the ability of a quantum state to establish a secret key is not a trivial consequence of its entanglement content. Indeed, the seminal work of [HHHO05, HHHO09] established the existence of bound entangled states [HHH98] that furnish a secret key upon local measurements. This motivates a separate discussion of the privacy content in a quantum state that is clearly distinct from its entanglement content.

The distillation of secret key from a quantum state under a restricted set of operations has garnered interest [DW05, HHHO05, Chr06, CEH+07, HHH+08, HHHO09, CSW12], due to its practical and foundational significance in quantum information science and, particularly, quantum privacy [WTB17, QSW18]. Despite the differences, the theory of entanglement is intimately linked with quantum privacy, and a deeper understanding of one can reveal insights into the other. A specific task of interest is the distillation of secret key under local operations and one-way classical communication, abbreviated as one-way LOCC, due to its physically motivated setting and relation with the private capacity of quantum channels [CWY04, Dev05].

In this paper, we analyze the probabilistic secret-key distillation approach in which a perfect secret key is distilled from an initial bipartite state, albeit probabilistically. In particular, we study the one-way distillable secret key of a bipartite state in the probabilistic setting, which is roughly defined as the maximum achievable expected rate of distilling

secret key bits from an arbitrarily large number of copies of the state using one-way LOCC channels.

The particular contributions of our paper are as follows. We first establish the definition of probabilistic one-way distillable secret key, which is fundamentally different from approximate one-way distillable secret key [DW05]. We find a set of states, called the set of *super two-extendible* states, which have no probabilistic one-way distillable secret key and can also be described via semidefinite constraints. Using the examples of erased states and full-rank states, we show that there exists an extreme gap between the probabilistic one-way distillable secret key and the approximate one-way distillable secret key for several states, with the former being equal to zero while the latter is strictly non-zero for these examples.

Our results establish fundamental limitations on probabilistic secret-key distillation, and consequently on probabilistic entanglement distillation, under one-way LOCC channels. The class of super two-extendible states provides a computationally-friendly framework for analyzing secret-key distillation in a resource-theoretic setting, due to its semidefinite characterization. Furthermore, our results emphasize the importance of allowing some error in secret-key distillation, as doing so can facilitate key distillation from otherwise undistillable states.

One of the main tools that we use to establish our results is the resource theory of unextendibility [KDWW19, KDWW21] and its state-dependent variation [WWW24]. This resource theory was developed in [KDWW19, KDWW21] as a relaxation of the resource theory of entanglement, in which one-way LOCC channels are allowed for free. An important quantity that we employ is the min-unextendible entanglement of a bipartite state [WWW24]. Our work also provides significant improvements on existing

bounds [WWW24, Sec. V.D] regarding the overhead of probabilistic one-way secret key distillation.

2.3 One-way secret-key distillation

Let us begin by considering the task of secret-key distillation. The objective of such a protocol $\mathcal{L}_{AB\to A'B'}$ is to transform a bipartite state ρ_{AB}, purified by ψ_{ABE}, into a tripartite key state as follows:

$$\mathcal{L}_{AB\to A'B'}(\psi_{ABE}) = \frac{1}{k}\sum_{i=0}^{k-1} |i\rangle\langle i|_{A'} \otimes |i\rangle\langle i|_{B'} \otimes \sigma_E, \tag{2.1}$$

where σ_E is an arbitrary quantum state. Alice and Bob, holding systems A' and B' respectively, can use the classically correlated state shared between them to communicate a message of $\log_2 k$ bits using the one-time-pad scheme. Any eavesdropper holding the system E cannot decipher anything about the message because σ_E is independent of the symbol i, hence, ensuring secrecy of the communication.

In [HHHO05, HHHO09], it has been shown that the distillation of a secret key is equivalent to the distillation of a bipartite private state of the following form:

$$\gamma^k_{A_0A_1B_0B_1} \coloneqq \frac{1}{k}\sum_{i,j=0}^{k-1} |ii\rangle\langle jj|_{A_0B_0} \otimes U_i\omega_{A_1B_1}U_j^\dagger, \tag{2.2}$$

where $\omega_{A_1B_1}$ is an arbitrary quantum state and $(U_i)_{i=0}^{k-1}$ is a tuple of unitary operators. The systems A_0B_0 are the key systems, and A_1B_1 are the shield systems. The bipartite private state defined in (2.2) can be used to distill at least $\log_2 k$ secret key bits. We can hence reframe the task of secret key distillation into the distillation of bipartite private states. From here on we simplify the labeling for the key systems and shield systems: when

referring to a private state $\gamma^k_{A_0A_1B_0B_1}$, we group the systems held by Alice into one system label $A \coloneqq A_0A_1$ and all the systems held by Bob into one system label $B \coloneqq B_0B_1$.

In a probabilistic one-way secret-key distillation protocol, Alice and Bob use local operations and one-way classical communication from Alice to Bob to distill a secret key, or equivalently a bipartite private state, from a shared resource state ρ_{AB} with some probability $p \in [0, 1]$. The distillation process can be mathematically described as the action of a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to XA'B'}$ on the resource state ρ_{AB} as follows:

$$\mathcal{L}^{\rightarrow}_{AB\to XA'B'}(\rho_{AB}) = p[1]_X \otimes \gamma^k_{A'B'} + (1-p)[0]_X \otimes \sigma_{A'B'}, \tag{2.3}$$

where we have used the shorthand $[i] \coloneqq |i\rangle\langle i|$. In (2.3), $\gamma^k_{A'B'}$ is a bipartite private state with at least $\log_2 k$ bits of secrecy, system X is a classical flag indicating the success or failure of the protocol, and $\sigma_{A'B'}$ is an arbitrary quantum state generated when the protocol fails to distill a private state.

In any probabilistic secret-key distillation protocol, both parties must have access to the flag X in order to use the distilled key for private communication. Suppose a probabilistic secret-key distillation protocol fails to establish a secret key. In that case, both parties involved in the distillation process can discard their systems and repeat the protocol with another instance of the resource state. If one-way LOCC channels are available for free, it suffices to demand that Alice receives the flag X since she can send the flag to Bob using the freely available forward classical channel.

We can now quantify the resource in a bipartite state that is relevant for the task of secret-key distillation using one-way LOCC channels. For this purpose, we define the probabilistic one-way distillable secret key of a bipartite state as follows:

Definition 2.1 *The probabilistic one-way distillable secret key of a bipartite state ρ_{AB} is the max-*

imum expected rate at which secret key bits can be distilled from a bipartite state using one-way LOCC channels. It is formally defined as

$$K_D^{\rightarrow}(\rho_{AB}) := \liminf_{n\to\infty} \frac{1}{n} K_D^{(1),\rightarrow}(\rho_{AB}^{\otimes n}), \tag{2.4}$$

where the one-shot probabilistic one-way distillable secret key is defined as

$$K_D^{(1),\rightarrow}(\rho_{AB}) := \sup_{\substack{p\in[0,1],k\in\mathbb{N} \\ \mathcal{L}^{\rightarrow}\in 1\text{WL},\gamma^k_{A'B'}}} \left\{ \begin{array}{c} p\log_2 k : \\ \mathcal{L}^{\rightarrow}(\rho_{AB}) = p[1]_{X_A}\otimes\gamma^k_{A'B'} + (1-p)[0]_{X_A}\otimes\frac{I_{A'B'}}{d'_A d'_B} \end{array} \right\}. \tag{2.5}$$

In the above, $\mathcal{L}^{\rightarrow}_{AB\to X_A A'B'}$ is a one-way LOCC channel, 1WL denotes the set of all one-way LOCC channels, the optimization is over every private state $\gamma^k_{A'B'}$ of $\log_2 k$ secret key bits, X_A is a classical flag held by Alice, and $I_{A'B'}$ is the identity operator.

In (2.5) we require that the state generated upon failure of the protocol is a maximally mixed state. This additional constraint on secret-key distillation protocols does not affect the maximum expected number of secret key bits that can be distilled from a bipartite state using one-way LOCC channels as we show in Appendix 2.A.

It is worthwhile to note that a maximally entangled state of Schmidt rank k is a private state holding $\log_2 k$ secret key bits [HHHO05, HHHO09]. As such, any entanglement distillation protocol can be transformed into a secret-key distillation protocol without affecting the rate of distillation. Hence, the one-way distillable secret key of a quantum state is not less than the one-way distillable entanglement of the state in both the probabilistic and approximate settings.

A simpler way to analyze the probabilistic distillation of secret keys under the action of one-way LOCC channels is by considering the erasure symbol. The erasure symbol $[e]$ is defined to be orthogonal to every state in the span of $\{|i\rangle\langle j|\}_{i,j=0}^{d-1}$, where d is the dimension of the underlying system. For practical purposes, one can think of the erasure symbol as

a pure state in the $(d+1)$-dimensional Hilbert space that is orthogonal to every state in the d-dimensional Hilbert space which represents the system of interest. In the case of a joint system S which comprises multiple subsystems, say, $S_1, S_2, \ldots, S_k$, the erasure symbol $[e]_S$ can be represented as follows:

$$[e]_S = [e]_{S_1} \otimes [e]_{S_2} \otimes \cdots \otimes [e]_{S_k}, \tag{2.6}$$

which is orthogonal to every state on the system S, and hence, it is consistent with the definition of the erasure symbol.

In a one-way secret-key distillation protocol, if Alice finds the flag X_A in the state $[0]_{X_A}$, she can erase her state, and she can instruct Bob to erase his state as well. We call the resulting state the doubly erased private state, which has the following form:

$$\eta_{AB}^{p,k} := p\, \gamma_{AB}^{k} + (1-p)[e]_A \otimes [e]_B, \tag{2.7}$$

where Both Alice and Bob can retrieve the flag by performing the POVM $\{\Pi, [e]\}$ on their respective systems, where $\Pi := \sum_{i=0}^{d-1}[i]$. They can further replace their state with a maximally mixed state upon measuring the erasure symbol, hence retrieving the distilled state in (2.5). That is,

$$\eta_{AB}^{p,k} \overset{\text{LO}}{\longleftrightarrow} p[1]_{X_A} \otimes \gamma_{A'B'}^{k} + (1-p)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'}d_{B'}}. \tag{2.8}$$

Since the transformation in (2.8) can be effected by one-way LOCC only, the distillation of the doubly erased private state $\eta_{AB}^{p,k}$ is equivalent to the distillation of $\log_2 k$ secret key bits with probability p.

Min-unextendible entanglement—The min-unextendible entanglement of a bipartite state was defined in [WWW24, Sec. 4.2] as a monotone for the state-dependent resource theory of unextendibility. We briefly mention the relevant properties of this quantity here, and we refer the reader to [WWW24] for a detailed presentation of the resource theory of unextendibility.

The min-unextendible entanglement is defined with respect to the min-relative entropy [Dat09, Def. 2] as follows:

$$E^{u}_{\min}(\rho_{AB}) \coloneqq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} -\frac{1}{2}\log_2 \operatorname{Tr}\left[\Pi^{\rho}_{AB}\sigma_{AB}\right], \tag{2.9}$$

where Π^{ρ}_{AB} is the projection onto the support of ρ_{AB} and the optimization is over all states in the following set:

$$\mathcal{F}(\rho_{AB}) \coloneqq \left\{ \begin{array}{c} \operatorname{Tr}_B[\omega_{ABB'}] : \rho_{AB} = \operatorname{Tr}_{B'}[\omega_{ABB'}], \\ \omega_{ABB'} \in \mathcal{S}(ABB') \end{array} \right\}, \tag{2.10}$$

with $\mathcal{S}(ABB')$ the set of all states of the joint system ABB' and system B' being isomorphic to system B.

The min-unextendible entanglement of a bipartite state has several properties relevant to our discussion. Firstly, it is non-negative, and it is additive with respect to tensor products of states. It is monotonic under the action of two-extendible channels, as defined in [KDWW19, KDWW21], which is a superset of one-way LOCC channels. As such, the min-unextendible entanglement of a bipartite state does not increase under the action of one-way LOCC channels. Lastly, the min-unextendible entanglement of a bipartite private state is not less than the number of secret key bits held by the private state. See Appendix 2.B for more details.

Remark 2.1 *The min-unextendible entanglement of a bipartite state does not increase under one-way LOCC channels. Hence, the transformation in* (2.8) *implies the following equality:*

$$E^{u}_{\min}\left(\eta^{p,k}_{AB}\right) = E^{u}_{\min}\left(p[1]_{X_A}\otimes\gamma^{k}_{AB} + (1-p)[0]_{X_A}\otimes\frac{I_{AB}}{d_A d_B}\right). \tag{2.11}$$

2.4 Limitations on probabilistic one-way distillable secret key

The monotonicity of the min-unextendible entanglement of a bipartite state under the action of one-way LOCC channels implies that the min-unextendible entanglement of the target state in a probabilistic one-way secret-key distillation protocol does not exceed the min-unextendible entanglement of the source state. We first present a lower bound on the min-unextendible entanglement of the doubly erased private state, which is the target state of a probabilistic one-way secret-key distillation protocol.

Lemma 2.1 *For all $p \in [0,1]$ and every integer $k \geq 2$, the min-unextendible entanglement of a doubly erased private state $\eta_{AB}^{p,k}$ is bounded from below by the following quantity:*

$$E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) \geq -\frac{1}{2}\log_2\left(\frac{p}{k^2}+1-p\right). \tag{2.12}$$

Proof: See Appendix 2.C. □

The min-unextendible entanglement of the doubly erased private state $\eta_{AB}^{p,k}$ is strictly positive for all $p \in (0,1]$ and every integer $k \geq 2$, and it is only equal to zero at $p = 0$ because the resulting state is a product state ([WWW24, Proposition 3]). As a consequence of the one-way LOCC monotonicity of the min-unextendible entanglement, a state whose min-unextendible entanglement is equal to zero cannot be used to distill any number of secret key bits with a non-zero probability using one-way LOCC channels. This is formally stated and proved in what follows.

Let us first analyze the set of states whose min-unextendible entanglement is equal to zero. If there exists a state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\rho_{AB} = \sigma_{AB}$, then ρ_{AB} is a two-extendible state [Wer89a, DPS02, DPS04], and its min-unextendible entanglement is equal to zero. A

more general set of states for which the min-unextendible entanglement is equal to zero, which we call super two-extendible states, can be defined as follows:

$$2\text{-EXT}_{\text{sup}}(A:B) := \left\{ \begin{array}{c} \rho_{AB} : \exists \sigma_{AB} \in \mathcal{F}(\rho_{AB}), \\ \text{supp}(\sigma_{AB}) \subseteq \text{supp}(\rho_{AB}) \end{array} \right\}. \tag{2.13}$$

The set of super two-extendible states is convex and open (see Appendix 2.D).

Proposition 2.1 *The min-unextendible entanglement of a quantum state is equal to zero if and only if it is super two-extendible.*

Proof: See Appendix 2.E. □

While the approximate one-way distillable secret key of a two-extendible state, also known as an anti-degradable state [LDS18], is equal to zero [KW24, Thm. 15.43], the same is not true for a general super two-extendible state, as we shall see later in this paper. However, a super two-extendible state cannot be used for probabilistic one-way secret key distillation since its min-unextendible entanglement is equal to zero. Combining this fact with the additive property of the min-unextendible entanglement, we arrive at our main no-go theorem stated as Theorem 2.1, which identifies a broad set of states for which the probabilistic one-way distillable secret key is equal to zero.

Theorem 2.1 *The probabilistic one-way distillable secret key of a super two-extendible state is equal to zero.*

Proof: See Appendix 2.F. □

2.5 Erased private state

Let us consider the following state, which is established if Bob's share of a bipartite private state γ_{AB}^k gets erased with probability $1-p$:

$$\widetilde{\eta}_{AB}^{p,k} := p\, \gamma_{AB}^k + (1-p)\, \mathrm{Tr}_B\left[\gamma_{AB}^k\right] \otimes [e]_B, \tag{2.14}$$

where $\mathrm{Tr}_B[\cdot]$ refers to the partial trace of the argument over system B. We call the state in (2.14) an erased private state.

Proposition 2.2 *For all $p \in [0,1)$ and every integer $k \geq 2$, the erased private state $\widetilde{\eta}_{AB}^{p,k}$ is a super two-extendible state and thus has probabilistic one-way distillable secret key equal to zero.*

Proof: See Appendix 2.G. □

An erased state is defined as follows:

$$\widetilde{\Phi}_{AB}^{p,d} := p\, \Phi_{AB}^d + (1-p)\frac{I_A}{d_A} \otimes [e]_B, \tag{2.15}$$

where Φ_{AB}^d is the maximally entangled state with Schmidt rank equal to d. Since the erased state is a special case of an erased private state, it is in the set of super two-extendible states for all $p \in [0,1)$, which leads to Corollary 2.1 stated below.

Corollary 2.1 *For all $p \in [0,1)$ and every integer $d \geq 2$, the probabilistic one-way distillable secret key of the erased state $\widetilde{\Phi}_{AB}^{p,d}$ is equal to zero.*

The class of full-rank states also is in the set of super two-extendible states, which leads to Corollary 2.2 below.

Corollary 2.2 *All full-rank states are super two-extendible states, and the probabilistic one-way distillable secret key of such quantum states is equal to zero.*

Proof: See Appendix 2.H. □

The inability to probabilistically distill resource from full-rank states has been observed in general quantum resource theories [Ken98, FL20, Reg22b]. Corollary 2.2 extends this result to probabilistic secret-key distillation under one-way LOCC channels. This result also implies that the overhead of probabilistic secret-key distillation considered in [WWW24, Sec. V-B] is infinite for quantum states with full-rank density matrices, thus providing a significant strengthening of the bounds from [WWW24, Sec. V-B].

2.6 Approximate vs. probabilistic secret key distillation

The probabilistic one-way distillable secret key is demonstrably different from the more commonly studied approximate one-way distillable secret key of bipartite states. The approximate one-way distillable secret key is not less than the approximate one-way distillable entanglement of a state, which in turn is bounded from below by the coherent information of the state [DW05, Thm. 10]. For $p > \frac{1}{2}$, the coherent information of an erased state $\widetilde{\Phi}_{AB}^{p,d}$ is strictly non-negative. Similarly, the coherent information of some isotropic [HH99] and Werner states [Wer89b], which are full-rank states, is non-zero (see Appendices 2.I and 2.J). However, Corollaries 2.1 and 2.2 state that the probabilistic one-way distillable secret key of these states is equal to zero, demonstrating an extreme gap between the probabilistic and approximate one-way distillable secret key.

2.7 Conclusion

We found a convex and open set of states, that we call super two-extendible states, from which it is impossible to probabilistically distill secret key bits with any non-zero probability. Our main result is a no-go theorem stating that the probabilistic one-way distillable secret key of a super two-extendible state, and consequently its probabilistic one-way distillable entanglement, is equal to zero.

We demonstrated an extreme gap between the probabilistic and approximate one-way distillable secret key for some states. Considering the intermediate regime between probabilistic and approximate distillation [FL20, Reg22a, EW22], where the goal is to distill high-fidelity maximal-resource states with a non-zero probability, should interpolate between the two extreme cases.

BIBLIOGRAPHY

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[CEH+07] Matthias Christandl, Artur Ekert, Michał Horodecki, Paweł Horodecki, Jonathan Oppenheim, and Renato Renner. Unifying classical and quantum key distillation. In Salil P. Vadhan, editor, *Theory of Cryptography*, pages 456–478, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. arXiv:quant-ph/0608199.

[Chr06] Matthias Christandl. The structure of bipartite quantum states—insights from group theory and cryptography, 2006. arXiv:quant-ph/0604183.

[CLL04] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Physical Review Letters*, 92:217903, May 2004. doi:10.1103/PhysRevLett.92.217903.

[CSW12] Matthias Christandl, Norbert Schuch, and Andreas Winter. Entanglement of the antisymmetric state. *Communications in Mathematical Physics*, 311(2):397–422, 2012. arXiv:0910.4151, doi:10.1007/s00220-012-1446-7.

[CWY04] N. Cai, A. Winter, and R. W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2004. doi:10.1007/s11122-005-0002-x.

[Dat09] Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, 2009. arXiv:0803.2770, doi:10.1109/TIT.2009.2018325.

[Dev05] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005. arXiv:quant-ph/0304127, doi:10.1109/TIT.2004.839515.

[DPS02] A. C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88(18):187904, April 2002. arXiv:quant-ph/0112007, doi:10.1103/PhysRevLett.88.187904.

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69(2):022308, February 2004. arXiv:quant-ph/0308032, doi:10.1103/PhysRevA.69.022308.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A*, 461(2053):207–235, 2005. arXiv:quant-ph/0306078, doi:10.1098/rspa.2004.1372.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991. doi:10.1103/PhysRevLett.67.661.

[EW22] Jens Eisert and Mark M. Wilde. A smallest computable entanglement monotone. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 2439–2444, 2022. arXiv:2201.00835, doi:10.1109/ISIT50566.2022.9834375.

[FL20] Kun Fang and Zi-Wen Liu. No-go theorems for quantum resource purification. *Physcial Review Letters*, 125(6):060405, August 2020. arXiv:1909.02540, doi:10.1103/PhysRevLett.125.060405.

[HH99] Michał Horodecki and Paweł Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59(6):4206–4216, June 1999. arXiv:quant-ph/9708015, doi:10.1103/PhysRevA.59.4206.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 80(24):5239–5242, June 1998. arXiv:quant-ph/9801069, doi:10.1103/PhysRevLett.80.5239.

[HHH+08] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Debbie Leung, and Jonathan Oppenheim. Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity. *IEEE Transactions on Information Theory*, 54(6):2604–2620, 2008. arXiv:quant-ph/0608195, doi:10.1109/TIT.2008.921870.

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*,

94(16):160502, April 2005. arXiv:quant-ph/0309110, doi:10.1103/PhysRevLett.94.160502.

[HHHO09] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009. arXiv:quant-ph/0506189, doi:10.1109/TIT.2008.2009798.

[KDWW19] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. *Physical Review Letters*, 123(7):070502, August 2019. arXiv:2108.03137, doi:10.1103/PhysRevLett.123.070502.

[KDWW21] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Resource theory of unextendibility and nonasymptotic quantum capacity. *Physical Review A*, 104(2):022401, August 2021. arXiv:1803.10710, doi:10.1103/PhysRevA.104.022401.

[Ken98] Adrian Kent. Entangled mixed states and local purification. *Physical Review Letters*, 81(14):2839–2841, October 1998. doi:10.1103/PhysRevLett.81.2839.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. Chapman and Hall/CRC, 2007.

[KW24] Sumeet Khatri and Mark M. Wilde. Principles of quantum communication theory: A modern approach, 2024. arXiv:2011.04672v2.

[LDS18] Felix Leditzky, Nilanjana Datta, and Graeme Smith. Useful states and entanglement distillation. *IEEE Transactions on Information Theory*, 64(7):4689–4708, 2018. arXiv:1701.03081, doi:10.1109/TIT.2017.2776907.

[ON02] T. Ogawa and H. Nagaoka. A new proof of the channel coding theorem via hypothesis testing in quantum information theory. In *Proceedings IEEE International Symposium on Information Theory,*, page 73, 2002. doi:10.1109/ISIT.2002.1023345.

[PR22] Christopher Portmann and Renato Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94:025008, June 2022. doi:10.1103/RevModPhys.94.025008.

[PV10] Yury Polyanskiy and Sergio Verdú. Arimoto channel coding converse and Rényi divergence. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing*, pages 1327–1333. IEEE, 2010. doi:10.1109/ALLERTON.2010.5707067.

[QSW18] Haoyu Qi, Kunal Sharma, and Mark M Wilde. Entanglement-assisted private communication over quantum broadcast channels. *Journal of Physics A: Mathematical and Theoretical*, 51(37):374001, August 2018. arXiv:1803.03976, doi:10.1088/1751-8121/aad5f3.

[Reg22a] Bartosz Regula. Probabilistic transformations of quantum resources. *Physical Review Letters*, 128(11):110505, March 2022. arXiv:2109.04481, doi:10.1103/PhysRevLett.128.110505.

[Reg22b] Bartosz Regula. Tight constraints on probabilistic convertibility of quantum states. *Quantum*, 6:817, September 2022. arXiv:2112.11321, doi:10.22331/q-2022-09-22-817.

[SN96] Benjamin Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Physical Review A*, 54(4):2629–2635, October 1996. arXiv:quant-ph/9604022, doi:10.1103/PhysRevA.54.2629.

[vN27] Johann von Neumann. Thermodynamik quantenmechanischer gesamtheiten. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1927:273–291, 1927. URL: http://eudml.org/doc/59231.

[Wer89a] Reinhard F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17(4):359–363, 1989. doi:10.1007/BF00399761.

[Wer89b] Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, October 1989. doi:10.1103/PhysRevA.40.4277.

[WTB17] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, 2017. arXiv:1602.08898, doi:10.1109/TIT.2017.2648825.

[WWW24] Kun Wang, Xin Wang, and Mark M Wilde. Quantifying the unextendibility

of entanglement. *New Journal of Physics*, 26(3):033013, mar 2024. arXiv:1911.07433v3, doi:10.1088/1367-2630/ad264e.

[XMZ+20] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92:025002, May 2020. doi:10.1103/RevModPhys.92.025002.

[ZvLAF+23] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. Advances in device-independent quantum key distribution. *npj Quantum Information*, 9(1):10, 2023. doi:10.1038/s41534-023-00684-x.

APPENDIX

2.A Equivalent definitions of probabilistic one-way distillable secret key

In this section, we justify the definition of one-shot probabilistic one-way distillable secret key of a bipartite state given in (2.5) by showing an equivalence between (2.5) and a more general definition of the one-shot probabilistic one-way distillable secret key that we propose in (2.A.2).

Consider a general probabilistic one-way secret-key distillation protocol in which a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to X_A A'B'}$ acts on a bipartite state ρ_{AB} to establish the following state:

$$\mathcal{L}^{\rightarrow}(\rho_{AB}) = p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \sigma_{A'B'}, \tag{2.A.1}$$

where $\gamma^k_{A'B'}$ is a bipartite private state holding $\log_2 k$ secret key bits and $\sigma_{A'B'}$ is an arbitrary bipartite state. As such, this protocol can be used to distill an expected number $p \log_2 k$ of secret key bits from a single instance of ρ_{AB}. The one-shot probabilitic one-way distillable secret key of the state ρ_{AB} is defined generally as

$$K_D^{(1),\rightarrow}(\rho_{AB}) \coloneqq \sup_{\substack{p\in[0,1],k\in\mathbb{N} \\ \mathcal{L}^{\rightarrow}\in 1\text{WL},\gamma^k_{A'B'}}} \left\{ \begin{array}{c} p\log_2 k : \\ \mathcal{L}^{\rightarrow}(\rho_{AB}) = p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \sigma_{A'B'}, \\ \sigma_{A'B'} \in \mathcal{S}(A'B') \end{array} \right\}. \tag{2.A.2}$$

In the presence of forward classical communication, Alice can send a copy of the flag X_A to Bob, so that both parties know when the protocol is unsuccessful in establishing the

private state $\gamma^k_{A'B'}$, hence, arriving at the following state:

$$(C_{X_A \to X_A X_B} \circ \mathcal{L}^{\to})(\rho_{AB}) = p[1]_{X_A} \otimes [1]_{X_B} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes [0]_{X_B} \otimes \sigma_{A'B'}, \tag{2.A.3}$$

where $C_{X_A \to X_A X_B}$ is a classical channel that copies the classical data from X_A to X_B. Now that both parties hold a copy of the flag, they can trace out their states and replace them with a locally prepared maximally mixed state if the flag indicates that the protocol was unsuccessful in establishing a private state. That is, Alice applies the following local channel on her system:

$$\mathcal{R}_{X_A A' \to X_A A'}(\cdot) = \frac{I_{A'}}{d_{A'}} \otimes \mathrm{Tr}_{B'}[[0]_{X_B}(\cdot)[0]_{X_B}] + \mathrm{id}_{X_A A' \to X_A A'}([1]_{X_A}(\cdot)[1]_{X_A}), \tag{2.A.4}$$

and Bob applies the corresponding local channel on his systems. Tracing out Bob's flag, we arrive at the following quantum state:

$$(\mathcal{R} \circ C \circ \mathcal{L}^{\to})(\rho_{AB}) = p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \frac{I_{A'}}{d_{A'}} \otimes \frac{I_{B'}}{d_{B'}} \tag{2.A.5}$$

$$= p[1]_{X_A} \otimes \gamma^k_{A'B'} + (1-p)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'} d_{B'}}. \tag{2.A.6}$$

Observe that $\mathcal{R} \circ C \circ \mathcal{L}^{\to}$ is also a one-way LOCC channel that distills an expected number $p \log_2 k$ of secret key bits from a single instance of ρ_{AB}. Since such a one-way LOCC transformation can be designed for every one-way LOCC channel $\mathcal{L}^{\to}_{AB \to X_A A' B'}$, we can conclude the following statement: if there exists a one-way LOCC channel that distills a quantum state of the form given in (2.A.1), then there also exists a one-way LOCC channel that distills the quantum state of the form given in (2.A.6). As the expected number of secret key bits distilled from ρ_{AB} using either of the channels is equal to $p \log_2 k$, we can restrict the optimization in the definition of one-shot probabilistic one-way distillable secret key to channels that establish a quantum state of the form given in (2.A.6). Hence, we arrive at the following equivalent definition of the one-shot probabilistic one-way distillable secret key given in (2.5).

2.B The min-unextendible entanglement of bipartite states

A measure for quantifying the unextendibility of quantum states, called unextendible entanglement, was introduced in [WWW24]. Let us briefly discuss this quantity, which is one of the major components used to prove our main results. Recall that a generalized divergence $\mathbf{D}$ is a function of two quantum states that is non-increasing under the action of a quantum channel [PV10]. The unextendible entanglement of a bipartite state [WWW24] is defined in terms of a generalized divergence as follows:

Definition 2.2 ([WWW24]) *The generalized unextendible entanglement of a bipartite state ρ_{AB}, induced by a generalized divergence $\mathbf{D}$, is defined as*

$$\mathbf{E}^u(\rho_{AB}) := \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2}\mathbf{D}(\rho_{AB}\|\sigma_{AB}), \tag{2.B.1}$$

where $\mathcal{F}(\rho_{AB})$ is defined in (2.10).

We also use the notation $\mathbf{E}^u(\rho_{A:B})$ to clarify the bipartition of systems over which the unextendible entanglement is being considered.

The unextendible entanglement provides a framework to quantify the unextendibility of a bipartite state ρ_{AB} with respect to the system B. Crucially, this quantity is monotonic under the action of two-extendible channels [WWW24, Theorem 2], and hence, it is also monotonic under the action of one-way LOCC channels. (See [KDWW19, KDWW21, WWW24] for the definition of a two-extendible channel.) Stated formally, [WWW24, Theorem 2] establishes the following: for every quantum state ρ_{AB} and two-extendible channel $\mathcal{N}_{AB\to A'B'}$, the following inequality holds:

$$\mathbf{E}^u(\rho_{AB}) \geq \mathbf{E}^u(\mathcal{N}_{AB\to A'B'}(\rho_{AB})). \tag{2.B.2}$$

A different measure for unextendibility was considered in [KDWW19, KDWW21] where the divergence was measured with respect to a fixed set of two-extendible states. However, in Definition 2.2, the divergence is measured by means of a set of states that depend on the input state itself. Although both measures are equal to the minimal possible value of **D** when ρ_{AB} is two-extendible, they are not equal in general.

A particular example of interest and one of the main tools in our paper is the min-unextendible entanglement [WWW24], defined as follows:

$$E^{u}_{\min}(\rho_{AB}) \coloneqq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2} D_{\min}(\rho_{AB}\|\sigma_{AB}), \tag{2.B.3}$$

where $D_{\min}$ is the min-relative entropy [Dat09, Def. 2]:

$$D_{\min}(\omega\|\tau) \coloneqq -\log_2 \mathrm{Tr}[\Pi^{\omega}\tau], \tag{2.B.4}$$

with ω a state, τ a positive semidefinite operator, and Π^{ω} the projection onto the support of ω.

The min-unextendible entanglement has the following properties [WWW24]:

1. **Non-negativity:** The min-unextendible entanglement is non-negative for a bipartite quantum state, as a consequence of the min-relative entropy being non-negative for all pairs of states; that is,

$$E^{u}_{\min}(\rho_{AB}) \geq 0 \quad \forall \rho_{AB} \in \mathcal{S}(AB). \tag{2.B.5}$$

2. **Additivity [WWW24, Prop. 15]:** The min-unextendible entanglement is additive with respect to a tensor product of the states $\rho_{A_1B_1}$ and $\sigma_{A_2B_2}$:

$$E^{u}_{\min}(\rho_{A_1:B_1}\otimes\sigma_{A_2:B_2}) = E^{u}_{\min}(\rho_{A_1:B_1}) + E^{u}_{\min}(\sigma_{A_2:B_2}). \tag{2.B.6}$$

3. **Privacy bound [WWW24, Prop. 21]** The min-unextendible entanglement of a bipartite private state γ_{AB}^k, holding $\log_2 k$ secret key bits, is bounded from below as follows:

$$E_{\min}^u\left(\gamma_{AB}^k\right) \geq \log_2 k. \tag{2.B.7}$$

2.C Proof of Lemma 2.1

Consider the following dephasing channel:

$$\Delta_A(\cdot) \coloneqq \Pi_A\,(\cdot)\,\Pi_A + [e]_A\,(\cdot)\,[e]_A, \tag{2.C.1}$$

where $\Pi_A \coloneqq \sum_{i=0}^{d-1}[i]$, so that $\Pi_A[e] = [e]\Pi_A = 0$. In Lemmas 2.2 and 2.3, we first characterize the action of Δ_A on an arbitrary state $\omega_{AE} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$. We then use Lemmas 2.2 and 2.3 to prove Lemma 2.1.

Lemma 2.2 *Let ω_{AE} be an arbitrary state in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$, where $\eta^{p,k}$ is a doubly erased state, as defined in (2.7). Then $\Delta_A(\omega_{AE})$ is also in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$, where Δ_A is defined in (2.C.1).*

Proof: For every quantum state $\omega_{AE} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$, there exists a state ω_{ABE} with the following marginals;

$$\mathrm{Tr}_E[\omega_{ABE}] = \eta_{AB}^{p,k}, \tag{2.C.2}$$

$$\mathrm{Tr}_B[\omega_{ABE}] = \omega_{AE}. \tag{2.C.3}$$

Note that the doubly erased state $\eta_{AB}^{p,k}$ is invariant under the action of Δ_A. Therefore, the following equalities hold:

$$\Delta_A\left(\eta_{AB}^{p,k}\right) = \Delta_A(\mathrm{Tr}_E[\omega_{ABE}]) \tag{2.C.4}$$

$$= \mathrm{Tr}_E[\Delta_A(\omega_{ABE})] \tag{2.C.5}$$

$$= \eta_{AB}^{p,k}. \tag{2.C.6}$$

This implies that $\Delta(\omega_{ABE})$ is also an extension of $\eta_{AB}^{p,k}$, and consequently, $\mathrm{Tr}_B[\Delta_A(\omega_{ABE})] = \Delta_A(\omega_{AE})$ is in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$. □

Lemma 2.3 *Let ω_{AE} be an arbitrary state in the set $\mathcal{F}\left(\eta_{AB}^{p,k}\right)$, where $\eta^{p,k}$ is a doubly erased state of the following form:*

$$\eta_{AB}^{p,k} = p\,\gamma_{AB}^{k} + (1-p)[e]_A \otimes [e]_B, \tag{2.C.7}$$

with γ_{AB}^{k} a bipartite private state holding $\log_2 k$ secret key bits. Here systems E and B are isomorphic to each other. The action of the dephasing channel Δ_A, defined in (2.C.1), on the state ω_{AE} results in the following state:

$$\Delta_A(\omega_{AE}) = p\,\sigma_{AE} + (1-p)[e]_A \otimes \tau_E, \tag{2.C.8}$$

where $\sigma_{AE} \in \mathcal{F}\left(\gamma_{AB}^{k}\right)$ and $\tau_E \in \mathcal{S}(E)$.

Proof: For every quantum state $\omega_{AE} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$, there exists a state ω_{ABE} with the following marginals;

$$\mathrm{Tr}_E[\omega_{ABE}] = \eta_{AB}^{p,k}, \tag{2.C.9}$$

$$\mathrm{Tr}_B[\omega_{ABE}] = \omega_{AE}. \tag{2.C.10}$$

Recall the definition of the dephasing channel Δ_A from (2.C.1). The state arising from the action of Δ_A on the state ω_{ABE} can be decomposed as follows:

$$\Delta_A(\omega_{ABE}) = X_{ABE} + [e]_A \otimes Y_{BE}, \tag{2.C.11}$$

where $[e]_A X_{ABE} = X_{ABE}[e]_A = 0$. Since $\Delta_A(\omega_{ABE})$ is a quantum state, $\Delta(\omega_{ABE}) \geq 0$, which implies the following operator inequalities:

$$X_{ABE} \geq 0, \tag{2.C.12}$$

$$[e]_A \otimes Y_{BE} \geq 0, \tag{2.C.13}$$

$$\Rightarrow Y_{BE} \geq 0, \tag{2.C.14}$$

where we have used the fact that X_{ABE} and $[e]_A \otimes Y_{BE}$ are orthogonal to each other.

Consider the marginal of $\Delta_A(\omega_{ABE})$ on systems AB, which is equal to the following:

$$\mathrm{Tr}_E[\Delta_A(\omega_{ABE})] = \mathrm{Tr}_E[X_{ABE}] + \mathrm{Tr}_E[Y_{BE}] \otimes [e]_A \tag{2.C.15}$$

We can also evaluate the marginal by first tracing out the system E and then applying the dephasing channel; that is,

$$\mathrm{Tr}_E[\Delta_A(\omega_{ABE})] = \Delta_A\left(\mathrm{Tr}_E[\omega_{ABE}]\right) \tag{2.C.16}$$

$$= p\, \gamma^k_{AB} + (1-p)[e]_A \otimes [e]_B. \tag{2.C.17}$$

Comparing (2.C.15) and (2.C.17), and using the fact that $[e]_A X_{ABE} = 0$, we arrive at the following equalities:

$$\mathrm{Tr}_E[X_{ABE}] = p\, \gamma^k_{AB}, \tag{2.C.18}$$

$$\mathrm{Tr}_E[Y_{BE}] = (1-p)[e]_B. \tag{2.C.19}$$

Recall from (2.C.12) and (2.C.14) that X_{ABE} and Y_{BE} are positive semidefinite operators. Using (2.C.18), we can further conclude that $\frac{X_{ABE}}{p}$ is a quantum state that extends γ^k_{AB}. Similarly, (2.C.19) implies that $\frac{Y_{BE}}{1-p}$ is a quantum state that extends $[e]_B$.

Any quantum state that extends $[e]_B$ is of the form $[e]_B \otimes \tau_E$, where τ_E is an arbitrary quantum state (and which can even be $[e]_E$). Let us define the quantum state $\sigma_{AE} :=$

$\frac{1}{p}\operatorname{Tr}_B[X_{ABE}]$. Since $\frac{1}{p}\operatorname{Tr}_E[X_{ABE}] = \gamma^k_{AB}$, σ_{AE} is in the set $\mathcal{F}\left(\gamma^k_{AB}\right)$. The marginal of the state $\Delta_A(\omega_{ABE})$ on systems AE can now be written as follows:

$$\Delta_A(\omega_{AE}) = p\,\sigma_{AE} + (1-p)[e]_A \otimes \tau_E, \tag{2.C.20}$$

where $\tau_E \in \mathcal{S}(E)$ and $\sigma_{AE} \in \mathcal{F}\left(\gamma^k_{AB}\right)$. □

Proof: [Proof of Lemma 2.1] The min-unextendible entanglement of $\eta^{p,k}_{AB}$ is as follows:

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) = \inf_{\omega_{AB}\in\mathcal{F}\left(\eta^{p,k}\right)} \frac{1}{2} D_{\min}\left(\eta^{p,k}_{AB}\middle\|\omega_{AB}\right), \tag{2.C.21}$$

where $\eta^{p,k}_{AB} = p\,\gamma^k_{AB} + (1-p)[e]_A \otimes [e]_B$ with γ^k_{AB} a bipartite private state holding $\log_2 k$ secret key bits.

Consider an arbitrary state $\omega_{AB} \in \mathcal{F}\left(\eta^{p,k}_{AB}\right)$. The min-relative entropy between $\eta^{p,k}_{AB}$ and ω_{AB} obeys the following inequality:

$$\begin{aligned} D_{\min}\left(\eta^{p,k}_{AB}\middle\|\omega_{AB}\right) &\geq D_{\min}\left(\Delta_A\left(\eta^{p,k}_{AB}\right)\middle\|\Delta_A(\omega_{AB})\right) && (2.C.22)\\ &= D_{\min}\left(\eta^{p,k}_{AB}\middle\|\Delta_A(\omega_{AB})\right), && (2.C.23)\end{aligned}$$

where Δ_A is defined in (2.C.1). The above inequality follows from the data-processing of min-relative entropy and the subsequent equality follows from the invariance of the doubly erased state under the action of the dephasing channel Δ_A. We have shown in Lemma 2.2 that $\Delta_A(\omega_{AB})$ also is in the set $\mathcal{F}\left(\eta^{p,k}_{AB}\right)$. Then the inequality in (2.C.22)–(2.C.23) implies that we can restrict the optimization in (2.C.21) to states ω_{AB} such that $\omega_{AB} = \Delta_A(\omega_{AB})$. Alternatively, we can write the min-unextendible entanglement of the doubly erased state as follows:

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) = \inf_{\omega_{AB}\in\mathcal{F}\left(\eta^{p,k}\right)} \frac{1}{2} D_{\min}\left(\eta^{p,k}_{AB}\middle\|\Delta_A(\omega_{AB})\right). \tag{2.C.24}$$

We have shown in Lemma 2.3 that the action of the channel Δ_A on every state $\omega_{AB} \in \mathcal{F}\left(\eta_{AB}^{p,k}\right)$ results in a state of the following form:

$$\Delta_A(\omega_{AB}) = p\,\sigma_{AB} + (1-p)[e]_A \otimes \tau_B, \tag{2.C.25}$$

where $\tau_B \in \mathcal{S}(B)$, and $\sigma_{AB} \in \mathcal{F}\left(\gamma_{AB}^{k}\right)$. This leads to the following equalities:

$$\begin{aligned} E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) &= \inf_{\omega_{AB}\in\mathcal{F}\left(\eta^{p,k}\right)} \frac{1}{2} D_{\min}\left(\eta_{AB}^{p,k} \middle\| \Delta_A(\omega_{AB})\right) && (2.C.26)\\ &= \inf_{\sigma,\tau} -\frac{1}{2}\log_2 \operatorname{Tr}\left[\Pi^{\eta^{p,k}}\left(p\,\sigma_{AB} + (1-p)[e]_A \otimes \tau_B\right)\right] && (2.C.27)\\ &= -\frac{1}{2}\log_2 \sup_{\sigma,\tau} \operatorname{Tr}\left[\Pi^{\eta^{p,k}}\left(p\,\sigma_{AB} + (1-p)[e]_A \otimes \tau_B\right)\right], && (2.C.28) \end{aligned}$$

where $\Pi^{\eta^{p,k}}$ is the projection onto the support of $\eta_{AB}^{p,k}$. The optimization in the second and third equality is over all $\sigma_{AB} \in \mathcal{F}\left(\gamma_{AB}^{k}\right)$ and $\tau_B \in \mathcal{S}(B)$. The last equality follows from the monotonicity of the logarithm.

Note that γ_{AB}^{k} is orthogonal to $[e]_A \otimes [e]_B$, and $[e]_A \otimes [e]_B$ is a projection. Therefore, we can write the projection onto the support of $\eta_{AB}^{p,k}$ as the following sum:

$$\Pi_{AB}^{\eta^{p,k}} = \Pi_{AB}^{\gamma^{k}} + [e]_A \otimes [e]_B, \tag{2.C.29}$$

where $\Pi_{AB}^{\gamma^{k}}$ is the projection onto the support of the bipartite private state γ_{AB}^{k}. Consequently,

$$\begin{aligned} E_{\min}^{u}\left(\eta_{AB}^{p,k}\right) &= -\frac{1}{2}\log_2 \sup_{\sigma,\tau}\left(p\operatorname{Tr}\left[\Pi_{AB}^{\gamma^{k}}\sigma_{AB}\right] + (1-p)\operatorname{Tr}[([e]_A \otimes [e]_B)([e]_A \otimes \tau_B)]\right) && (2.C.30)\\ &= -\frac{1}{2}\log_2 \sup_{\sigma,\tau}\left(p\operatorname{Tr}\left[\Pi_{AB}^{\gamma^{k}}\sigma_{AB}\right] + (1-p)\operatorname{Tr}[[e]_A \otimes ([e]_E\tau_B)]\right), && (2.C.31) \end{aligned}$$

where the first equality follows from the fact that $([e]_A \otimes I_B)\,\sigma_{AB} = 0$ and $\Pi_{AB}^{\gamma^{k}}([e]_A \otimes \tau_B) = 0$ for every quantum state τ_E.

It is clear that τ_B should be $[e]_B$ in order for the second term inside the logarithm in

(2.C.31) to be non-zero. Therefore,

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) = -\frac{1}{2}\log_2 \sup_{\sigma\in\mathcal{F}\left(\gamma^k_{AB}\right)} \left(p\,\mathrm{Tr}\left[\Pi^{\gamma^k}\sigma_{AB}\right] + 1 - p\right) \tag{2.C.32}$$

$$= -\frac{1}{2}\log_2 \sup_{\sigma\in\mathcal{F}\left(\gamma^k_{AB}\right)} \left(p\, 2^{-D_{\min}\left(\gamma^k_{AB}\middle\|\sigma_{AB}\right)} + 1 - p\right) \tag{2.C.33}$$

$$= -\frac{1}{2}\log_2 \left(p\, 2^{-\inf_{\sigma\in\mathcal{F}\left(\gamma^k_{AB}\right)} D_{\min}\left(\gamma^k_{AB}\middle\|\sigma_{AB}\right)} + 1 - p\right) \tag{2.C.34}$$

$$= -\frac{1}{2}\log_2 \left(p\, 2^{-2E^u_{\min}\left(\gamma^k_{AB}\right)} + 1 - p\right), \tag{2.C.35}$$

where the second equality follows from the definition of min-relative entropy, the third equality follows from the monotonicity of the exponential function, and the last equality follows from the definition of the min-unextendible entanglement of quantum states.

It has been shown in [WWW24, Corollary 22] that the min-unextendible entanglement of a bipartite private state holding $\log_2 k$ bits of secrecy is not less than $\log_2 k$; that is,

$$E^u_{\min}\left(\gamma^k_{AB}\right) \geq \log_2 k. \tag{2.C.36}$$

Therefore,

$$p\, 2^{-2E^u_{\min}\left(\gamma^k\right)} \leq p\, 2^{-2\log_2 k} = \frac{p}{k^2}. \tag{2.C.37}$$

From the monotonicity of the logarithm function,

$$\log_2 \left(p\, 2^{-2E^u_{\min}\left(\gamma^k_{AB}\right)} + 1 - p\right) \leq \log_2 \left(\frac{p}{k^2} + 1 - p\right), \tag{2.C.38}$$

and hence,

$$E^u_{\min}\left(\eta^{p,k}_{AB}\right) \geq -\frac{1}{2}\log_2 \left(\frac{p}{k^2} + 1 - p\right) \quad \forall p \in (0,1), k \geq 2. \tag{2.C.39}$$

When $p = 0$, $\eta^{p,k}_{AB}$ is a separable state, and hence, its min-unextendible entanglement is equal to zero [WWW24, Proposition 3]. When $p = 1$, $\eta^{p,k}_{AB}$ is a bipartite private state holding $\log_2 k$ bits of secrecy, and hence, its min-uenxtendible entanglement is not less than $\log_2 k$ as stated in [WWW24, Corollary 22]. Thus, we conclude the statement of Lemma 2.1. □

2.D Convexity and openness of the set of super two-extendible states

First we show that the set of super two-extendible states is convex. Consider two quantum states ρ_{AB} and τ_{AB} that are in the set of super two-extendible states. Let $\overline{\rho}_{ABE}$ be an extension of ρ_{AB} such that the following containment holds:

$$\operatorname{supp}(\operatorname{Tr}_B[\overline{\rho}_{ABE}]) \subseteq \operatorname{supp}(\rho_{AB}), \tag{2.D.1}$$

where E is isomorphic to B. Note that the existence of such an extension is guaranteed by the fact that ρ_{AB} is in the set of super two-extendible states. Similarly, let $\overline{\tau}_{ABE}$ be an extension of τ_{AB} such that the following containment holds:

$$\operatorname{supp}(\operatorname{Tr}_B[\overline{\tau}_{ABE}]) \subseteq \operatorname{supp}(\tau_{AB}). \tag{2.D.2}$$

Consider an arbitrary convex combination of the states ρ_{AB} and τ_{AB}:

$$\sigma_{AB} \coloneqq p\,\rho_{AB} + (1-p)\tau_{AB}, \tag{2.D.3}$$

where $p \in [0,1]$. The following state is a valid extension of σ_{AB}:

$$\omega_{ABE} \coloneqq p\,\overline{\rho}_{ABE} + (1-p)\overline{\tau}_{ABE}, \tag{2.D.4}$$

because

$$\operatorname{Tr}_E[\omega_{ABE}] = p\,\rho_{AB} + (1-p)\tau_{AB} = \sigma_{AB}. \tag{2.D.5}$$

The other relevant marginal of ω_{ABE} can be expressed as follows:

$$\operatorname{Tr}_B[\omega_{ABE}] = p\operatorname{Tr}_B[\overline{\rho}_{ABE}] + (1-p)\operatorname{Tr}_B[\overline{\tau}_{ABE}]. \tag{2.D.6}$$

Note that σ_{AB} is in the set of super two-extendible states for $p = 0$ and $p = 1$ by the assumption that ρ_{AB} and τ_{AB} are super two-extendible states. For all $p \in (0,1)$, the

following holds:

$$\begin{aligned}
\operatorname{supp}(\operatorname{Tr}_B[\omega_{ABE}]) &= \operatorname{supp}(\operatorname{Tr}_B[\overline{\rho}_{ABE}]) \cup \operatorname{supp}(\operatorname{Tr}_B[\overline{\tau}_{ABE}]) && \text{(2.D.7)}\\
&\subseteq \operatorname{supp}(\operatorname{Tr}_E[\overline{\rho}_{ABE}]) \cup \operatorname{supp}(\operatorname{Tr}_E[\overline{\tau}_{ABE}]) && \text{(2.D.8)}\\
&= \operatorname{supp}(\operatorname{Tr}_E[\omega_{ABE}]) && \text{(2.D.9)}\\
&= \operatorname{supp}(\sigma_{AB})\,, && \text{(2.D.10)}
\end{aligned}$$

where the containment of the sets follows from (2.D.1) and (2.D.2).

Since the support of $\operatorname{Tr}_B[\omega_{ABE}]$ is in the support of $\operatorname{Tr}_E[\omega_{ABE}]$, we conclude that $\operatorname{Tr}_E[\omega_{ABE}] = \sigma_{AB}$ is a super two-extendible state for all $p \in (0,1)$ as well. Therefore, the state σ_{AB}, which is a convex combination of two arbitrary super two-extendible states, is super two-extendible for all $p \in [0,1]$, justifying that the set of super two-extendible states is convex.

To show that the set of super two-extendible states is open, let us consider the example of erased states defined in (2.15). The erased state $\widetilde{\Phi}_{AB}^{p,k}$ is a special case of an erased private state $\widetilde{\eta}_{AB}^{p,k}$. Appendix 2.G establishes that an erased private state is super two-extendible for every $p \in [0,1)$. This implies that an erased state $\widetilde{\Phi}_{AB}^{p,k}$ is also super two-extendible for all $p \in [0,1)$. However, for $p = 1$, $\widetilde{\Phi}_{AB}^{p,k}$ is a maximally entangled state of Schmidt rank k, which is not super two-extendible. In fact, this state has a min-unextendible entanglement of $\log_2 k$. Hence, the set of super two-extendible states is open.

2.E Proof of Proposition 2.1

For every super two-extendible state ρ_{AB}, there exists a quantum state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\operatorname{supp}(\sigma_{AB}) \subseteq \operatorname{supp}(\rho_{AB})$. This implies that $\Pi_{AB}^{\rho}\sigma_{AB} = \sigma_{AB}$, where Π_{AB}^{ρ} is the projection

onto the support of ρ_{AB}. The min-unextendible entanglement of ρ_{AB} can then be bounded as follows:

$$0 \leq E^{u}_{\min}(\rho_{AB}) \tag{2.E.1}$$

$$= \inf_{\tau \in \mathcal{F}(\rho)} -\frac{1}{2} \log_2 \operatorname{Tr}\left[\Pi^{\rho}_{AB} \tau_{AB}\right] \tag{2.E.2}$$

$$\leq -\frac{1}{2} \log_2 \operatorname{Tr}\left[\Pi^{\rho}_{AB} \sigma_{AB}\right] \tag{2.E.3}$$

$$= -\frac{1}{2} \log_2 \operatorname{Tr}[\sigma_{AB}] \tag{2.E.4}$$

$$= 0, \tag{2.E.5}$$

where the first inequality follows from (2.B.5), the first equality follows from the definition of min-unextendible entanglement of a bipartite state, and the last equality follows from the fact that σ_{AB} is a quantum state with unit trace. Therefore, the min-unextendible entanglement of a super two-extendible state is equal to zero.

We now establish the opposite implication. Consider an arbitrary quantum state ρ_{AB} such that $E^{u}_{\min}(\rho_{AB}) = 0$. This is true only if there exists a quantum state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\operatorname{Tr}\left[\Pi^{\rho}_{AB} \sigma_{AB}\right] = 1$, which follows from the definition of the min-unextendible entanglement of a bipartite state. From the gentle measurement lemma [ON02, Lemma 5], it is known for a state τ and a projector P that

$$\frac{1}{2} \|\tau - P\tau P\|_1 \leq \sqrt{1 - \operatorname{Tr}[P\tau]}. \tag{2.E.6}$$

Applying this to our case, we conclude that

$$\left\| \Pi^{\rho}_{AB} \sigma_{AB} \Pi^{\rho}_{AB} - \sigma_{AB} \right\|_1 = 0, \tag{2.E.7}$$

which implies that $\Pi^{\rho}_{AB} \sigma_{AB} \Pi^{\rho}_{AB} = \sigma_{AB}$. This in turns implies that the support of σ_{AB} is in the support of ρ_{AB}. We finally conclude that the min-unextendible entanglement of ρ_{AB} is equal to zero only if there exists a quantum state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$ such that $\operatorname{supp}(\sigma_{AB}) \subseteq \operatorname{supp}(\rho_{AB})$, which is precisely the definition of a super two-extendible state.

2.F Proof of Theorem 2.1

Consider a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{A^nB^n\to X_AA'B'}$ that acts on n copies of a super two-extendible state ρ_{AB} as follows:

$$\mathcal{L}^{\rightarrow}((\rho_{AB})^{\otimes n}) = q[1]_{X_A} \otimes \gamma^{k'}_{A'B'} + (1-q)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'}d_{B'}}, \tag{2.F.1}$$

for some $q \in [0,1]$ and integer $k' \geq 2$. Then

$$\begin{aligned}
0 &\leq E^u_{\min}\left(q[1]_{X_A} \otimes \gamma^{k'}_{A'B'} + (1-q)[0]_{X_A} \otimes \frac{I_{A'B'}}{d_{A'}d_{B'}}\right) && \text{(2.F.2)}\\
&= E^u_{\min}\left(\eta^{q,k'}_{A'B'}\right) && \text{(2.F.3)}\\
&= E^u_{\min}(\mathcal{L}^{\rightarrow}((\rho_{AB})^{\otimes n})) && \text{(2.F.4)}\\
&\leq E^u_{\min}((\rho_{AB})^{\otimes n}) && \text{(2.F.5)}\\
&= nE^u_{\min}(\rho_{AB}) && \text{(2.F.6)}\\
&= 0, && \text{(2.F.7)}
\end{aligned}$$

The first inequality follows from (2.B.5). The first equality follows from Remark 2.1 (the min-unextendible entanglement of the state in (2.F.1) is the same as the min-unextendible entanglement of the doubly erased private state $\eta^{q,k'}_{A'B'}$). The second inequality follows from the monotonicity of min-unextendible entanglement under one-way LOCC channels, the third equality follows from the additivity of min-unextendible entanglement (recall (2.B.6)), and the final equality follows from Proposition 2.1.

Inspecting (2.F.2) and (2.F.7), it follows that $E^u_{\min}\left(\eta^{q,k'}_{A'B'}\right) = 0$. By applying Lemma 2.1, using the fact that $-\frac{1}{2}\log_2\left(\frac{q}{k'^2} + 1 - q\right) \geq 0$ for all $q \in [0,1]$ and integer $k' \geq 2$, and solving the equation $0 = -\frac{1}{2}\log_2\left(\frac{q}{k'^2} + 1 - q\right)$, along with the assumption that $k' \geq 2$, we conclude that $q = 0$. As such, the expected number of secret key bits distilled by the channel $\mathcal{L}^{\rightarrow}_{A^nB^n\to X_AA'B'}$ from n copies of ρ_{AB} is equal to zero. This conclusion holds for every one-way LOCC

channel $\mathcal{L}^{\rightarrow}_{A^nB^n\to X_AA'B'}$, every super two-extendible state ρ_{AB}, and every $n \in \mathbb{N}$. Hence, the one-shot probabilistic one-way distillable secret key of $(\rho_{AB})^{\otimes n}$ is equal to zero for all $n \in \mathbb{N}$, and consequently, the probabilistic one-way distillable entanglement of every super two-extendible state is equal to zero.

2.G Proof of Proposition 2.2

Consider the following extension of an erased private state $\widetilde{\eta}^{p,k}_{AB}$:

$$\omega_{ABE} \coloneqq p\ \gamma^k_{AB} \otimes [e]_E + (1-p)\gamma^k_{AE} \otimes [e]_B, \tag{2.G.1}$$

where E is isomorphic to B. The two relevant marginals of the state ω_{ABE} are

$$\mathrm{Tr}_E[\omega_{ABE}] = p\ \gamma^k_{AB} + (1-p)\gamma^k_A \otimes [e]_B = \widetilde{\eta}^{p,k}_{AB}, \tag{2.G.2}$$

$$\mathrm{Tr}_B[\omega_{ABE}] = (1-p)\gamma^k_{AE} + p\ \gamma^k_A \otimes [e]_E = \widetilde{\eta}^{1-p,k}_{AE}, \tag{2.G.3}$$

where $\gamma^k_A \coloneqq \mathrm{Tr}_B\left[\gamma^k_{AB}\right] = \mathrm{Tr}_E\left[\gamma^k_{AE}\right]$.

Note that the min-relative entropy between two quantum states, ρ and σ, is equal to zero if $\mathrm{supp}(\rho) = \mathrm{supp}(\sigma)$. We know that $\mathrm{supp}(\widetilde{\eta}^{p,k}_{AB}) = \mathrm{supp}(\widetilde{\eta}^{1-p,k}_{AB})$ for all $p \in (0,1)$ and every integer $k \geq 2$. Therefore, we arrive at the following relations:

$$E^u_{\min}\left(\widetilde{\eta}^{p,k}_{AB}\right) \leq \frac{1}{2} D_{\min}\left(\widetilde{\eta}^{p,k}_{AB} \middle\| \widetilde{\eta}^{1-p,k}_{AB}\right) = 0 \quad \forall p \in (0,1), k \geq 2. \tag{2.G.4}$$

The min-unextendible entanglement of a bipartite state is a non-negative quantity since the underlying divergence is non-negative. Therefore,

$$E^u_{\min}\left(\widetilde{\eta}^{p,k}_{AB}\right) = 0 \quad \forall p \in (0,1), k \geq 2. \tag{2.G.5}$$

Finally, the erased private state $\widetilde{\eta}_{AB}^{p,k}$ is a separable state for $p = 0$, and the min-unextendible entanglement of a separable state is equal to zero [WWW24, Proposition 3]. Thus, we conclude the statement of Proposition 2.2.

2.H Proof of Corollary 2.2

Consider a bipartite quantum state that has a full-rank density operator ρ_{AB}. The quantum state $\rho_{AB} \otimes \frac{I_E}{d_E}$ is a valid extension of the state, and its marginal $\frac{1}{d_E} \operatorname{Tr}_B[\rho_{AB} \otimes I_E]$ is in the set $\mathcal{F}(\rho_{AB})$ when $E \cong B$. The min-unextendible entanglement of the state ρ_{AB} obeys the following inequality by definition:

$$E_{\min}^{u}(\rho_{AB}) \leq \frac{1}{2} D_{\min}\left(\rho_{AB} \middle\| \frac{1}{d_E} \operatorname{Tr}_B[\rho_{AB} \otimes I_E]\right) \tag{2.H.1}$$

$$= \frac{1}{2} D_{\min}\left(\rho_{AB} \middle\| \rho_A \otimes \frac{I_E}{d_E}\right) \tag{2.H.2}$$

$$= -\frac{1}{2} \log_2\left(\operatorname{Tr}\left[\Pi_{AB}^{\rho}\left(\rho_A \otimes \frac{I_E}{d_E}\right)\right]\right), \tag{2.H.3}$$

where Π_{AB}^{ρ} is the projection onto the support of ρ_{AB}, and $\rho_A := \operatorname{Tr}_B[\rho_{AB}]$. Since ρ_{AB} is a full-rank density operator, the projection onto the support of ρ_{AB} is the identity operator; that is,

$$\Pi_{AB}^{\rho} = I_{AB}. \tag{2.H.4}$$

Therefore,

$$0 \leq E_{\min}^{u}(\rho_{AB}) \tag{2.H.5}$$

$$\leq -\frac{1}{2} \log_2\left(\frac{1}{d_E} \operatorname{Tr}[I_{AB}\,(\rho_A \otimes I_E)]\right) \tag{2.H.6}$$

$$= -\frac{1}{2} \log_2(\operatorname{Tr}[\rho_A]) \tag{2.H.7}$$

$$= 0, \tag{2.H.8}$$

where the first inequality follows from the non-negativity of the min-unextendible entanglement of states. The first equality follows from the the fact that $E \cong B$, and the last equality follows from the fact that ρ_A is a quantum state with unit trace. Since (2.H.5) and (2.H.8) hold for every full-rank state ρ_{AB}, we conclude that the min-unextendible entanglement of all full-rank states is equal to zero; that is, all full-rank states are super two-extendible.

As a consequence of Theorem 2.1, all full-rank states being contained in the set of super two-extendible states implies that the probabilistic one-way distillable secret key of all full-rank states is also equal to zero.

2.I Coherent information of Werner states

Proposition 2.3 *Consider a d-dimensional Werner state defined as follows:*

$$W_{AB}^{p,d} := p\frac{I_{AB} + F_{AB}}{d(d+1)} + (1-p)\frac{I_{AB} - F_{AB}}{d(d-1)}, \tag{2.I.1}$$

where $p \in [0,1]$, $d = d_A = d_B \in \{2,3,4,\ldots\}$, *and* F_{AB} *is the swap operator defined as* $F_{AB} := \sum_{i,j=0}^{d-1} |i\rangle\langle j|_A \otimes |j\rangle\langle i|_B$. *The coherent information of the state* $W_{AB}^{p,d}$ *is equal to the following quantity:*

$$I(A\rangle B)_{W^{p,d}} = 1 - h_2(p) - p\log_2(d+1) - (1-p)\log_2(d-1)\,. \tag{2.I.2}$$

Proof: The coherent information of a bipartite state ρ_{AB} is defined as follows [SN96]:

$$I(A\rangle B)_\rho := H(\mathrm{Tr}_A[\rho_{AB}]) - H(\rho_{AB})\,, \tag{2.I.3}$$

where $H(\rho)$ is the von Neumann entropy [vN27], defined as

$$H(\rho) := -\mathrm{Tr}[\rho\log_2\rho]\,. \tag{2.I.4}$$

The d-dimensional Werner state defined in (2.I.1) can be rearranged into the following form:

$$W_{AB}^{p,d} = p\frac{2}{d(d+1)}\Pi_{AB}^{\text{sym}} + (1-p)\frac{2}{d(d-1)}\Pi_{AB}^{\text{asym}}, \tag{2.I.5}$$

where Π^{sym} and Π^{asym} are the projections on the symmetric and asymmetric subspaces of the underlying Hilbert space, respectively. For a bipartite system, the symmetric and asymmetric projection operators can be written as follows:

$$\Pi_{AB}^{\text{sym}} = \frac{1}{2}\left(I_{AB} + F_{AB}\right), \tag{2.I.6}$$

$$\Pi_{AB}^{\text{asym}} = \frac{1}{2}\left(I_{AB} - F_{AB}\right), \tag{2.I.7}$$

where F_{AB} is the swap operator. The symmetric and asymmetric projection operators are orthogonal to each other:

$$\Pi_{AB}^{\text{sym}}\Pi_{AB}^{\text{asym}} = 0. \tag{2.I.8}$$

Let us first evaluate the von Neumann entropy of $\text{Tr}_A\left[W_{AB}^{p,d}\right]$. Note that

$$\text{Tr}_A[F_{AB}] = I_B. \tag{2.I.9}$$

Therefore,

$$\text{Tr}_A\left[\Pi_{AB}^{\text{sym}}\right] = \frac{d+1}{2}I_B, \tag{2.I.10}$$

$$\text{Tr}_A\left[\Pi_{AB}^{\text{asym}}\right] = \frac{d-1}{2}I_B, \tag{2.I.11}$$

and consequently,

$$\text{Tr}_A\left[W_{AB}^{p,d}\right] = \frac{p}{d}I_B + \frac{1-p}{d}I_B = \frac{I_B}{d}, \tag{2.I.12}$$

which is the maximally mixed state on system B. The von Neumann entropy of a d-dimensional maximally mixed state is equal to $\log_2 d$. Therefore,

$$H\left(\text{Tr}_A\left[W_{AB}^{p,d}\right]\right) = \log_2 d. \tag{2.I.13}$$

Now let us evaluate the von Neumann entropy of the Werner state $W_{AB}^{p,d}$:

$$H\Big(W_{AB}^{p,d}\Big) = -\operatorname{Tr}\Big[W_{AB}^{p,d}\log_2 W_{AB}^{p,d}\Big]. \tag{2.I.14}$$

Since Π_{AB}^{sym} and Π_{AB}^{asym} are orthogonal to each other, we can reduce the von Neumann entropy of the Werner state into the following form:

$$\begin{aligned} H\Big(W_{AB}^{p,d}\Big) = &-\operatorname{Tr}\left[p\frac{2}{d(d+1)}\Pi_{AB}^{\text{sym}}\log_2\left(p\frac{2}{d(d+1)}\Pi_{AB}^{\text{sym}}\right)\right] \\ &-\operatorname{Tr}\left[\frac{2(1-p)}{d(d-1)}\Pi_{AB}^{\text{asym}}\log_2\left(\frac{2(1-p)}{d(d-1)}\Pi_{AB}^{\text{asym}}\right)\right]. \end{aligned} \tag{2.I.15}$$

The eigenvalues of a projection operator are either equal to one or zero. Hence, for an arbitrary scalar α and an arbitrary projection operator Π^x,

$$\log_2(\alpha\Pi^x) = \Pi^x\log_2\alpha. \tag{2.I.16}$$

Therefore,

$$\begin{aligned} H\Big(W_{AB}^{p,d}\Big) = &-p\frac{2}{d(d+1)}\log_2\left(p\frac{2}{d(d+1)}\right)\operatorname{Tr}\Big[\Pi_{AB}^{\text{sym}}\Big] \\ &-(1-p)\frac{2}{d(d-1)}\log_2\left((1-p)\frac{2}{d(d-1)}\right)\operatorname{Tr}\Big[\Pi_{AB}^{\text{asym}}\Big]. \end{aligned} \tag{2.I.17}$$

From (2.I.10) and (2.I.11), it is straightforward to see the following equalities:

$$\operatorname{Tr}\Big[\Pi_{AB}^{\text{sym}}\Big] = \frac{d(d+1)}{2}, \tag{2.I.18}$$

$$\operatorname{Tr}\Big[\Pi_{AB}^{\text{asym}}\Big] = \frac{d(d-1)}{2}. \tag{2.I.19}$$

Substituting these values in (2.I.22), we arrive at the following expression for the von Neumann entropy of the Werner state:

$$H\Big(W_{AB}^{p,d}\Big) = -p\log_2\left(p\frac{2}{d(d+1)}\right) - (1-p)\log_2\left((1-p)\frac{2}{d(d-1)}\right) \tag{2.I.20}$$

$$= h_2(p) + p\log_2(d(d+1)) - p + (1-p)\log_2(d(d-1)) - (1-p) \tag{2.I.21}$$

$$= \log_2 d + h_2(p) - 1 + p \log_2(d+1) + (1-p)\log_2(d-1), \tag{2.I.22}$$

where $h_2(p) \coloneqq -p \log_2 p - (1-p)\log_2(1-p)$. Combining (2.I.3), (2.I.13), and (2.I.22), we conclude (2.I.2). □

2.J Coherent information of isotropic states

Proposition 2.4 *Consider a d-dimensional isotropic state $\zeta_{AB}^{F,d}$ which is defined as follows:*

$$\zeta_{AB}^{F,d} = F\, \Phi_{AB}^{d} + (1-F)\frac{I_{AB} - \Phi_{AB}^{d}}{d^2-1}, \tag{2.J.1}$$

where $F \in [0,1]$ and $d = d_A = d_B \in \{2,3,4,\ldots\}$. The coherent information of the state $\zeta_{AB}^{F,d}$ is equal to the following quantity:

$$I(A\rangle B)_{\zeta^{F,d}} = \log_2 d - h_2(F) - (1-F)\log_2(d^2-1), \tag{2.J.2}$$

where $h_2(x) \coloneqq -x \log_2 x - (1-x)\log_2(1-x)$.

Proof: Recall the definition of coherent information of a bipartite state ρ_{AB} from (2.I.3):

$$I(A\rangle B)_{\rho} \coloneqq H(\mathrm{Tr}_A[\rho_{AB}]) - H(\rho_{AB})\,. \tag{2.J.3}$$

The marginal of the isotropic state on either systems, A or B, is equal to the maximally mixed state for all $F \in [0,1]$ and $d \geq 2$. Therefore,

$$H\Big(\mathrm{Tr}_B\Big[\zeta_{AB}^{F,d}\Big]\Big) = H\Big(\frac{I_A}{d}\Big) = \log_2 d. \tag{2.J.4}$$

Now let us evaluate the von Neumann entropy of the isotropic state. Note that Φ_{AB}^{d} and $I_{AB} - \Phi_{AB}^{d}$ are orthogonal projectors. This implies the following equalities:

$$H\Big(\zeta_{AB}^{F,d}\Big) = -\,\mathrm{Tr}\Big[\zeta_{AB}^{F,d} \log_2 \zeta_{AB}^{F,d}\Big] \tag{2.J.5}$$

$$= -\operatorname{Tr}\Big[F\Phi_{AB}^{d}\log_2\Big(F\Phi_{AB}^{d}\Big)\Big] - \operatorname{Tr}\left[\frac{1-F}{d^2-1}\left(I_{AB}-\Phi_{AB}^{d}\right)\log_2\left(\frac{1-F}{d^2-1}\left(I_{AB}-\Phi_{AB}^{d}\right)\right)\right] \tag{2.J.6}$$

$$= -F\log_2 F\operatorname{Tr}\Big[\Phi_{AB}^{d}\Big] - \frac{1-F}{d^2-1}\log_2\left(\frac{1-F}{d^2-1}\right)\operatorname{Tr}\Big[I_{AB}-\Phi_{AB}^{d}\Big] \tag{2.J.7}$$

$$= -F\log_2 F - (1-F)\log_2\left(\frac{1-F}{d^2-1}\right) \tag{2.J.8}$$

$$= -F\log_2 F - (1-F)\log_2(1-F) + (1-F)\log_2\Big(d^2-1\Big) \tag{2.J.9}$$

$$= h_2(F) + (1-F)\log_2\Big(d^2-1\Big) \tag{2.J.10}$$

where we have used the property of projection operators mentioned in (2.I.16) to arrive at the third equality. Substituting (2.J.4) and (2.J.10) in the definition of coherent information, we arrive at (2.J.2). □

CHAPTER 3

UNEXTENDIBLE ENTANGLEMENT OF QUANTUM CHANNELS[1]

3.1 Abstract

Quantum communication relies on the existence of high quality quantum channels to exchange information. In practice, however, all communication links are affected by noise from the environment. Here we investigate the ability of quantum channels to perform quantum communication tasks by restricting the participants to use only local operations and one-way classical communication (one-way LOCC) along with the available quantum channel. In particular, a channel can be used to distill a highly entangled state between two parties, which further enables quantum or private communication. In this work, we invoke the framework of superchannels to study the distillation of a resourceful quantum state, such as a maximally entangled state or a private state, using multiple instances of a point-to-point quantum channel. We use the idea of k-extendibility to obtain a semidefinite relaxation of the set of one-way LOCC superchannels and define a class of entanglement measures for quantum channels that decrease monotonically under such superchannels; therefore these measures, dubbed collectively the "unextendible entanglement of a channel", yield upper bounds on several communication-theoretic quantities of interest in the regimes of resource distillation and zero error. We then generalize the formalism of k-extendibility to bipartite superchannels, thus obtaining functions that are monotone under two-extendible superchannels. This allows us to analyze probabilistic distillation of ebits or secret key bits from a bipartite state when using a resourceful quantum channel. Moreover, we propose semidefinite programs to evaluate several of

[1] V. Singh and M. M. Wilde, "Unextendible entanglement of quantum channels", accepted in *Transactions on Information Theory*, https://doi.org/10.1109/TIT.2025.3566737

these quantities, providing a computationally feasible method of comparison between quantum channels for resource distillation.

3.2 Introduction

Quantum communication technologies revolve around the transmission of quantum data between two spatially separated parties. The promise of a future quantum internet [LSW+04, Kim08, WEH18] relies on our ability to exchange quantum data and generate highly entangled states [HHHH09] shared across distant locations. However, it is challenging to realize an ideal quantum communication link between two distant parties, and in practice, we only have a noisy channel to transmit quantum data. Thus, it is crucial to understand our ability to perform quantum communication tasks over a noisy channel in order to recognize the advantages of a realizable quantum network over existing classical networks.

Finding limitations on the rate of communication imposed by the underlying noisy channel has been a topic of interest in both classical [Sha48, EGK11] and quantum information theory [Hay17, Wil17, Wat18, Hol19, KW20]. The quantum capacity of a channel is equal to the largest rate at which qubits can be reliably transmitted over asymptotically many uses of the channel, such that the error vanishes in this limit. The laws of quantum mechanics also allow for unconditionally secure communication [BB84, Eke91, HHHO05, HHHO09], unlike classical networks, which often rely on the computational power of the adversary to implement privacy. This has sparked interest in understanding limitations on private communication over quantum channels.

While the standard definitions of quantum capacities allow for arbitrarily small errors

in communication that vanish in the asymptotic limit of many channel uses, zero-error communication [Sha56] is a special case in which the quantum channel is required to perform a communication task exactly (i.e., without error). While a noisy channel is incapable of doing so on its own, one can use error-correction protocols along with the channel to reduce the error probability in transmitting data, albeit at the cost of a reduced rate of communication. In some cases, one can use such protocols to reduce the error probability to zero.

Any error-correction protocol can be mathematically described using the language of superchannels [CDP08, LM15, Gou19], a linear map that transforms one quantum channel into another. In doing so, one needs to restrict the allowed superchannels to mimic the physical reality of the protocols. A natural restriction is that the two participants, Alice and Bob, can only perform local quantum operations. In our setting, we also allow Alice to send classical data to Bob. This restricts the set of allowed superchannels to the set of one-way LOCC (local operations and classical communication) superchannels, as done, e.g., in [LM15, BBFS21, HSW23], which also serves as the set of free operations in the resource theory of quantum memories developed in [RBL18]. Allowing one-way LOCC is motivated not only by its power, as is evident from the teleportation [BBC$^+$93] and super-dense coding [BW92] protocols, but also by the low cost of classical communication nowadays.

In this paper, as a companion to our recent findings in [SW24], we use the concept of unextendibility of a quantum channel [KDWW19, KDWW21] in order to quantify its capability for quantum communication. The presence of quantum correlations imposes a fundamental restriction on the extendibility of any quantum resource. This property has been studied in the context of the entanglement content of quantum states [Wer89, DPS02, Doh14]. Similar notions of k-extendibility have been explored for

quantum channels [KDWW19, KDWW21, BBFS21]. The unextendibility of a resourceful quantum channel arises from its inability to broadcast the same quantum data to multiple parties and is closely related to the no-cloning theorem [Par70, WZ82]. Unextendibility has also been studied in some resource-theoretic frameworks [KDWW21, WWW24], and it has been used to obtain tight bounds on information processing quantities such as one-way distillable entanglement [BDSW96, CCGFZ99, PSBZ01, RST+18] and distillable secret key [BB84, HHHO05, HHHO09]. Extendible channels can be understood as a relaxation of the set of one-way LOCC channels [KDWW21], which is one of the foundations upon which the present work builds.

We also define a family of entanglement measures for a quantum channel based on its unextendibility, which we call the unextendible entanglement of quantum channels. The definition of these measures is motivated from the unextendible entanglement for quantum states, previously defined in [WWW24]. We use this entanglement measure to give bounds on multiple quantities of interest in quantum information processing tasks in the regimes of zero error and probabilistic distillation. Additionally, several of our bounds can be computed via semidefinite programs. In what follows, we briefly discuss our contributions in more detail.

First, we give an upper bound on the exact one-way distillable key of a quantum channel, which is roughly defined as the maximum rate of distilling exact secret bits using the channel along with one-way LOCC assistance. We investigate one-shot as well as asymptotic protocols for distributing bipartite private quantum states, from which a secret key can be realized. These upper bounds are practically relevant because quantum key distribution [Eke91, BB84, May01] is one of the major advantages of quantum networks over classical networks, as this method ensures unconditional private communication between two parties, based on the laws of quantum mechanics.

Next we give an upper bound on the exact one-way distillable entanglement of a quantum channel, which is roughly defined as the maximum rate of distilling exact Bell states (ebits) using the channel with one-way LOCC assistance. This is a task of utmost importance to establish an ideal quantum network as a large number of quantum communication tasks, including teleportation, super-dense coding, secret key distillation, etc., rely on distant parties sharing highly entangled states. We investigate limitations on entanglement distribution in the presence of a noisy channel, assisted by local operations and one-way classical communication.

Our formalism allows us to investigate various capacities of a quantum channel as well. We give an upper bound on the zero-error private capacity of a quantum channel assisted by one-way LOCC superchannels, which is defined as the maximum rate at which secret bits can be transmitted exactly over multiple uses of the channel. Zero-error capacities have been studied in classical information theory extensively [KO98], and they have been explored to a lesser degree in quantum information theory [GDAM06] (see also [CS12, Shi15, LY16] and references therein). We also give an upper bound on the zero-error quantum capacity of an arbitrary quantum channel assisted by a one-way LOCC superchannel, which is defined as the maximum rate at which qubits can be transmitted exactly over multiple uses of a quantum channel. We present a brief summary of our results for point-to-point channels in Table 3.1.

We also extend our formalism to semicausal bipartite quantum channels [BGNP01]. Semicausal bipartite quantum channels describe quantum operations that allow only one party to send information, quantum or classical, to the other. Such channels can be used to distill bipartite resourceful states, such as ebits or secret keys, from an existing bipartite noisy resource state. We establish the notion of k-extendibility of a bipartite superchannel and define an entanglement measure for bipartite quantum channels based on unex-

Operational Quantity	Upper bound	Reference
Exact distillable key	$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B})$	Corollary 3.1
Exact distillable entanglement	$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B})$	Corollary 3.2
Zero-error private capacity	$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B})$	Corollary 3.3
Zero-error quantum capacity	$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B})$	Corollary 3.4

Table 3.1: A list of our results for point-to-point quantum channels. We give upper bounds on several quantities related to quantum communication, as well as private communication, over a quantum channel in terms of the unextendible entanglement of the channel. In each of these scenarios, the quantum channel is denoted by $\mathcal{N}_{A\to B}$, and local operations and forward classical communication from Alice to Bob are allowed for free.

Operational Quantity	Upper bound	Reference
Probabilistic distillable entanglement	$\frac{1}{n}\widehat{E}^u(\rho_{AB}) + \widehat{E}^u(\mathcal{N}_{AB\to A'B'})$	Proposition 3.18
Exact distillable entanglement	$\frac{1}{n}\widehat{E}^u_{\min}(\rho_{AB}) + \widehat{E}^u_{\min}(\mathcal{N}_{AB\to A'B'})$	Proposition 3.19
Probabilistic distillable key	$\frac{1}{n}\widehat{E}^u(\rho_{AB}) + \widehat{E}^u(\mathcal{N}_{AB\to A'B'})$	Proposition 3.20
Exact distillable key	$\frac{1}{n}\widehat{E}^u_{\min}(\rho_{AB}) + \widehat{E}^u_{\min}(\mathcal{N}_{AB\to A'B'})$	Proposition 3.21

Table 3.2: A list of our results for bipartite quantum channels. We give upper bounds on the non-asymptotic probabilistic and zero-error distillable entanglement and distillable key of a bipartite quantum state ρ_{AB} and n instances of a bipartite quantum channel $\mathcal{N}_{AB\to A'B'}$, in terms of the unextendible entanglement of the state and channel.

tendibility. We use the unextendible entanglement of a bipartite channel to investigate its ability to increase the unextendibility of an existing bipartite state, hence, boosting the resource available for quantum communication between two parties.

The task of entanglement distillation and secret key distillation from a bipartite quantum state using only local operations and classical communication has been a subject of interest for some time in quantum information theory. Several interesting bounds have

been obtained for resources that can be distilled using only local operations and one-way classical communication [WWW24]. We look at a more general setting in which the two parties involved have access to a bipartite quantum channel that is not necessarily simulable by local operations and one-way classical communication, and we employ the unextendible entanglement of bipartite channels to upper bound the distillable entanglement and distillable secret key of a bipartite channel used in conjunction with a bipartite resource state, along with local operations and classical communication. Table 3.2 presents a brief summary of our results for bipartite semicausal channels.

We consider the example of the erasure channel and the depolarizing channel to demonstrate our results for the point-to-point case. We show that the exact one-way distillable key, exact one-way distillable entanglement, forward-assisted zero-error private capacity, and forward-assisted zero-error quantum capacity of the erasure and the depolarizing channel are all equal to zero. More generally, we show that a quantum channel with a full-rank Choi operator cannot be used for exact entanglement distillation or exact key distillation when employing one-way LOCC superchannels, and the forward-assisted zero-error quantum capacity as well as the forward-assisted zero-error private capacity of such channels are equal to zero.

To demonstrate our results for bipartite quantum channels, we consider an extension of the erasure channel in which either Bob's system gets erased and Alice retains the state she was trying to send to Bob, or Bob receives the state and Alice receives the erasure symbol. We give an analytical expression for the unextendible entanglement of this channel induced by the Belavkin–Staszewski relative entropy, which is an upper bound on the probabilistic one-way distillable entanglement and probabilistic one-way distillable key of the channel. We also consider a less idealistic setting where Alice receives some classical information indicating if the quantum data she sent to Bob was erased or not. Using a

semidefinite program, we compute upper bounds on the probabilistic one-way distillable entanglement and probabilistic one-way distillable key of this channel.

This paper is organized as follows:

- Section 3.3: Definitions and notations used in the paper along with preliminary information on quantum states, channels, and superchannels.
- Section 3.4: Background on k-extendibility for bipartite states, point-to-point channels, and superchannels.
- Section 3.5: Background on divergences of quantum states and channels, and formal definition of the unextendible entanglement of channels.
- Section 3.6: Applications of the unextendible entanglement in establishing upper bounds on exact one-way distillable key and exact one-way disillable entanglement of a channel in the one-shot and asymptotic settings, and establishing upper bounds on the forward assisted zero-error quantum capacity and forward assisted zero-error private capacity of channels.
- Section 3.7: Generalizes the notion of k-extendibility to bipartite superchannels and defines the unextendible entanglement of bipartite quantum channels.
- Section 3.8: Applications of the unextendible entanglement of bipartite quantum channels in bounding the probabilistic one-way distillable entanglement and probabilistic one-way distillable key of a bipartite state-channel pair.
- Section 3.9: Semidefinite program to calculate the unextendible entanglement of point-to-point and bipartite channels induced by the α-geometric Rényi relative entropy. Analytical and numerical calculation of the unextendible entanglement of special channels induced by geometric Rényi relative entropies.

3.3 Preliminaries

In this section we establish some background on the three major elements that we use in the rest of the work: quantum states, channels, and superchannels.

3.3.1 Quantum states and channels

A quantum state ρ_A is a positive semidefinite, unit-trace operator acting on a Hilbert space $\mathcal{H}_A$. All linear operators acting on the Hilbert space $\mathcal{H}_A$ form the set $\mathcal{L}(A)$, and all quantum states acting on this Hilbert space form the set $\mathcal{S}(A)$. A bipartite quantum state ρ_{AB} acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is called separable if it can be written as

$$\rho_{AB} = \sum_x p(x)\sigma_A^x \otimes \tau_B^x, \tag{3.3.1}$$

where $\{p(x)\}_x$ is a probability distribution and $\{\sigma_A^x\}_x$ and $\{\tau_B^x\}_x$ are sets of states. Any quantum state that is not separable is said to be entangled. The d-dimensional maximally entangled state vector on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is

$$|\Phi^d\rangle_{AB} \coloneqq \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B, \tag{3.3.2}$$

where $\frac{1}{\sqrt{d}}$ is the normalizing factor and $\{|i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis. The corresponding density operator is written as $\Phi_{AB}^d \equiv |\Phi^d\rangle\langle\Phi^d|_{AB}$.

A quantum channel $\mathcal{N}_{A\to B}$ is a completely positive (CP) and trace preserving (TP) linear map that takes an operator acting on the Hilbert space $\mathcal{H}_A$ as input and outputs an operator acting on the Hilbert space $\mathcal{H}_B$. Let $\Gamma_{RB}^{\mathcal{N}}$ denote the Choi operator of the quantum channel $\mathcal{N}_{A\to B}$, which is defined as follows:

$$\Gamma_{RB}^{\mathcal{N}} \coloneqq \mathcal{N}_{A\to B}(\Gamma_{RA}), \tag{3.3.3}$$

where $\Gamma_{RA} \coloneqq d\Phi^d_{RA}$ is the unnormalized maximally entangled operator.

Throughout our paper, we have to consider extensions of quantum states and channels. We define the set of relevant extensions of a quantum state ρ by $\text{Ext}(\rho)$ and the set of relevant extensions of a quantum channel $\mathcal{N}$ by $\text{Ext}(\mathcal{N})$. The precise definitions of these sets are given later in (3.5.34), (3.5.68), and (3.7.20). In the rest of the work, we use the abbreviation B_S for a joint system that contains the isomorphic systems $\{B_i\}_i$ for all values of i in a subset S of all positive integers. For a positive integer k, we use the shorthand $[k]$ for the set $\{1, 2, \ldots, k\}$, and the shorthand $[k] \setminus i$ for the set $[k] \setminus \{i\}$.

3.3.2 Quantum superchannels

A quantum superchannel $\Theta_{(A\to B)\to(C\to D)}$ is a linear map that transforms a quantum channel $\mathcal{N}_{A\to B}$ to another quantum channel $\mathcal{M}_{C\to D}$. By definition, a superchannel is a completely CPTP preserving map (see Definition 3.1 for a formal definition). It can be perceived as a mathematical model for any physical transformation that a quantum channel can undergo, as long as the resulting map is also a quantum channel. Quantum superchannels were introduced in [CDP08] and further investigated in [Gou19], both of which provide a detailed discussion. Below we include a short review on superchannels that is relevant for this work.

Definition 3.1 (Superchannel) *Let $\mathcal{T}_{A\to B} : \mathcal{L}(A) \to \mathcal{L}(B)$ be a linear map. Let the space of all such maps be denoted by $\mathbb{L}^{AB}$. A linear map $\Theta_{(A\to B)\to(C\to D)} : \mathbb{L}^{AB} \to \mathbb{L}^{CD}$ is a superchannel if*

1. *It is completely CP preserving; i.e.,*

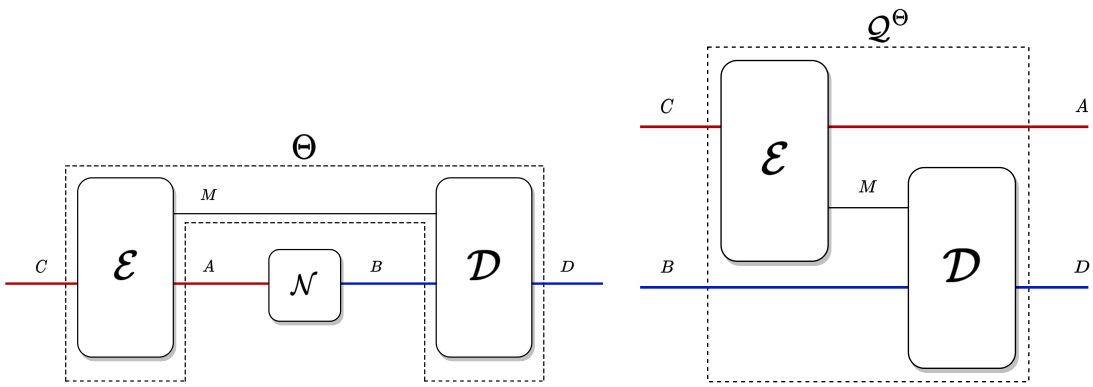


Figure 3.1: The figure on the left shows the decomposition of a superchannel $\Theta_{(A\to B)\to(C\to D)}$ into a pre-processing channel $\mathcal{E}_{C\to AM}$ and a post-processing channel $\mathcal{D}_{BM\to D}$ connected by a memory system M. The figure on the right shows the composition of the unique bipartite channel $Q^{\Theta}_{CB\to AD}$ associated with a superchannel $\Theta_{(A\to B)\to(C\to D)}$.

$(\mathrm{id}_{(E)\to(E)} \otimes \Theta_{(A\to B)\to(C\to D)})(\mathcal{T}_{EA\to EB})$ *is a CP map if* $\mathcal{T}_{EA\to E'B}$ *is a CP map, for all dimensions of system* E.

2. *It is TP preserving; i.e.,*

   $\Theta_{(A\to B)\to(C\to D)}(\mathcal{T}_{A\to B})$ *is a TP map if* $\mathcal{T}_{A\to B}$ *is a TP map.*

The fundamental theorem of superchannels states that every superchannel can be decomposed into a pre-processing channel $\mathcal{E}_{C\to MA}$ and a post-processing channel $\mathcal{D}_{MB\to D}$ connected by a memory system M [CDP08]; i.e., for every superchannel $\Theta_{(A\to B)\to(C\to D)}$, there exist $\mathcal{E}_{C\to MA}$ and $\mathcal{D}_{MB\to D}$ such that

$$\Theta_{(A\to B)\to(C\to D)}(\mathcal{N}_{A\to B}) = \mathcal{D}_{MB\to D} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}_{C\to MA}. \tag{3.3.4}$$

The pre-processing and post-processing channels are not unique to the superchannel. For example, we can introduce an isometric channel $\mathcal{V}$ and its corresponding reversal map $\mathcal{V}^{\dagger}$ acting on the memory system M without changing the superchannel. However, a unique bipartite channel is associated with every superchannel.

Theorem 3.1 ([Gou19]) *A superchannel with the following decomposition*

$$\Theta_{(A\to B)\to(C\to D)}(\mathcal{N}_{A\to B}) = \mathcal{D}_{MB\to D} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}_{C\to MA}, \tag{3.3.5}$$

has a unique bipartite quantum channel associated with it

$$Q^{\Theta}_{CB\to AD} := \mathcal{D}_{MB\to D} \circ \mathcal{E}_{C\to AM}. \tag{3.3.6}$$

We define the Choi operator of a superchannel using the unique bipartite quantum channel from (3.3.6):

$$\Gamma^{\Theta}_{A'D'CB} := (\mathrm{id}_{A'D'} \otimes Q^{\theta}_{CB\to AD})(\Gamma_{A'C} \otimes \Gamma_{D'B}), \tag{3.3.7}$$

where $\Gamma_{A'C} \equiv |\Gamma\rangle\langle\Gamma|_{A'C}$ is defined from the unnormalized maximally entangled vector:

$$|\Gamma\rangle_{A'C} := \sum_i |i\rangle_{A'}|i\rangle_C. \tag{3.3.8}$$

It suffices to choose systems A' and D' to be isomorphic to the systems A and D, respectively. The following theorem, established as Theorem 1 of [Gou19], provides conditions on the Choi operator in order for it to correspond to a legitimate superchannel:

Theorem 3.2 ([Gou19]) *The Choi operator of a superchannel $\Theta_{(A\to B)\to(C\to D)}$ satisfies the following constraints:*

$$\Gamma^{\Theta}_{ADCB} \geq 0, \tag{3.3.9}$$

$$\mathrm{Tr}_{AD}[\Gamma^{\Theta}_{ADCB}] = I_{CB}, \tag{3.3.10}$$

$$\mathrm{Tr}_{D}[\Gamma^{\Theta}_{ADCB}] = \frac{1}{d_B}\mathrm{Tr}_{BD}[\Gamma^{\Theta}_{ADCB}] \otimes I_B. \tag{3.3.11}$$

In the above, the first condition corresponds to the completely CP preserving condition, the second condition corresponds to the TP preserving condition, and the last condition corresponds to the nonsignaling constraint.

The Choi operator of the input channel $\mathcal{N}_{A\to B}$ and output channel $\mathcal{M}_{C\to D}$ of a superchannel $\Theta_{(A\to B)\to(C\to D)}$ are related through the following propagation rule [CDP08, Gou19]:

$$\Gamma^{\mathcal{M}}_{CD} = \mathrm{Tr}_{AB}[T_{AB}(I_{CD}\otimes\Gamma^{\mathcal{N}}_{AB})\Gamma^{\Theta}_{ADCB}], \tag{3.3.12}$$

where T_{AB} is the partial transpose map acting on systems A and B.

3.4 k-extendibility

In this section, we review the concepts of k-extendible states [Wer89, DPS02, DPS04] and channels [KDWW19, KDWW21], and we establish the notion of k-extendible superchannels. The framework of two-extendible superchannels was employed in [BBFS21] and [HSW23] for the purpose of analyzing quantum error correction. We present a more general discussion for arbitrary k in this section.

Several quantities of interest in quantum information theory are defined in terms of optimizations over the set of separable states, but it is computationally hard to optimize over this set [Gur03, Gha10]. The framework of k-extendibility allows us to approximate the set of separable states in terms of a larger set that contains all separable states. The set of k-extendible states is described by semidefinite constraints, and optimizations over this set are possible using semidefinite programs. The notions of k-extendible channels and superchannels are developed to circumnavigate the computational difficulty that arises when optimizing over the set of one-way LOCC channels [Gur03, Gha10].

3.4.1 k-extendible states

Let us first recall the definition of a k-extendible state [Wer89, DPS02, DPS04]. For a positive integer $k \geq 2$, a bipartite state ρ_{AB} is k-extendible with respect to system B if the following conditions hold:

1. There exists an extension state $\omega_{AB_{[k]}}$ such that

$$\mathrm{Tr}_{B_{[k]\setminus 1}}[\omega_{AB_{[k]}}] = \rho_{AB}, \tag{3.4.1}$$

   where each system B_i is isomorphic to B, for all $i \in [k]$.

2. The extended state is invariant under permutations of the B systems, i.e.,

$$\omega_{AB_{[k]}} = W^{\pi}_{B_{[k]}} \omega_{AB_{[k]}} W^{\pi^\dagger}_{B_{[k]}} \qquad \forall \pi \in S_k, \tag{3.4.2}$$

   where $W^{\pi}_{B_{[k]}}$ is the unitary permutation operator corresponding to the permutation π in the symmetric group S_k.

The set of k-extendible states is a semidefinite relaxation of the set of separable states. The main idea behind this formulation is that the higher the entanglement content between the systems A and B, the lower the number of systems B_i, each isomorphic to B, that can share correlations in the same way with A.

The weakest approximation of the set of separable states in this family is the set of two-extendible states. It is straightforward to see that every separable state, written as in (3.3.1), is two extendible with the extension $\omega_{AB_1B_2} = \sum_x p(x)\sigma^x_A \otimes \tau^x_{B_1} \otimes \tau^x_{B_2}$. However, not all two-extendible states are separable. As an example, sending one share of a maximally entangled state through an erasure channel characterized by erasure probability

1/2 results in the following two-extendible state that is not separable:

$$\frac{1}{2}\Phi_{AB}^{d} + \frac{1}{2}\pi_A \otimes |e\rangle\langle e|_B, \tag{3.4.3}$$

where $\pi_A := I_A/d$ and $|e\rangle\langle e|_B$ is the erasure symbol.

Remark 3.1 ([DPS04]) *The set of k-extendible states converges to the set of separable states when* $k \to \infty$.

3.4.2 *k*-extendible channels

For a positive integer $k \geq 2$, a point-to-point quantum channel $\mathcal{N}_{A\to B}$ is k-extendible with respect to B if the following conditions hold [PBaHS13]:

1. There exists an extension channel $\mathcal{P}_{A\to B_{[k]}}$ such that

$$\mathrm{Tr}_{B_{[k]\setminus 1}} \circ \mathcal{P}_{A\to B_{[k]}} = \mathcal{N}_{A\to B}. \tag{3.4.4}$$

2. The extended channel is invariant under permutations of the B systems, i.e.,

$$\mathcal{W}^{\pi}_{B_{[k]}} \circ \mathcal{P}_{A\to B_{[k]}} = \mathcal{P}_{A\to B_{[k]}} \qquad \forall \pi \in S_k, \tag{3.4.5}$$

   where $\mathcal{W}^{\pi}_{B_{[k]}}$ is the unitary channel that permutes the B systems by the permutation π in the symmetric group S_k.

Remark 3.2 *The Choi state of a point-to-point k-extendible channel is a k-extendible state.*

If a k-extendible state is input to a k-extendible channel, the output state is also k-extendible. This makes the definition of k-extendible channels consistent in a resource-theoretic approach; a free operation (k-extendible channel) cannot turn a free state (k-extendible state) into a resource.

Proposition 3.1 ([KDWW19]) *All point-to-point one-way LOCC channels are k-extendible for every $k \geq 2$. Furthermore, a point-to-point channel is k-extendible for every $k \geq 2$ if and only if it is a one-way LOCC channel.*

Proof: First we will show that every point-to-point one-way LOCC channel is k-extendible for every $k \geq 2$. The action of a one-way LOCC channel can be written as

$$\mathcal{N}_{A\to B}(\rho_A) = \sum_x \mathrm{Tr}[\Lambda_A^x \rho_A]\, \sigma_B^x, \tag{3.4.6}$$

where $\{\Lambda^x\}_x$ is a positive operator-valued measure (POVM) and $\left\{\sigma_B^x\right\}_x$ is a set of quantum states. This is also the same as an entanglement-breaking channel [HSR03].

Consider an extension of this channel that acts as follows:

$$\mathcal{P}_{A\to B_{[k]}}(\rho_A) \coloneqq \sum_x \mathrm{Tr}[\Lambda_A^x \rho_A]\, \sigma_{B_1}^x \otimes \cdots \otimes \sigma_{B_k}^x. \tag{3.4.7}$$

This is a valid quantum channel because x encodes classical data that can be copied any number of times. This extension obeys the permutation covariance conditions. Hence, $\mathcal{N}_{A\to B}$ is a k-extendible channel.

Recall that the Choi state of a point-to-point k-extendible channel is a k-extendible state. It is known from [DPS04] that a bipartite state is k-extendible for every $k \geq 2$ if and only if it is a separable state. Therefore, a channel is k-extendible for every $k \geq 2$ if and only if its Choi state is separable implying that it is a one-way LOCC channel (also called an entanglement-breaking channel). □

3.4.3 k-extendible superchannels

We further build upon the notion of extendibility and define the set of k-extendible superchannels. For a positive integer $k \geq 2$, a superchannel $\Theta_{(A\to B)\to(C\to D)}$, associated with the unique bipartite channel $Q^{\Theta}_{CB\to AD}$, is k-extendible if the following conditions hold.

1. There exists an extension superchannel $\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}$, with associated unique quantum channel $Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}}$, such that,

$$\mathrm{Tr}_{D_{[k]\setminus 1}} \circ Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}} = Q^{\Theta}_{CB\to AD} \circ \mathrm{Tr}_{B_{[k]\setminus 1}} . \tag{3.4.8}$$

2. $Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}}$ is covariant with respect to permutations of the input systems $B_{[k]}$ and output systems $D_{[k]}$, i.e.,

$$\mathcal{W}^{\pi}_{D_{[k]}} \circ Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}} = Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}} \circ \mathcal{W}^{\pi}_{B_{[k]}}, \qquad \forall \pi \in S_k \tag{3.4.9}$$

   where $\mathcal{W}^{\pi}_{D_{[k]}}$ and $\mathcal{W}^{\pi}_{B_{[k]}}$ are unitary channels representing the permutation π.

This definition of k-extendible superchannels is consistent with the definition of two-extendible superchannels given in [HSW23] and the notion of k-extendible channels considered in [KDWW19, KDWW21].

Let us consider a specific decomposition of a superchannel $\Theta_{(A\to B)\to(C\to D)}$ in terms of a pre-processing channel $\mathcal{E}^{\Theta}_{C\to AM}$ and a post-processing channel $\mathcal{D}^{\Theta}_{MB\to D}$. Neither of the conditions implying k-extendibility of a superchannel involve systems A, C, and M. Thus, the conditions of k-extendibility of a superchannel can be reduced to conditions on the post-processing channel only.

Proposition 3.2 *The k-extendibility conditions for a superchannel are semidefinite constraints on the Choi operators of the superchannel $\Theta_{(A\to B)\to(C\to D)}$ and its extension $\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}$. Along*

with the conditions in Theorem 3.2, the Choi operators Γ^{Θ}_{ADCB} *and* $\Gamma^{\Upsilon}_{AD_{[k]}CB_{[k]}}$ *satisfy the following:*

$$\mathrm{Tr}_{D_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}_{CB_{[k]}AD_{[k]}}\right] = \Gamma^{\Theta}_{CBAD} \otimes \frac{I_{B_{[k]\setminus 1}}}{d_B^{k-1}}, \tag{3.4.10}$$

$$W^{\pi}_{D_{[k]}} \Gamma^{\Upsilon} W^{\pi\dagger}_{D_{[k]}} = W^{\pi\dagger}_{B_{[k]}} \Gamma^{\Upsilon} W^{\pi}_{B_{[k]}} \quad \forall \pi \in S_k. \tag{3.4.11}$$

Proposition 3.3 *Let* $\Theta_{(A\to B)\to(C\to D)}$ *be a k-extendible superchannel with the k-extension* $\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}$. *Then each marginal of the channel obtained by acting with the superchannel* Υ *on a channel* $\mathcal{P}_{A\to B_{[k]}}$ *is the same as the channel obtained by acting with the superchannel* Θ *on the respective marginal of the channel* $\mathcal{P}_{A\to B_{[k]}}$. *That is,*

$$\mathrm{Tr}_{D_{[k]\setminus i}} \circ \left(\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}\left(\mathcal{P}_{A\to B_{[k]}}\right)\right) = \Theta_{(A\to B)\to(C\to D)}\left(\mathrm{Tr}_{B_{[k]\setminus i}} \circ \mathcal{P}_{A\to B_{[k]}}\right) \ \forall i \in [k]. \tag{3.4.12}$$

Proof: Let $\Theta_{(A\to B)\to(C\to D)}$ be a k-extendible superchannel with the k-extension $\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}$. As such,

$$\mathrm{Tr}_{D_{[k]\setminus i}} \circ Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}} = Q^{\Theta}_{CB\to AD} \circ \mathrm{Tr}_{B_{[k]\setminus i}} \ \forall i \in [k], \tag{3.4.13}$$

where $Q^{\Theta}_{CB\to AD}$ and $Q^{\Upsilon}_{CB_{[k]}\to AD_{[k]}}$ are the unique quantum channels associated with the respective superchannels above. Let $\mathcal{N}_{A\to B}$ be a marginal of the channel $\mathcal{P}_{A\to B_{[k]}}$:

$$\mathrm{Tr}_{B_{[k]\setminus i}} \circ \mathcal{P}_{A\to B_{[k]}} = \mathcal{N}_{A\to B} \qquad \forall i \in [k]. \tag{3.4.14}$$

The Choi operator of the channel obtained by acting with the superchannel $\Theta_{(A\to B)\to(C\to D)}$ on $\mathcal{N}_{A\to B}$ is

$$\Gamma^{\Theta[\mathcal{N}]}_{CD} = \mathrm{Tr}_{AB}\left[T_{AB}\left(\Gamma^{\mathcal{N}}_{AB}\right)\Gamma^{\Theta}_{CBAD}\right], \tag{3.4.15}$$

where $\Gamma^{\mathcal{N}}_{AB}$ and Γ^{Θ}_{ADCB} are the Choi operators of the channel $\mathcal{N}_{A\to B}$ and the superchannel $\Theta_{(A\to B)\to(C\to D)}$, respectively.

Similarly, the Choi operator of the channel obtained by acting with the superchannel $\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}$ on the channel $\mathcal{P}_{A\to B_{[k]}}$ is,

$$\Gamma^{\Upsilon[\mathcal{P}]}_{CD_{[k]}} = \mathrm{Tr}_{AB_{[k]}}\left[T_{AB_{[k]}}\left(\Gamma^{\mathcal{P}}_{AB_{[k]}}\right)\Gamma^{\Upsilon}_{CB_{[k]}AD_{[k]}}\right]. \tag{3.4.16}$$

This channel has the marginal,

$$\begin{aligned}
\mathrm{Tr}_{D_{[k]\setminus i}}\left[\Gamma^{\Upsilon[\mathcal{P}]}_{CD_{[k]}}\right] &= \mathrm{Tr}_{AB_{[k]}D_{[k]\setminus i}}\left[T_{AB_{[k]}}\left(\Gamma^{\mathcal{P}}_{AB_{[k]}}\right)\Gamma^{\Upsilon}_{CB_{[k]}AD_{[k]}}\right] && (3.4.17)\\
&= \mathrm{Tr}_{AB_{[k]}}\left[T_{AB_{[k]}}\left(\Gamma^{\mathcal{P}}_{A_{[k]}}\right)\mathrm{Tr}_{D_{[k]\setminus i}}\left[\Gamma^{\Upsilon}_{CB_{[k]}AD_{[k]}}\right]\right] && (3.4.18)\\
&= \frac{1}{d_B^{k-1}}\mathrm{Tr}_{AB_{[k]}}\left[T_{AB_{[k]}}\left(\Gamma^{\mathcal{P}}_{AB_{[k]}}\right)\left(\Gamma^{\Theta}_{CB_iAD_i}\otimes I_{B_{[k]\setminus i}}\right)\right] && (3.4.19)\\
&= \mathrm{Tr}_{AB_i}\left[T_{AB_i}\left(\Gamma^{\mathcal{N}}_{AB_i}\right)\Gamma^{\Theta}_{CB_iAD_i}\right] && (3.4.20)\\
&= \Gamma^{\Theta[\mathcal{N}]}_{CD_i}, && (3.4.21)
\end{aligned}$$

where the equality in (3.4.19) follows from the non-signaling condition in (3.4.10) and the equality in (3.4.20) follows from the fact that $\mathcal{P}_{A\to B_{[k]}}$ is an extension of the channel $\mathcal{N}_{A\to B}$. Hence, we conclude (3.4.12). □

One-way LOCC superchannels

We briefly review one-way LOCC superchannels to establish their connection with k-extendible superchannels.

A superchannel $\Theta_{(A\to B)\to(C\to D)}$ is called one-way LOCC if it can be implemented using local operations and one-way classical communication only. The action of a one-way LOCC superchannel can be described by

$$\Theta_{(A\to B)\to(C\to D)}(\mathcal{N}_{A\to B}) = \sum_x \mathcal{D}^x_{B\to D}\circ\mathcal{N}_{A\to B}\circ\mathcal{E}^x_{C\to A}, \tag{3.4.22}$$

where $\{\mathcal{E}^x_{C\to A}\}_x$ is a set of CP maps such that the sum map $\sum_x \mathcal{E}^x_{C\to A}$ is trace preserving and $\{\mathcal{D}^x_{B\to D}\}_x$ is a set of quantum channels. This can be interpreted as the memory system M

being a purely classical system X and the pre-processing and post-processing channels being

$$\mathcal{E}_{C\to AX}(\rho_C) = \sum_x \mathcal{E}^x_{C\to A}(\rho_C)\otimes |x\rangle\langle x|_X, \tag{3.4.23}$$

$$\mathcal{D}_{BX\to D}(\sigma_{BX}) = \sum_x \mathcal{D}^x_{B\to D}(\langle x|\sigma_{BX}|x\rangle_X), \tag{3.4.24}$$

such that

$$\Theta_{(A\to B)\to(C\to D)}(\mathcal{N}_{A\to B}) = \mathcal{D}_{BX\to D}\circ\mathcal{N}_{A\to B}\circ\mathcal{E}_{C\to AX}. \tag{3.4.25}$$

The unique bipartite channel associated with a one-way LOCC superchannel is of the form

$$Q^{\Theta}_{CB\to AD} = \sum_x \mathcal{E}^x_{C\to A}\otimes\mathcal{D}^x_{B\to D}. \tag{3.4.26}$$

Proposition 3.4 *All one-way LOCC superchannels are k-extendible for all $k \geq 2$.*

Proof: Once again we exploit the fact that x is classical data and can be copied as many times as needed. Hence, we can construct a superchannel $\Upsilon_{(A\to B_{[k]})\to(C\to D_{[k]})}$ that acts on a quantum channel $\mathcal{P}_{A\to B_{[k]}}$ as

$$\Upsilon(\mathcal{P}_{A\to B_{[k]}}) := \sum_x \left(\mathcal{D}^x_{B_1\to D_1}\otimes\cdots\otimes\mathcal{D}^x_{B_k\to D_k}\right)\circ(\mathcal{P}_{A\to B_{[k]}})\circ\mathcal{E}^x_{C\to A}. \tag{3.4.27}$$

It is straightforward to verify that such an extension meets the necessary conditions for $\Theta_{(A\to B)\to(C\to D)}$ to be a k-extendible superchannel. □

We note here that the case of $k = 2$ in Proposition 3.4 was already considered in [BBFS21, HSW23].

3.5 Unextendible entanglement of quantum channels

With the framework of k-extendibility in hand, we can now define entanglement measures for quantum channels. We will further restrict our development to the case when $k = 2$. We begin by discussing some mathematical background prior to defining the entanglement measures that arise from unextendibility of quantum channels.

3.5.1 Generalized divergence of quantum states

Let $\mathbb{R}$ denote the field of real numbers. A generalized divergence [PV10] is a functional $\mathbf{D} : \mathcal{S}(A) \times \mathcal{S}(A) \to \mathbb{R} \cup \{+\infty\}$, such that, for arbitrary states $\rho_A, \sigma_A \in \mathcal{S}(A)$ and an arbitrary channel $\mathcal{N}_{A\to B}$, the data-processing inequality holds

$$\mathbf{D}(\rho_A \| \sigma_A) \geq \mathbf{D}(\mathcal{N}_{A\to B}(\rho_A) \| \mathcal{N}_{A\to B}(\sigma_A)) \,. \tag{3.5.1}$$

Some examples of divergences that commonly appear in quantum information theory are the quantum relative entropy [Ume62], Petz-Rényi relative entropies [Pet86], sandwiched Rényi relative entropies [MLDS+13, WWY14], and geometric Rényi relative entropies [Mat13, FF21a].

We are particularly interested in the geometric Rényi relative entropies, which are defined for $\alpha \in (0,1) \cup (1,\infty)$ and all states ω and τ as

$$\widehat{D}_\alpha(\omega\|\tau) := \frac{1}{\alpha - 1} \log_2 \widehat{Q}_\alpha(\omega\|\tau), \tag{3.5.2}$$

$$\widehat{Q}_\alpha(\omega\|\tau) := \lim_{\varepsilon \to 0^+} \operatorname{Tr}\left[\tau_\varepsilon \left(\tau_\varepsilon^{-\frac{1}{2}} \omega \tau_\varepsilon^{-\frac{1}{2}}\right)^\alpha\right], \tag{3.5.3}$$

where $\tau_\varepsilon := \tau + \varepsilon I$. Note that $\widehat{D}_1(\omega\|\tau)$ is defined as $\lim_{\alpha\to 1} \widehat{D}_\alpha(\omega\|\tau)$ so that $\widehat{D}_\alpha(\omega\|\tau)$ is defined for all $\alpha \in (0,\infty)$.

Lemma 3.1 (Proposition 74 of [KW21]) *The geometric Rényi relative entropy is strongly faithful; i.e., for all quantum states ω and τ and $\forall \alpha \in (0,1)\cup(1,\infty)$, $\widehat{D}_\alpha(\omega\|\tau) \geq 0$, and $\widehat{D}_\alpha(\omega\|\tau) = 0$ if and only if $\omega = \tau$.*

Lemma 3.2 (Proposition 72 of [KW21]) *The geometric Rényi relative entropy is monotonic in α for all $\alpha > 0$; i.e.,*

$$\alpha \geq \beta > 0 \quad \Rightarrow \quad \widehat{D}_\alpha(\omega\|\tau) \geq \widehat{D}_\beta(\omega\|\tau). \tag{3.5.4}$$

The geometric Rényi relative quasi-entropy $\widehat{Q}_\alpha(\omega\|\tau)$ takes the following form for $\alpha \in (0,1)$:

$$\widehat{Q}_\alpha(\omega\|\tau) = \operatorname{Tr}\left[\tau\left(\tau^{-\frac{1}{2}}\tilde{\omega}\tau^{-\frac{1}{2}}\right)^\alpha\right], \tag{3.5.5}$$

where

$$\tilde{\omega} := \omega_{0,0} - \omega_{0,1}\omega_{1,1}^{-1}\omega_{0,1}^\dagger, \tag{3.5.6}$$

$$\omega_{0,0} := \Pi_\tau \omega \Pi_\tau, \tag{3.5.7}$$

$$\omega_{0,1} := \Pi_\tau \omega \Pi_\tau^\perp, \tag{3.5.8}$$

$$\omega_{1,1} := \Pi_\tau^\perp \omega \Pi_\tau^\perp, \tag{3.5.9}$$

Π_τ is the projection onto the support of τ, and $\Pi_\tau^\perp$ is the projection onto the kernel of τ. All inverses are taken on the support of the respective operators. Note that when $\operatorname{supp}(\omega) \subseteq \operatorname{supp}(\tau)$, the geometric Rényi relative quasi-entropy converges to the following quantity:

$$\widehat{Q}_\alpha(\omega\|\tau) = \operatorname{Tr}\left[\tau\left(\tau^{-\frac{1}{2}}\omega\tau^{-\frac{1}{2}}\right)^\alpha\right]. \tag{3.5.10}$$

As recalled in Lemma 3.2 above, the α-geometric Rényi relative entropy increases monotonically in α, and the smallest quantity in this family of entropies is achieved when

$\alpha \to 0$. As such, we find that

$$\widehat{D}_0(\omega\|\tau) = \lim_{\alpha\to 0} \widehat{D}_\alpha(\omega\|\tau) = -\log_2 \mathrm{Tr}[\tau\Pi_\zeta], \tag{3.5.11}$$

where $\zeta \equiv \tau^{-\frac{1}{2}}\tilde{\omega}\tau^{-\frac{1}{2}}$, the operator $\tilde{\omega}$ was defined in (3.5.6), and Π_ζ is the projection onto the support of ζ.

When $\alpha \geq 1$, the geometric Rényi relative quasi-entropy takes the form in (3.5.10) if $\mathrm{supp}(\omega) \subseteq \mathrm{supp}(\tau)$, and it evaluates to $+\infty$ if $\mathrm{supp}(\omega) \not\subseteq \mathrm{supp}(\tau)$.

The geometric Rényi relative entropy obeys the data-processing inequality for $\alpha \in (0, 2]$; that is, for all states ρ and σ, every channel $\mathcal{N}$, and all $\alpha \in (0, 2]$, the following inequality holds:

$$\widehat{D}_\alpha(\rho\|\sigma) \geq \widehat{D}_\alpha(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)). \tag{3.5.12}$$

As $\alpha \to 1$, the geometric Rényi relative entropy converges to the Belavkin–Staszewski relative entropy [BS82]:

$$\widehat{D}(\omega\|\tau) \equiv \widehat{D}_1(\omega\|\tau) \tag{3.5.13}$$

$$:= \lim_{\alpha\to 1} \widehat{D}_\alpha(\omega\|\tau) \tag{3.5.14}$$

$$= \mathrm{Tr}\left[\omega \log_2\left(\omega^{\frac{1}{2}}\tau^{-1}\omega^{\frac{1}{2}}\right)\right], \tag{3.5.15}$$

as shown in [KW21, Proposition 79].

3.5.2 Generalized divergence of quantum channels

The notion of generalized divergence can be extended to quantum channels, and this extension provides a mathematical framework for comparing channels. The generalized

divergence between two channels is defined in terms of the generalized divergence between states, as follows [CMW16, LKDW18]:

$$\mathbf{D}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) := \sup_{\rho_{RA}} \mathbf{D}(\mathcal{N}_{A\to B}(\rho_{RA})\|\mathcal{M}_{A\to B}(\rho_{RA})), \tag{3.5.16}$$

where A and B are systems of arbitrary size and ρ_{RA} is a quantum state with no constraint on the reference system R in general. It suffices to restrict the optimization in (3.5.16) to pure states and the dimension of system R to be equal to the dimension of A. This follows from purification, the data-processing inequality, and the fact that all purifications of a state are related by an isometry acting on the purifying system (see [KW20, Proposition 4.79]).

A key property of an arbitrary generalized channel divergence is that it contracts under the action of a superchannel [Gou19, Eq. (92)]:

Theorem 3.3 ([Gou19]) *For two arbitrary quantum channels $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A\to B}$, and an arbitrary superchannel $\Theta_{(A\to B)\to(C\to D)}$, the generalized channel divergence obeys the inequality*

$$\mathbf{D}(\mathcal{N}\|\mathcal{M}) \geq \mathbf{D}(\Theta(\mathcal{N})\|\Theta(\mathcal{M}))\,, \tag{3.5.17}$$

where A, B, C, D are systems of arbitrary size.

Geometric Rényi relative entropy of channels

The α-geometric Rényi relative entropies form a family of generalized divergences between channels. We present a brief review of these quantities and their properties that are relevant for this work.

The α-geometric Rényi relative entropy of channels is defined for two arbitrary quantum channels and $\alpha \in (0,1) \cup (1,\infty)$ as

$$\widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) \coloneqq \sup_{\rho_{RA}} \widehat{D}_\alpha(\mathcal{N}_{A\to B}(\rho_{RA})\|\mathcal{M}_{A\to B}(\rho_{RA})). \tag{3.5.18}$$

For $\alpha \in (0,1) \cup (1,2]$, the data-processing inequality holds, and so the statement just after (3.5.16) applies, so that it suffices to perform the optimization over pure bipartite states with R isomorphic to A. This quantity is finite for $\alpha > 1$ if and only if $\operatorname{supp}(\Gamma^{\mathcal{N}}_{AB}) \subseteq \operatorname{supp}(\Gamma^{\mathcal{M}}_{AB})$ [FF21a]. The systems A and B can hold an arbitrary number of subsystems, a property that we shall use in Section 3.7 for bipartite quantum channels.

Note that the α-geometric Rényi relative entropy of channels converges to the Belavkin–Staszewski relative entropy when $\alpha \to 1$ [FF21a, KW20, DKQ+23]. Hence, we can remove the discontinuity in α by defining

$$\widehat{D}(\mathcal{N}\|\mathcal{M}) \equiv \widehat{D}_1(\mathcal{N}\|\mathcal{M}) \coloneqq \lim_{\alpha\to 1} \widehat{D}_\alpha(\mathcal{N}\|\mathcal{M})\,. \tag{3.5.19}$$

Lemma 3.3 ([FF21a, KW21]) *The geometric Rényi relative entropy for channels satisfies the following properties:*

1. *It is monotonic in α for $\alpha > 0$:*

$$\alpha \geq \beta > 0 \quad \Rightarrow \quad \widehat{D}_\alpha(\mathcal{N}\|\mathcal{M}) \geq \widehat{D}_\beta(\mathcal{N}\|\mathcal{M})\,. \tag{3.5.20}$$

2. *It is additive under tensor products of channels for $\alpha \in (0,2]$:*

$$\widehat{D}_\alpha(\mathcal{N}^1 \otimes \mathcal{N}^2\|\mathcal{M}^1 \otimes \mathcal{M}^2) = \widehat{D}_\alpha(\mathcal{N}^1\|\mathcal{M}^1) + \widehat{D}_\alpha(\mathcal{N}^2\|\mathcal{M}^2). \tag{3.5.21}$$

3. *For an arbitrary quantum channel $\mathcal{N}_{A\to B}$, a set $\mathcal{V}$ of completely positive maps described by semidefinite constraints, and $\alpha = 1 + 2^{-\ell}$ with $\ell \in \mathbb{N}$, the optimization $\min_{\mathcal{M}\in\mathcal{V}} \widehat{D}_\alpha(\mathcal{N}\|\mathcal{M})$ can be computed by a semidefinite program. See Section 3.9 for the full form of the SDP along with numerical calculations.*

Proof: The monotonicity of the α-geometric Rényi relative entropy of channels for all $\alpha \in (0,2]$ was shown in [KW21, Appendix H], and the semidefinite program to minimize the quantity $\widehat{D}_\alpha(\mathcal{N}\|\mathcal{M})$ over a set $\mathcal{V}$ of completely positive maps described by semidefinite constraints, was given in [FF21a, Lemma 9] for all $\alpha \in (1,2]$.

Additivity of α-geometric Rényi relative entropy for all $\alpha \in (0,2]$ is a corollary of [KW21, Proposition 47]. For completeness, we present a brief proof of additivity here. Consider two arbitrary pure states $\psi_{R_1A_1}$ and $\phi_{R_2A_2}$. The following inequality holds for the α-geometric Rényi relative entropy between two tensor-product channels:

$$\begin{aligned}
&\widehat{D}_\alpha\left(\mathcal{N}^1_{A_1\to B_1}\otimes\mathcal{N}^2_{A_2\to B_2}\middle\|\mathcal{M}^1_{A_1\to B_1}\otimes\mathcal{M}^2_{A_2\to B_2}\right)\\
&\geq \widehat{D}_\alpha\left(\left(\mathcal{N}^1\otimes\mathcal{N}^2\right)(\psi\otimes\phi)\middle\|\left(\mathcal{M}^1\otimes\mathcal{M}^2\right)(\psi\otimes\phi)\right) &(3.5.22)\\
&= \widehat{D}_\alpha\left(\mathcal{N}^1(\psi)\middle\|\mathcal{M}^1(\psi)\right)+\widehat{D}_\alpha\left(\mathcal{N}^2(\phi)\middle\|\mathcal{M}^2(\phi)\right). &(3.5.23)
\end{aligned}$$

Since the above inequality holds for all pure states $\psi_{R_1A_1}$ and $\phi_{R_2A_2}$, we can take a supremum over both and conclude that

$$\widehat{D}_\alpha\left(\mathcal{N}^1_{A_1\to B_1}\otimes\mathcal{N}^2_{A_2\to B_2}\middle\|\mathcal{M}^1_{A_1\to B_1}\otimes\mathcal{M}^2_{A_2\to B_2}\right)\geq\widehat{D}_\alpha\left(\mathcal{N}^1_{A_1\to B_1}\middle\|\mathcal{M}^1_{A_1\to B_1}\right)+\widehat{D}_\alpha\left(\mathcal{N}^2_{A_2\to B_2}\middle\|\mathcal{M}^2_{A_1\to B_1}\right). \tag{3.5.24}$$

Now consider the following inequality for channel composition given in Proposition 47 of [KW21],

$$\widehat{D}_\alpha(\mathcal{L}_1\circ\mathcal{L}_2\|\mathcal{K}_1\circ\mathcal{K}_2)\leq\widehat{D}_\alpha(\mathcal{L}_1\|\mathcal{K}_1)+\widehat{D}_\alpha(\mathcal{L}_2\|\mathcal{K}_2), \tag{3.5.25}$$

for channels $\mathcal{L}_1$, $\mathcal{L}_2$, $\mathcal{K}_1$, and $\mathcal{K}_2$, and $\alpha\in(0,1)\cup(1,2]$. Setting

$$\mathcal{L}_1 = \mathcal{N}^1_{A_1\to B_1}\otimes\mathrm{id}_{B_2}, \tag{3.5.26}$$

$$\mathcal{L}_2 = \mathrm{id}_{A_1}\otimes\mathcal{N}^2_{A_2\to B_2}, \tag{3.5.27}$$

$$\mathcal{K}_1 = \mathcal{M}^1_{A_1\to B_1}\otimes\mathrm{id}_{B_2}, \tag{3.5.28}$$

$$\mathcal{K}_2 = \mathrm{id}_{A_1}\otimes\mathcal{M}^2_{A_2\to B_2}, \tag{3.5.29}$$

we find that

$$\begin{aligned}
&\widehat{D}_\alpha\Big(\mathcal{N}^1_{A_1\to B_1}\otimes\mathcal{N}^2_{A_2\to B_2}\Big\|\mathcal{M}^1_{A_1\to B_1}\otimes\mathcal{M}^2_{A_2\to B_2}\Big)\\
&\leq \widehat{D}_\alpha\Big(\mathcal{N}^1_{A_1\to B_1}\otimes \mathrm{id}_{B_2}\Big\|\mathcal{M}^1_{A_1\to B_1}\otimes \mathrm{id}_{B_2}\Big)+\widehat{D}_\alpha\Big(\mathrm{id}_{A_1}\otimes\mathcal{N}^2_{A_2\to B_2}\Big\|\mathrm{id}_{A_1}\otimes\mathcal{M}^2_{A_1\to B_1}\Big) \qquad (3.5.30)\\
&= \widehat{D}_\alpha\Big(\mathcal{N}^1_{A_1\to B_1}\Big\|\mathcal{M}^1_{A_1\to B_1}\Big)+\widehat{D}_\alpha\Big(\mathcal{N}^2_{A_2\to B_2}\Big\|\mathcal{M}^2_{A_1\to B_1}\Big), \qquad (3.5.31)
\end{aligned}$$

where the last equality follows from the stability property of the channel divergence (i.e., it is not changed by tensoring the original channel with an arbitrary identity channel).

Finally, we can take the limit $\alpha \to 1$ on both sides and use the definition of $\widehat{D}_1(\cdot\|\cdot)$ in (3.5.19) to conclude that the α-geometric Rényi relative entropy of channels is additive under tensor products for all $\alpha \in (0, 2]$. □

3.5.3 Generalized unextendible entanglement of quantum states

The generalized unextendible entanglement of a bipartite state has been defined in [WWW24]. We include a short discussion on the topic for necessary development.

Definition 3.2 ([WWW24]) *The generalized unextendible entanglement of a bipartite state ρ_{AB}, induced by a generalized divergence* $\mathbf{D}$ *between states, is defined as*

$$\mathbf{E}^u(\rho_{AB}) \coloneqq \inf_{\rho_{AB_1B_2}\in\mathcal{S}(AB_1B_2)} \frac{1}{2}\Big\{\mathbf{D}(\rho_{AB}\|\operatorname{Tr}_{B_1}[\rho_{AB_1B_2}]) :\ \operatorname{Tr}_{B_2}[\rho_{AB_1B_2}] = \rho_{AB}\Big\}, \qquad (3.5.32)$$

where the optimization is over every state $\rho_{AB_1B_2}$ that is an extension of the state ρ_{AB}. We also adopt the following alternative notations sometimes because they can be helpful to make the bipartition $A|B$ clear:

$$\mathbf{E}^u(A;B)_\rho \equiv \mathbf{E}^u(\rho_{A:B}) \equiv \mathbf{E}^u(\rho_{AB}). \qquad (3.5.33)$$

Let us define the following set of extensions of a bipartite state ρ_{AB}:

$$\mathrm{Ext}(\rho_{AB}) \coloneqq \{\rho_{AB_1B_2} : \mathrm{Tr}_{B_2}[\rho_{AB_1B_2}] = \rho_{AB}\}, \tag{3.5.34}$$

where B_1 and B_2 are isomorphic to B. This allows us to write the generalized unextendible entanglement of ρ_{AB}, induced by the generalized divergence $\mathbf{D}$, as

$$\mathbf{E}^u(\rho_{AB}) = \inf_{\rho_{AB_1B_2} \in \mathrm{Ext}(\rho_{AB})} \frac{1}{2}\mathbf{D}(\rho_{AB} \| \mathrm{Tr}_{B_2}[\rho_{AB_1B_2}]). \tag{3.5.35}$$

The generalized unextendible entanglement provides a framework for quantifying the unextendibility of a bipartite state ρ_{AB} with respect to the system B. A different measure for unextendibility was considered in [KDWW19, KDWW21] where the divergence was measured from the fixed set of two-extendible states. However, in Definition 3.2, the divergence is measured by means of a set of states that depend on the input state itself. Although both measures are equal to the minimal possible value of $\mathbf{D}$ when ρ_{AB} is two-extendible, they are not equal in general.

Let us look specifically at the unextendible entanglement induced by the α-geometric Rényi relative entropy, $\widehat{E}^u_\alpha(\rho_{AB})$, for $\alpha \in (0, 2]$. This quantity is called the α-geometric unextendible entanglement in [WWW24].

Note that the underlying divergence of α-geometric unextendible entanglement had an intrinsic discontinuity at $\alpha = 1$, which was removed by defining the quantity $\widehat{D}(\cdot\|\cdot)$ as

$$\widehat{D}(\cdot\|\cdot) \equiv \widehat{D}_1(\cdot\|\cdot) \coloneqq \lim_{\alpha\to 1} \widehat{D}_\alpha(\cdot\|\cdot). \tag{3.5.36}$$

By definition, $\widehat{E}^u_\alpha$ is defined for $\alpha = 1$ as the unextendible entanglement induced by $\widehat{D}_1(\cdot\|\cdot)$; however, it is necessary to check if the function $\widehat{E}^u_\alpha$ is continuous at $\alpha = 1$. We denote the unextendible entanglement induced by $\widehat{D}_1(\cdot\|\cdot)$ as $\widehat{E}^u$; that is,

$$\widehat{E}^u(\rho_{AB}) \coloneqq \frac{1}{2} \inf_{\sigma\in\mathrm{Ext}(\rho)} \lim_{\alpha\to 1} \widehat{D}_\alpha(\rho\|\mathrm{Tr}_{B_1}[\sigma_{AB_1B_2}]). \tag{3.5.37}$$

Proposition 3.5 *The α-geometric unextendible entanglement of a state, in the limit $\alpha \to 1$, converges to the unextendible entanglement of states induced by the Belavkin–Staszewski relative entropy; i.e.,*

$$\lim_{\alpha\to 1} \widehat{E}^u_\alpha(\rho_{AB}) = \widehat{E}^u(\rho_{AB})\,. \tag{3.5.38}$$

Proof: See Appendix 3.A. □

The α-geometric unextendible entanglement of states increases monotonically in α, which is a consequence of the α-geometric Rényi relative entropy being monotonic in α. The smallest quantity in this family of unextendibility measures is achieved in the limit $\alpha \to 0$. We define this quantity as the min-geometric unextendible entanglement:

$$\widehat{E}^u_{\min}(\rho_{AB}) \coloneqq \lim_{\alpha\to 0^+} \widehat{E}^u_\alpha(\rho_{AB})\,. \tag{3.5.39}$$

Proposition 3.6 *The min-geometric unextendible entanglement of a quantum state is the unextendibe entanglement induced by the α-geometric Rényi relative entropy when $\alpha \to 0$; that is,*

$$\widehat{E}^u_{\min}(\rho_{AB}) = \frac{1}{2} \inf_{\sigma\in\operatorname{Ext}(\rho)} \lim_{\alpha\to 0^+} \widehat{D}_\alpha\Big(\rho\Big\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]\Big)\,. \tag{3.5.40}$$

Proof: Due to the monotonicity of the α-geometric unextendible entanglement in α, we can write

$$\begin{aligned}
\widehat{E}^u_{\min}(\rho_{AB}) &= \lim_{\alpha\to 0^+} \widehat{E}^u_\alpha(\rho_{AB}) && (3.5.41)\\
&= \inf_{\alpha\in(0,1)} \frac{1}{2} \inf_{\sigma\in\operatorname{Ext}(\rho)} \widehat{D}_\alpha(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) && (3.5.42)\\
&= \frac{1}{2} \inf_{\sigma\in\operatorname{Ext}(\rho)} \inf_{\alpha\in(0,1)} \widehat{D}_\alpha(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) && (3.5.43)\\
&= \frac{1}{2} \inf_{\sigma\in\operatorname{Ext}(\rho)} \lim_{\alpha\to 0^+} \widehat{D}_\alpha(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}])\,, && (3.5.44)
\end{aligned}$$

where the final equality follows from the monotonicity of the α-geometric Rényi relative entropy. □

Theorem 3.4 ([WWW24]) *The α-geometric unextendible entanglement of states for all $\alpha \in (0, 2]$ satisfies the following properties:*

1. *It is monotonic under a selective two-extendible bipartite operation $\left\{\mathcal{E}^y_{AB\to A'B'}\right\}_y$:*

$$\widehat{E}^u_\alpha(\rho_{AB}) \geq \sum_{y:p(y)>0} p(y)\widehat{E}^u_\alpha\left(\omega^y_{A'B'}\right), \tag{3.5.45}$$

   where

$$p(y) \coloneqq \mathrm{Tr}\left[\mathcal{E}^y_{AB\to A'B'}(\rho_{AB})\right], \tag{3.5.46}$$

$$\omega^y_{A'B'} \coloneqq \frac{1}{p(y)}\mathcal{E}^y_{AB\to A'B'}(\rho_{AB})\,. \tag{3.5.47}$$

2. *It obeys subadditivity for states $\rho_{A_1B_1}$ and $\sigma_{A_2B_2}$:*

$$\widehat{E}^u_\alpha(\rho_{A_1B_1}\otimes\sigma_{A_2B_2}) \leq \widehat{E}^u_\alpha(\rho_{A_1B_1}) + \widehat{E}^u_\alpha(\sigma_{A_2B_2})\,. \tag{3.5.48}$$

3. *Let Φ^d_{AB} be a maximally entangled state of Schmidt rank d. Then*

$$\widehat{E}^u_\alpha\left(\Phi^d_{AB}\right) = \log_2 d. \tag{3.5.49}$$

Proposition 3.7 (Direct–sum) *Let $\rho_{XX'AB}$ denote the following classical–classical–quantum state:*

$$\rho_{XX'AB} \coloneqq \sum_x p(x)|x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'} \otimes \rho^x_{AB}. \tag{3.5.50}$$

For $\alpha \in (1, 2]$, the α-geometric unextendible entanglement obeys the following inequalities:

$$\widehat{E}^u_\alpha(\rho_{XA:B}) \geq \sum_x p(x)\widehat{E}^u_\alpha(\rho^x_{AB}). \tag{3.5.51}$$

For $\alpha \in (0,2]$, it obeys the following:

$$\widehat{E}^u_\alpha(\rho_{XA:B}) = \widehat{E}^u_\alpha(\rho_{XA:X'B}) \geq \widehat{E}^u_\alpha(\rho_{A:X'B}). \tag{3.5.52}$$

The following equality holds for the Belavkin–Staszewski unextendible entanglement:

$$\widehat{E}^u(\rho_{XA:B}) = \sum_x p(x)\widehat{E}^u(\rho^x_{AB}). \tag{3.5.53}$$

Proof: Let us first prove the inequality in (3.5.51). A general extension of the state ρ_{XAB} is of the form,

$$\rho_{XAB_1B_2} = \sum_x p(x)|x\rangle\langle x|_X \otimes \rho^x_{AB_1B_2}, \tag{3.5.54}$$

where $\rho^x_{AB_1B_2}$ is an arbitrary extension of ρ^x_{AB}. Due to the direct-sum property of the α-geometric Rényi relative quasi-entropy defined in (3.5.3),

$$\log_2 \widehat{Q}_\alpha(\rho_{XAB}\|\operatorname{Tr}_{B_1}[\rho_{XAB_1B_2}]) = \log_2 \sum_x p(x)\widehat{Q}_\alpha\left(\rho^x_{AB}\|\operatorname{Tr}_{B_1}[\rho^x_{AB_1B_2}]\right) \tag{3.5.55}$$

$$\geq \sum_x p(x)\log_2 \widehat{Q}_\alpha\left(\rho^x_{AB}\|\operatorname{Tr}_{B_1}\left[\rho^x_{AB_1B_2}\right]\right), \tag{3.5.56}$$

where the inequality follows from concavity of the logarithm. Furthermore, for $\alpha > 1$, we can divide both sides by $\alpha - 1$ while preserving the inequality sign, implying that

$$\widehat{D}_\alpha(\rho_{XAB}\|\operatorname{Tr}_{B_1}[\rho_{XAB_1B_2}])$$

$$= \frac{1}{\alpha-1}\log_2 \widehat{Q}_\alpha(\rho_{XAB}\|\operatorname{Tr}_{B_1}[\rho_{XAB_1B_2}]) \tag{3.5.57}$$

$$\geq \frac{1}{\alpha-1}\sum_x p(x)\log_2 \widehat{Q}_\alpha\left(\rho^x_{AB}\|\operatorname{Tr}_{B_1}\left[\rho^x_{AB_1B_2}\right]\right) \tag{3.5.58}$$

$$= \sum_x p(x)\widehat{D}_\alpha\left(\rho^x_{AB}\|\operatorname{Tr}_{B_1}\left[\rho^x_{AB_1B_2}\right]\right) \tag{3.5.59}$$

$$\geq 2\sum_x p(x)\widehat{E}^u_\alpha(\rho^x_{AB}). \tag{3.5.60}$$

Since the above inequality holds for every extension $\rho_{XAB_1B_2}$, we can take the infimum over all such extensions and conclude (3.5.51).

Let us now prove the statements in (3.5.52). Observe that Alice can copy the contents of the classical register X to X' and send X' to Bob, and this action is a one-way LOCC channel. By invoking the fact that the α-geometric unextendible entanglement does not increase under one-way LOCC for $\alpha \in (0, 2]$ (see [WWW24, Remark 3]), we conclude that

$$\widehat{E}^u_\alpha(\rho_{XA:B}) \geq \widehat{E}^u_\alpha(\rho_{XA:X'B}). \tag{3.5.61}$$

Since performing a partial trace over the register X' in Bob's possession is also a one-way LOCC channel, we conclude the opposite inequality:

$$\widehat{E}^u_\alpha(\rho_{XA:X'B}) \geq \widehat{E}^u_\alpha(\rho_{XA:B}), \tag{3.5.62}$$

which, together with the inequality above, implies the equality in (3.5.52). Finally, discarding the register X in Alice's possession is also a one-way LOCC, which implies the inequality in (3.5.52).

We finally note that the inequality

$$\widehat{E}^u(\rho_{XA:B}) \geq \sum_x p(x)\widehat{E}^u(\rho^x_{AB}) \tag{3.5.63}$$

holds because (3.5.51) holds for all $\alpha > 1$, and thus we can invoke Proposition 3.5 and take the limit as $\alpha \to 1$. The opposite inequality is a consequence of the following reasoning. Let $\rho^x_{AB_1B_2}$ be an arbitrary extension of ρ^x_{AB} (i.e., $\mathrm{Tr}_{B_2}[\rho^x_{AB_1B_2}] = \rho^x_{AB}$). Consider that

$$\sum_x p(x)\widehat{D}(\rho^x_{AB_1}\|\rho^x_{AB_2}) = \widehat{D}(\rho_{XAB_1}\|\rho_{XAB_2}) \tag{3.5.64}$$

$$\geq 2\widehat{E}^u(\rho_{XA:B}), \tag{3.5.65}$$

where we invoked the direct-sum property of the Belavkin–Staszewski relative entropy (see [KW20, Eq. (4.7.62)]). Since the inequality holds for every extension of ρ^x_{AB}, we conclude that

$$\sum_x p(x)\widehat{E}^u(\rho^x_{AB}) \geq \widehat{E}^u(\rho_{XA:B}). \tag{3.5.66}$$

Combining the above inequality with the inequality in (3.5.63), we conclude (3.5.53). □

3.5.4 Generalized unextendible entanglement of point-to-point quantum channels

We are now in a position to define the unextendible entanglement of a point-to-point quantum channel. For a channel divergence $\mathbf{D}$, the unextendible entanglement of a quantum channel $\mathcal{N}_{A\to B}$ is defined as

$$\mathbf{E}^{u}(\mathcal{N}_{A\to B}) := \inf_{\mathcal{P}_{A\to B_1B_2}} \frac{1}{2}\{\mathbf{D}(\mathcal{N}_{A\to B}\|\mathrm{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) : \mathrm{Tr}_{B_2}\circ\mathcal{P}_{A\to B_1B_2} = \mathcal{N}_{A\to B}\}, \tag{3.5.67}$$

where the infimum is taken over every extension channel $\mathcal{P}_{A\to B_1B_2}$. Let us define the following set of extensions of the quantum channel $\mathcal{N}_{A\to B}$:

$$\mathrm{Ext}(\mathcal{N}_{A\to B}) := \{\mathcal{P}_{A\to B_1B_2} \in \mathrm{CP} : \mathrm{Tr}_{B_2}\circ\mathcal{P}_{A\to B_1B_2} = \mathcal{N}_{A\to B}\}, \tag{3.5.68}$$

where B_1 and B_2 are isomorphic to B and CP denotes the set of completely positive maps. The unextendible entanglement of a point-to-point quantum channel $\mathcal{N}_{A\to B}$, induced by a channel divergence $\mathbf{D}$, can thus be written as

$$\mathbf{E}^{u}(\mathcal{N}_{A\to B}) = \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}(\mathcal{N}_{A\to B}\|\mathrm{Tr}_{B_2}\circ\mathcal{P}_{A\to B_1B_2}). \tag{3.5.69}$$

This definition is motivated from the definition of unextendible entanglement of bipartite states in (3.5.32). The unextendible entanglement of a quantum channel $\mathcal{N}_{A\to B}$ between Alice and Bob quantifies the distinguishability of the two marginals of a quantum broadcast channel $\mathcal{P}_{A\to B_1B_2}$ such that one of the marginals is the channel of interest.

The no-broadcasting theorem [BCF+96], a generalization of the no-cloning theorem to mixed states, implies that there cannot exist a quantum channel $\mathcal{P}_{A\to B_1B_2}$ that can perfectly broadcast an arbitrary quantum state, in the sense that, for such a purported perfect broadcast channel, the marginal states on the output systems B_1 and B_2 are the same as the

input quantum state on system A. As such, there cannot exist a quantum channel $\mathcal{P}_{A\to B_1B_2}$ such that each of its marginals is the identity channel. However, a quantum broadcast channel can have identical marginals if the marginals are noisy channels, for example, a trivial channel that replaces the input with a fixed quantum state. The unextendible entanglement of a quantum channel thus can be understood as a measure of entanglement of the quantum channel arising from the limitations imposed by the non-broadcastability of quantum information.

The unextendible entanglement induced by a divergence $\mathbf{D}$ achieves its minimum for two-extendible channels. If the underlying divergence is strongly faithful, then the unextendible entanglement is equal to zero if and only if the channel is two-extendible.

Theorem 3.5 (Monotonicity) *The generalized unextendible entanglement of a channel does not increase under the action of a two-extendible superchannel. That is, for an arbitrary quantum channel $\mathcal{N}_{A\to B}$ and a two-extendible superchannel $\Theta_{(A\to B)\to(C\to D)}$,*

$$\mathbf{E}^u(\mathcal{N}_{A\to B}) \geq \mathbf{E}^u(\Theta(\mathcal{N}_{A\to B}))\,. \tag{3.5.70}$$

Proof: To begin with, consider a two-extendible superchannel $\Theta_{(A\to B)\to(C\to D)}$ with the two-extension $\Upsilon_{(A\to B_1B_2)\to(C\to D_1D_2)}$.

Let $\mathcal{P}_{A\to B_1B_2}$ be an extension of the channel $\mathcal{N}_{A\to B}$, implying $\mathcal{N}_{A\to B} = \mathrm{Tr}_{B_2}\circ\mathcal{P}_{A\to B_1B_2}$. The generalized divergence between the two marginals of the channel $\mathcal{P}_{A\to B_1B_2}$ satisfies

$$\begin{aligned}
\mathbf{D}(\mathcal{N}_{A\to B}\|\,\mathrm{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) &\geq \mathbf{D}(\Theta(\mathcal{N}_{A\to B})\|\Theta(\mathrm{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2})) && (3.5.71)\\
&= \mathbf{D}(\mathrm{Tr}_{D_2}\circ\Upsilon(\mathcal{P}_{A\to B_1B_2})\,\|\,\mathrm{Tr}_{D_1}\circ\Upsilon(\mathcal{P}_{A\to B_1B_2})) && (3.5.72)\\
&\geq 2\mathbf{E}^u(\Theta(\mathcal{N}_{A\to B}))\,. && (3.5.73)
\end{aligned}$$

The first inequality follows from the contraction of a generalized channel divergence under superchannels (Theorem 3.3). The equality follows from the nonsignaling property of two-extendible superchannels (Proposition 3.3), and the last inequality follows from the fact that $\Upsilon\left(\mathcal{P}_{A\to B_1B_2}\right)$ is a valid extension of the channel $\Theta\left(\mathcal{N}_{A\to B}\right)$.

Since (3.5.73) holds true for every extension $\mathcal{P}_{A\to B_1B_2}$ of the channel $\mathcal{N}_{A\to B}$, we can take the infimum over all such channels and conclude (3.5.70). □

Remark 3.3 *Since all one-way LOCC channels are two-extendible, the generalized unextendible entanglement of a channel does not increase under the action of a one-way LOCC superchannel.*

A superchannel Θ can also convert a point-to-point quantum channel $\mathcal{N}_{A\to B}$ to a bipartite quantum channel $\mathcal{M}_{C\to C'D}$ that is nonsignaling from D to C. We have not yet defined the unextendible entanglement of such channels (see Section 3.7 for unextendible entanglement of general bipartite channels); however, we can still compare the unextendible entanglement of any bipartite state that can be established by a channel of the form $\mathcal{M}_{C\to C'D}$ with the unextendible entanglement of point-to-point channels.

Theorem 3.6 *The unextendible entanglement of a quantum state $\sigma_{RC'D}$, with respect to the partition $RC' : D$, that can be established between two parties using a point-to-point quantum channel $\mathcal{N}_{A\to B}$ and a two-extendible superchannel $\Theta_{(A\to B)\to(C\to C'D)}$ is no greater than the unextendible entanglement of the quantum channel $\mathcal{N}_{A\to B}$; i.e.,*

$$\sup_{\rho_{RC}} \mathbf{E}^u(\sigma_{RC':D}) \leq \mathbf{E}^u(\mathcal{N}_{A\to B}), \tag{3.5.74}$$

where

$$\sigma_{RC'D} \coloneqq \left(\Theta_{(A\to B)\to(C\to C'D)}(\mathcal{N}_{A\to B})\right)(\rho_{RC}), \tag{3.5.75}$$

and ρ_{RC} is a quantum state.

Proof: Let $\Theta_{(A\to B)\to(C\to C'D)}$ be a two-extendible superchannel, and let $\Upsilon_{(A\to B_1B_2)\to(C\to C'D_1D_2)}$ be a two-extension of it. Consider the following state:

$$\sigma_{RC'D} \coloneqq \left(\Theta_{(A\to B)\to(C\to C'D)}(\mathcal{N}_{A\to B})\right)(\rho_{RC}), \tag{3.5.76}$$

where $\mathcal{N}_{A\to B}$ is a point-to-point channel. Let $\mathcal{P}_{A\to B_1B_2}$ be an arbitrary extension of the point-to-point channel $\mathcal{N}_{A\to B}$. Proposition 3.3 implies the following equality:

$$\begin{aligned}
\mathrm{Tr}_{D_2}[(\Upsilon(\mathcal{P}_{A\to B_1B_2}))(\rho_{RC})] &= (\Theta(\mathrm{Tr}_{B_2}\circ\mathcal{P}_{A\to B_1B_2}))(\rho_{RC}) && (3.5.77)\\
&= (\Theta(\mathcal{N}_{A\to B}))(\rho_{RC}) && (3.5.78)\\
&= \sigma_{RC'D}. && (3.5.79)
\end{aligned}$$

This implies that $\Upsilon(\mathcal{P}_{A\to B_1B_2})(\rho_{RC})$ is an extension of $\sigma_{RC'D}$ with respect to the partition $RC' : D$. By definition, the unextendible entanglement of the state $\sigma_{RC'D}$ satisfies the following inequality:

$$\begin{aligned}
\mathbf{E}^u(\sigma_{RC':D}) &\leq \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}(\sigma_{RC'D}\big\|\mathrm{Tr}_{D_1}[\Upsilon(\mathcal{P})(\rho_{RC})]) && (3.5.80)\\
&= \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}(\sigma_{RC'D}\big\|[\Theta(\mathrm{Tr}_{B_1}\circ\mathcal{P})(\rho_{RC})]). && (3.5.81)
\end{aligned}$$

Taking a supremum over every input state ρ_{RC}, we arrive at the following relations:

$$\begin{aligned}
\sup_{\rho_{RC}} \mathbf{E}^u(\sigma_{RC':D}) &\leq \sup_{\rho_{RC}} \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}(\sigma\big\|(\Theta(\mathrm{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}))(\rho_{RC})) && (3.5.82)\\
&= \sup_{\rho_{RC}} \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}((\Theta(\mathcal{N}))(\rho)\big\|(\Theta(\mathrm{Tr}_{B_1}\circ\mathcal{P}))(\rho)) && (3.5.83)\\
&\leq \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \sup_{\rho_{RC}} \frac{1}{2}\mathbf{D}((\Theta(\mathcal{N}))(\rho)\big\|(\Theta(\mathrm{Tr}_{B_1}\circ\mathcal{P}))(\rho)) && (3.5.84)\\
&= \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}(\Theta(\mathcal{N})\big\|\Theta(\mathrm{Tr}_{B_1}\circ\mathcal{P})) && (3.5.85)\\
&\leq \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}(\mathcal{N}_{A\to B}\big\|\mathrm{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) && (3.5.86)\\
&= \mathbf{E}^u(\mathcal{N}_{A\to B}), && (3.5.87)
\end{aligned}$$

where the second inequality follows from the max-min inequality, the second equality follows from the definition of generalized divergence of channels, the penultimate inequality follows from the data-processing inequality in Theorem 3.3, and the final equality follows from the definition of the unextendible entanglement of $\mathcal{N}_{A\to B}$. □

α-geometric unextendible entanglement of quantum channels

In this section, we consider the unextendible entanglement induced by the geometric Rényi relative entropy:

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) := \inf_{\mathcal{P}_{A\to B_1B_2}} \left\{ \widehat{D}_{\alpha}(\mathcal{N}_{A\to B} \| \operatorname{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2}) : \operatorname{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2} = \mathcal{N}_{A\to B} \right\} \quad \forall \alpha \in (0,2], \quad (3.5.88)$$

where the infimum is taken over every channel $\mathcal{P}_{A\to B_1B_2}$. We shall refer to this quantity as the α-geometric unextendible entanglement of channels following the convention used for unextendible entanglement of states. We list some important properties of the α-geometric unextendible entanglement of quantum channels.

1. **Subadditivity:** The α-geometric unextendible entanglement of a channel is subadditive with respect to tensor products of channels, for all $\alpha \in (0,2]$ (Proposition 3.8).
2. **Monotonicity in α:** The α-geometric unextendible entanglement of a channel increases monotonically with increasing α (Proposition 3.9).
3. **Computable via SDP:** For a positive integer ℓ, and $\alpha = 1+2^{-\ell}$, the α-geometric unextendible entanglement of a quantum channel can be computed using a semidefinite program (Proposition 3.24).

The α-geometric unextendible entanglement of quantum channels is subadditive under tensor products of channels, due to the additive property of the underlying divergence (see Lemma 3.3).

Proposition 3.8 (Subadditivity) *For every two quantum channels $\mathcal{N}^1_{A\to B}$ and $\mathcal{N}^2_{A'\to B'}$, the α-geometric unextendible entanglement is subadditive for all $\alpha \in (0,2]$:*

$$\widehat{E}^u_\alpha(\mathcal{N}^1_{A\to B}\otimes\mathcal{N}^2_{A'\to B'}) \leq \widehat{E}^u_\alpha(\mathcal{N}^1_{A\to B}) + \widehat{E}^u_\alpha(\mathcal{N}^2_{A'\to B'}). \tag{3.5.89}$$

Proof: Let $\mathcal{P}^1_{A\to B_1B_2}$ and $\mathcal{P}^2_{A'\to B'_1B'_2}$ be arbitrary extensions of the channels $\mathcal{N}^1_{A\to B}$ and $\mathcal{N}^2_{A'\to B'}$. As such,

$$\mathcal{N}^1_{A\to B} = \operatorname{Tr}_{B_2}\circ\mathcal{P}^1_{A\to B_1B_2}, \tag{3.5.90}$$

$$\mathcal{N}^2_{A'\to B'} = \operatorname{Tr}_{B'_2}\circ\mathcal{P}^2_{A'\to B'_1B'_2}. \tag{3.5.91}$$

The tensor-product channel $\mathcal{P}^1_{A\to B_1B_2}\otimes\mathcal{P}^2_{A'\to B'_1B'_2}$ is an extension of the channel $\mathcal{N}^1_{A\to B}\otimes\mathcal{N}^2_{A'\to B'}$ because

$$\mathcal{N}^1_{A\to B}\otimes\mathcal{N}^2_{A'\to B'} = \operatorname{Tr}_{B_2B'_2}\circ\left(\mathcal{P}^1_{A\to B_1B_2}\otimes\mathcal{P}^2_{A'\to B'_1B'_2}\right). \tag{3.5.92}$$

Note that in this case we are interested in the extendibility of the joint system BB' with respect to the joint system AA'. Then consider that

$$\widehat{E}^u_\alpha\left(\mathcal{N}^1\otimes\mathcal{N}^2\right) \leq \frac{1}{2}\widehat{D}_\alpha\left(\mathcal{N}^1\otimes\mathcal{N}^2\|\operatorname{Tr}_{B_1B'_1}\circ\left(\mathcal{P}^1\otimes\mathcal{P}^2\right)\right) \tag{3.5.93}$$

$$= \frac{1}{2}\widehat{D}_\alpha\left(\mathcal{N}^1\|\operatorname{Tr}_{B_1}\circ\mathcal{P}^1\right) + \frac{1}{2}\widehat{D}_\alpha\left(\mathcal{N}^2\|\operatorname{Tr}_{B'_1}\circ\mathcal{P}^2\right), \tag{3.5.94}$$

where the last equality follows from the additive property of α-geometric Rényi relative entropy of channels in (3.5.21). Since (3.5.94) holds for arbitrary extensions $\mathcal{P}^1_{A\to B_1B_2}$ and $\mathcal{P}^2_{A'\to B'_1B'_2}$, we can take the infimum over both and conclude (3.5.89). □

Proposition 3.9 *For all $\alpha \in (0,2]$, the α-geometric unextendible entanglement is monotonic in α, i.e.,*

$$2 \geq \alpha \geq \beta > 0 \quad \Rightarrow \quad \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \geq \widehat{E}^u_\beta(\mathcal{N}_{A\to B}). \tag{3.5.95}$$

Proof: This is a direct consequence of the monotonicity of geometric Rényi relative entropy of channels in α, which itself is a direct consequence of the α-monotonicity of the geometric Rényi relative entropy for states [KW21, Eq. (6.16)]. Let $\mathcal{P}_{A\to B_1B_2}$ be an arbitrary extension of $\mathcal{N}_{A\to B}$. Then

$$\frac{1}{2}\widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \geq \frac{1}{2}\widehat{D}_\beta(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \tag{3.5.96}$$

$$\geq \widehat{E}^u_\beta(\mathcal{N}_{A\to B})\,, \tag{3.5.97}$$

where the first inequality follows from the monotonicity of geometric Rényi relative entropy in α and the last inequality follows from the definition of β-geometric Rényi unextendible entanglement of channels. Since the inequality holds for every extension, we conclude the desired claim by taking the infimum over all such extensions. □

Remark 3.4 *The smallest quantity in the family of α-geometric unextendible entanglement is achieved in the limit $\alpha \to 0^+$, as implied by Proposition 3.9. We call this quantity the min-geometric unextendible entanglement and define it as follows:*

$$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B}) := \lim_{\alpha\to 0^+}\widehat{E}^u_\alpha(\mathcal{N}_{A\to B})\,. \tag{3.5.98}$$

Proposition 3.10 *The min-geometric unextendible entanglement of a channel is the unextendible entanglement induced by the α-geometric Rényi relative entropy as $\alpha \to 0$:*

$$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B}) = \inf_{\mathcal{P}\in\operatorname{Ext}(\mathcal{N})}\sup_{\psi_{RA}}\widehat{D}_0(\mathcal{N}(\psi)\,\|\operatorname{Tr}_{B_1}[\mathcal{P}(\psi)])\,. \tag{3.5.99}$$

Proof: Invoking the definition of min-geometric unextendible entanglement,

$$\widehat{E}^u_{\min}(\mathcal{N}_{A\to B}) = \lim_{\alpha\to 0^+}\widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \tag{3.5.100}$$

$$= \inf_{\alpha\in(0,2]}\inf_{\mathcal{P}\in\operatorname{Ext}(\mathcal{N})}\sup_{\psi_{RA}}\widehat{D}_\alpha(\mathcal{N}(\psi)\,\|\operatorname{Tr}_{B_1}[\mathcal{P}(\psi)]) \tag{3.5.101}$$

$$= \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \inf_{\alpha\in(0,2]} \sup_{\psi_{RA}} \widehat{D}_\alpha(\mathcal{N}(\psi) \,\|\, \mathrm{Tr}_{B_1}[\mathcal{P}(\psi)])\,, \tag{3.5.102}$$

where the second equality follows from the monotonicity of α-geometric unextendible entanglement with α and the third equality is arrived at by exchanging the infimums.

The α-geometric Rényi relative entropy $\widehat{D}_\alpha(\rho\|\sigma)$ is lower semi-continuous in (ρ,σ) [FF21b, Lemma A.3], and increases monotonically in α in the range $(0,2]$. Hence, we can employ the Mosonyi–Hiai minimax theorem from [MH11, Corollary A.2] (up to a minus sign on the outside therein) and establish that

$$\inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \inf_{\alpha\in(0,2]} \sup_{\psi_{RA}} \widehat{D}_\alpha(\mathcal{N}(\psi) \,\|\, \mathrm{Tr}_{B_1}[\mathcal{P}(\psi)]) = \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \sup_{\psi_{RA}} \inf_{\alpha\in(0,2]} \widehat{D}_\alpha(\mathcal{N}(\psi) \,\|\, \mathrm{Tr}_{B_1}[\mathcal{P}(\psi)]) \tag{3.5.103}$$

$$= \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \sup_{\psi_{RA}} \lim_{\alpha\to 0^+} \widehat{D}_\alpha(\mathcal{N}(\psi) \,\|\, \mathrm{Tr}_{B_1}[\mathcal{P}(\psi)]) \tag{3.5.104}$$

$$= \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \sup_{\psi_{RA}} \widehat{D}_0(\mathcal{N}(\psi) \,\|\, \mathrm{Tr}_{B_1}[\mathcal{P}(\psi)])\,. \tag{3.5.105}$$

This concludes the proof. □

Proposition 3.11 *The α-geometric unextendible entanglement of quantum channels converges to the unextendible entanglement induced by the Belavkin–Staszewski relative entropy as $\alpha \to 1$:*

$$\lim_{\alpha\to 1} \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) = \widehat{E}^u(\mathcal{N}_{A\to B}) \tag{3.5.106}$$

$$:= \inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})} \widehat{D}(\mathcal{N}_{A\to B} \| \,\mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1 B_2})\,. \tag{3.5.107}$$

Proof: See Appendix 3.B. □

Remark 3.5 *Using a semidefinite program, we can compute the α-geometric unextendible entanglement of a channel for $\alpha = 1 + 2^{-\ell}$, where ℓ is a positive integer. This quantity closely approximates the unextendible entanglement of the channel induced by the Belavkin–Staszewski*

relative entropy for large enough values of ℓ. However, it remains open to determine a semidefinite program to compute the α-geometric unextendible entanglement for $\alpha \in (0,1)$, which makes it difficult to estimate the min-geometric unextendible entanglement of a channel computationally.

3.6 Applications

In this section, we discuss some applications of the unextendible entanglement of a point-to-point quantum channel in establishing upper bounds on some operational quantities of interest, including a channel's exact one-way distillable key (Section 3.6.1), its probabilistic distillable entanglement (Section 3.6.2), its zero-error private capacity (Section 3.6.3), and its zero-error quantum capacity (Section 3.6.4).

3.6.1 Exact one-way distillable key of a channel

Quantum key distribution (QKD) [Eke91, BB84, May01] is the process of distributing information-theoretic secret keys between two parties, for the purpose of conducting private communication after the keys are established. The key distribution task establishes a maximally classically-correlated state between Alice and Bob, and it ensures secrecy by forcing any eavesdropper's system to be completely uncorrelated with this state. As such, the joint state between Alice, Bob, and an eavesdropper holding system E, after an ideal key distillation protocol, can be mathematically described as follows:

$$\tau_{ABE} \coloneqq \frac{1}{K} \sum_{k=1}^{K} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \sigma_E. \tag{3.6.1}$$

This is called an ideal tripartite key state. Such a tripartite key state is said to hold $\log_2 K$ secret bits.

In [HHHO05, HHHH09], it was shown that the task of distilling tripartite secret keys is equivalent to establishing bipartite private states between Alice and Bob, which yield a secret key between Alice and Bob upon measurement. A quantum state $\rho_{ABA'B'}$ is called a bipartite private state [HHHO05, HHHO09] if Alice and Bob can extract a maximally classically-correlated state by applying local measurements, such that the resulting state is in product form with any purifying system of $\rho_{ABA'B'}$:

$$(\mathcal{M}_A \otimes \mathcal{M}_B \otimes \mathrm{Tr}_{A'B'})\left(\psi^{\rho}_{ABA'B'E}\right) = \frac{1}{K}\sum_{k=1}^{K} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \otimes \sigma_E, \tag{3.6.2}$$

where $\psi^{\rho}_{ABA'B'E}$ is a purification of the state $\rho_{ABA'B'}$, $\mathcal{M}(\cdot) := \sum_k |k\rangle\langle k|\,(\cdot)\,|k\rangle\langle k|$ is a projective measurement channel, and σ_E is an arbitrary state of the purifying system E. Here A and B are the key systems, and A' and B' are the shield systems (see Figure 3.2).

While a maximally entangled state is an example of a bipartite private state, it was shown in [HHHO05, HHHH09] that there exist private states that hold a finite number of secret bits but have vanishing distillable entanglement. Therefore, the task of secret-key distillation is distinct from entanglement distillation, and it is not easily understood using the resource theory of entanglement.

We consider the task of establishing a bipartite private state $\gamma^{K}_{CDC'D'}$ between Alice and Bob, capable of generating a secret key of $\log_2 K$ bits, using multiple instances of a quantum channel $\mathcal{N}_{A\to B}$, an arbitrary state $\psi_{C\hat{C}}$, and a one-way LOCC superchannel $\Theta_{(A^n\to B^n)\to(\hat{C}\to C'DD')}$. The result of the protocol acting on an input state $\psi_{C\hat{C}}$ is specified mathematically as follows:

$$\Theta_{(A^n\to B^n)\to(\hat{C}\to C'DD')}(\mathcal{N}^{\otimes n}_{A\to B})\,(\psi_{C\hat{C}}) = \gamma^{K}_{CDC'D'}, \tag{3.6.3}$$

where the pre-processing and post-processing channels in Θ are taken to be isometric channels, with C' and D' as the corresponding purifying systems (see Figure 3.2).

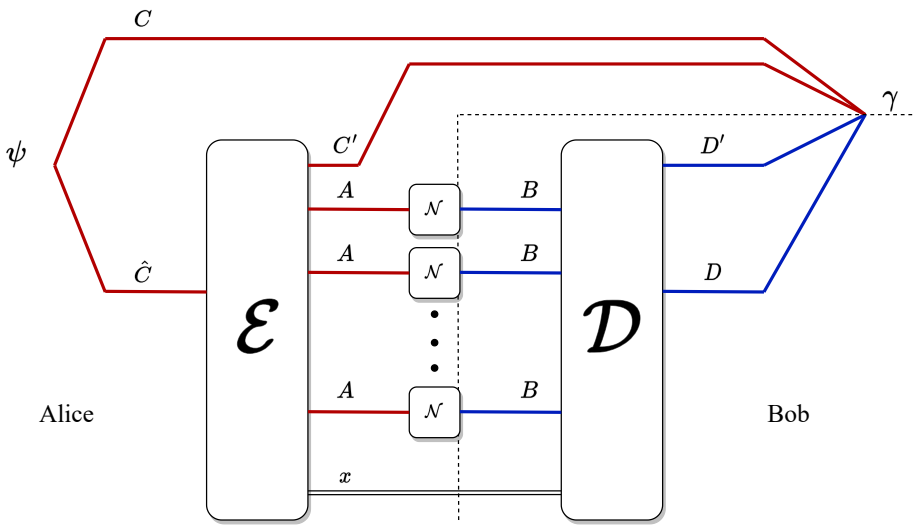


Figure 3.2: Diagrammatic representation of a protocol generating a bipartite private state $\gamma_{CDC'D'}$ between Alice and Bob through multiple uses of a quantum channel $\mathcal{N}_{A\to B}$. The protocol is enacted through the local operations $\mathcal{E}$ and $\mathcal{D}$ and one-way classical communication from Alice to Bob. Systems C and D form the key while C' and D' are the shield systems.

One-shot exact one-way distillable key

Let us first define the one-shot exact distillable key of a quantum channel; that is, we are considering the one-shot setting in which a single instance of the quantum channel $\mathcal{N}_{A\to B}$ is used. Let us define the set of all possible bipartite private states, holding $\log_2 K$ secret bits, as follows:

$$\mathcal{K} := \left\{\gamma^K_{CDC'D'} : K \in \mathbb{N}\right\}, \tag{3.6.4}$$

where $\gamma^K_{CDC'D'}$ is a private state holding $\log_2 K$ secret bits shared between two parties possessing systems CC' and DD', respectively, with C and D key systems and C' and D' shield systems.

Definition 3.3 *The one-shot exact distillable key of a quantum channel $\mathcal{N}_{A\to B}$ is the number of secret bits that can be distilled by a single use of the channel assisted by a one-way LOCC super-*

channel $\Theta_{(A\to B)\to(\hat{C}\to C'DD')}$*:*

$$K^{(1)}_{\text{1WL}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{\psi_{C\hat{C}}\in\mathcal{S}(C\hat{C}),\Theta\in\text{1WL},\\ \gamma^K_{CDC'D'}\in\mathcal{K}}} \left\{ \begin{array}{c} \log_2 K : \\ \Theta\left(\mathcal{N}\right)\left(\psi_{C\hat{C}}\right) = \gamma^K_{CDC'D'} \end{array} \right\}. \tag{3.6.5}$$

Definition 3.3 is motivated by the fact that once a bipartite private state with $\log_2 K$ bits of secrecy is established between two parties, a secret key of $\log_2 K$ bits can be distilled by only local operations.

We can also define the one-shot exact distillable key in a similar way when the channel is assisted by two-extendible superchannels:

$$K^{(1)}_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{\psi_{C\hat{C}}\in\mathcal{S}(C\hat{C}),\Theta\in\text{2-EXT},\\ \gamma^K_{CDC'D'}\in\mathcal{K}}} \left\{ \begin{array}{c} \log_2 K : \\ \Theta\left(\mathcal{N}\right)\left(\psi_{C\hat{C}}\right) = \gamma^K_{CDC'D'} \end{array} \right\}. \tag{3.6.6}$$

Since all one-way LOCC superchannels are two-extendible,

$$K^{(1)}_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \geq K^{(1)}_{\text{1WL}}(\mathcal{N}_{A\to B}). \tag{3.6.7}$$

Proposition 3.12 *The number of secret bits that can be distilled by using n instances of a quantum channel $\mathcal{N}_{A\to B}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the min-geometric unextendible entanglement of the channel $\mathcal{N}_{A\to B}$ (as defined in (3.5.98)). That is,*

$$\frac{1}{n}K^{(1)}_{\text{1WL}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \frac{1}{n}K^{(1)}_{\text{2-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}). \tag{3.6.8}$$

Proof: Let $\Theta_{(A^n\to B^n)\to(\hat{C}\to DC'D')}$ be a two-extendible superchannel that transforms n instances of quantum channel $\mathcal{N}_{A\to B}$ into a channel that acts on an input state $\psi_{C\hat{C}}$ to yield a private state $\gamma^K_{CDC'D'}$ holding $\log_2 K$ bits of secrecy with probability p; i.e.,

$$\Theta_{(A^n\to B^n)\to(\hat{C}\to DC'D')}(\mathcal{N}^{\otimes n}_{A\to B})\left(\psi_{C\hat{C}}\right) = \gamma^K_{CDC'D'}. \tag{3.6.9}$$

The α-geometric unextendible entanglement of a channel can be bounded from below as follows: using Theorem 3.6, monotonicity of and subadditivity of α-geometric unextendible entanglement under tensor products from Proposition 3.8,

$$
\begin{aligned}
n\widehat{E}^u_\alpha(\mathcal{N}) &\geq \widehat{E}^u_\alpha(\mathcal{N}^{\otimes n}) && (3.6.10)\\
&\geq \widehat{E}^u_\alpha(\Theta\left(\mathcal{N}^{\otimes n}\right)) && (3.6.11)\\
&\geq \widehat{E}^u_\alpha(\Theta\left(\mathcal{N}^{\otimes n}\right)(\psi_{C\hat{C}})) && (3.6.12)\\
&= \widehat{E}^u_\alpha\left(\gamma^K_{CDC'D'}\right) && (3.6.13)\\
&\geq \log_2 K, && (3.6.14)
\end{aligned}
$$

where the first inequality follows from the subadditivity of α-geometric unextendible entanglement (Proposition 3.8), the second inequality follows from the monotonicity of unextendible entanglement of a channel under the action of a two-extendible superchannel (Theorem 3.5), the third inequality follows from Theorem 3.6, and the last inequality follows from [WWW24, Corollary 22].

We can get the tightest possible upper bound with this technique by taking the limit $\alpha \to 0$ and applying Proposition 3.10, arriving at the following inequality:

$$
\widehat{E}^u_{\min}(\mathcal{N}_{A\to B}) \geq \frac{1}{n}\log_2 K. \tag{3.6.15}
$$

Since this inequality holds for every two-extendible superchannel Θ, input state $\psi_{C\hat{C}}$, and secret-key dimension K, we conclude (3.6.8). □

Asymptotic exact one-way distillable key

Now let us now consider the asymptotic setting in which an arbitrarily large number of independent uses of a channel are allowed along with a restricted set of superchannels

to establish a secret key between two parties. We begin by defining the asymptotic exact one-way distillable key of a quantum channel.

Definition 3.4 *The asymptotic exact one-way distillable key of a channel $\mathcal{N}_{A\to B}$ is the maximum achievable rate at which secret bits can be distilled by an arbitrarily large number of channel uses in parallel, along with one-way LOCC superchannels:*

$$K_{\text{1WL}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} K^{(1)}_{\text{1WL}}(\mathcal{N}^{\otimes n}_{A\to B}). \tag{3.6.16}$$

We can define the asymptotic two-extendible exact distillable key of the channel by relaxing the constraint on the superchannels to be two-extendible:

$$K_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} K^{(1)}_{\text{2-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}). \tag{3.6.17}$$

The definitions imply the following inequalities:

$$K_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \geq K^{(1)}_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \geq K^{(1)}_{\text{1WL}}(\mathcal{N}_{A\to B}), \tag{3.6.18}$$

and

$$K_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \geq K_{\text{1WL}}(\mathcal{N}_{A\to B}) \geq K^{(1)}_{\text{1WL}}(\mathcal{N}_{A\to B}). \tag{3.6.19}$$

Corollary 3.1 *The asymptotic exact distillable key of a channel $\mathcal{N}_{A\to B}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the min-geometric unextendible entanglement of the channel:*

$$\widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}) \geq K_{\text{2-EXT}}(\mathcal{N}_{A\to B}) \geq K_{\text{1WL}}(\mathcal{N}_{A\to B}). \tag{3.6.20}$$

Proof: The proof follows from the fact that Proposition 3.12 is true for all values of $n \in \mathbb{N}$. □

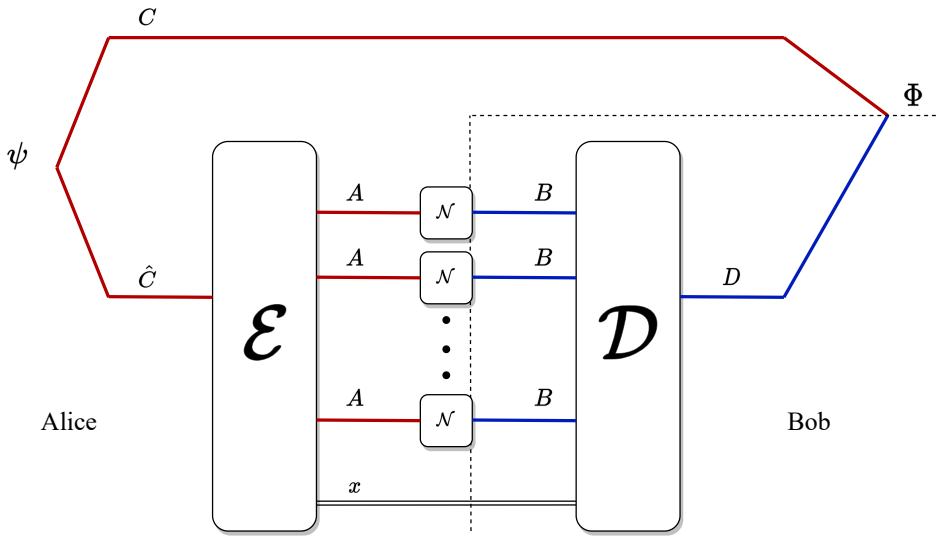


Figure 3.3: Diagrammatic representation of the protocol establishing a d-dimensional maximally entangled state Φ_{CD}^{d} between Alice and Bob through multiple uses of a quantum channel $\mathcal{N}_{A\to B}$ in parallel. The protocol is enacted through the local operations $\mathcal{E}$ and $\mathcal{D}$ and one-way classical communication from Alice to Bob.

3.6.2 Exact one-way distillable entanglement of a channel

All current quantum network models rely on distant parties holding one or more shares of a maximally entangled bipartite state (also known as an ebit). It is crucial to analyse the ability of a quantum channel to distribute entanglement between its participants such that a quantum network can be sustained by employing several of these channels.

We consider the task of entanglement distillation where Alice prepares ebits locally and sends shares of the ebits to Bob using a noisy quantum channel $\mathcal{N}_{A\to B}$ assisted by local operations and one-way classical communication from Alice to Bob. For a more general setting, we allow Alice to prepare any arbitrary bipartite state instead of ebits (see Figure 3.3).

One-shot exact one-way distillable entanglement

Let us first consider the one-shot case where Alice and Bob use a point-to-point quantum channel assisted by one-way LOCC superchannels to distill a maximally entangled state. The ability of a channel to distill a maximally entangled state between the two parties can be quantified by its one-shot exact one-way distillable entanglement, as defined below.

Definition 3.5 *The one-shot exact one-way distillable entanglement of a channel $\mathcal{N}_{A\to B}$ is the maximum number of ebits that can be established between two parties using the channel $\mathcal{N}_{A\to B}$ and a one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{C}\to D)}$:*

$$E^{(1)}_{D,1\text{WL}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{\psi_{C\hat{C}}\in\mathcal{S}(C\hat{C}),\\ \Theta\in 1\text{WL}}} \left\{ \begin{array}{c} \log_2 d : \\ \Theta\left(\mathcal{N}\right)\left(\psi_{C\hat{C}}\right) = \Phi^d_{CD} \end{array} \right\}. \tag{3.6.21}$$

We can relax the set of allowed superchannels to be the set of two-extendible superchannels and define the one-shot two-extendible exact distillable entanglement of a channel:

$$E^{(1)}_{D,2\text{-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{\psi_{C\hat{C}}\in\mathcal{S}(C\hat{C}),\\ \Theta\in 2\text{-EXT}}} \left\{ \begin{array}{c} \log_2 d : \\ \Theta\left(\mathcal{N}\right)\left(\psi_{C\hat{C}}\right) = \Phi^d_{CD} \end{array} \right\}. \tag{3.6.22}$$

An ebit shared between Alice and Bob can always be used to distill one bit of secret key between them. Hence, the number of secret bits that can be distilled from a channel is no less than the number of ebits that can be distilled from the channel, which leads to the following inequalities that hold for all $n \in \mathbb{N}$:

$$\frac{1}{n} E^{(1)}_{D,1\text{WL}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \frac{1}{n} K^{(1)}_{1\text{WL}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}), \tag{3.6.23}$$

and

$$\frac{1}{n} E^{(1)}_{D,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \frac{1}{n} K^{(1)}_{2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}). \tag{3.6.24}$$

Asymptotic exact one-way distillable entanglement of a channel

In general, we expect the exact one-way distillable key of the channel to be strictly larger than the exact one-way distillable entanglement of the channel because there exist private states that hold a finite number of exact secret bits but have no exact distillable entanglement [HHHO05]. Thus, the min-geometric unextendible entanglement of a channel is a tighter bound on the one-shot exact one-way distillable key of the channel than it is on the one-shot exact one-way distillable entanglement of the channel.

The asymptotic exact one-way distillable entanglement of a channel is defined as follows:

$$E_{D,1\text{WL}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} E^{(1)}_{D,1\text{WL}}(\mathcal{N}^{\otimes n}_{A\to B}), \tag{3.6.25}$$

which is the maximum achievable rate at which ebits can be distilled with an arbitrarily large number of uses of the channel $\mathcal{N}_{A\to B}$, assisted by a one-way LOCC superchannel. Similarly, the asymptotic generalization of the one-shot quantity in (3.6.22) is the following:

$$E_{D,2\text{-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} E^{(1)}_{D,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}), \tag{3.6.26}$$

which is the asymptotic two-extendible exact distillable entanglement of the channel. For every given channel $\mathcal{N}_{A\to B}$, the following inequalities are consequences of their definitions:

$$E_{D,2\text{-EXT}}(\mathcal{N}_{A\to B}) \geq E_{D,1\text{WL}}(\mathcal{N}_{A\to B}) \geq E^{(1)}_{D,1\text{WL}}(\mathcal{N}_{A\to B}). \tag{3.6.27}$$

This leads us to identify the min-geometric unextendible entanglement as an upper bound on the exact one-way distillable entanglement of a channel as we state formally in Corollary 3.2.

Corollary 3.2 *The exact one-way distillable entanglement of a channel is bounded from above by*

the min-geometric unextendible entanglement of the channel. That is, the following inequality holds for every channel $\mathcal{N}_{A\to B}$:

$$E_{D,1\text{WL}}(\mathcal{N}_{A\to B}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B})\,. \tag{3.6.28}$$

Proof: The inequalities in (3.6.24) hold for all $n \in \mathbb{N}$. The exact one-way distillable entanglement of a channel $\mathcal{N}_{A\to B}$ can be bounded as follows:

$$\begin{aligned} E_{D,1\text{WL}}(\mathcal{N}_{A\to B}) &\leq E_{D,2\text{-EXT}}(\mathcal{N}_{A\to B}) && (3.6.29)\\ &= \liminf_{n\to\infty} \frac{1}{n} E_{D,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}) && (3.6.30)\\ &\leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B})\,, && (3.6.31) \end{aligned}$$

where the first inequality follows from the fact that all one-way LOCC sueprchannels are two-extendible, the equality follows from the definition of the asymptotic two-extendible exact distillable entanglement of a channel given in (3.6.26), and the final inequality follows from (3.6.24). □

3.6.3 Zero-error private capacity assisted by one-way LOCC

The private capacity of a channel is defined as the largest rate at which private bits can be sent through the channel.

Consider a general protocol for private communication:

1. Alice encodes her classical message $|m\rangle\langle m|_{A_0}$ into a quantum state by means of an encoder $\mathcal{E}_{A_0\to A}$.

$$\omega^{m}_{A} := \mathcal{E}_{A_0\to A}(|m\rangle\langle m|_{A_0})\,. \tag{3.6.32}$$

2. Alice sends the encoded data to Bob through the channel $\mathcal{N}_{A\to B}$, which is extended by an isometric channel $\mathcal{U}^{\mathcal{N}}_{A\to BE}$.

3. Bob decodes the state he received by applying a POVM $\left\{\Lambda_B^{\hat{m}}\right\}_{\hat{m}}$. The final state of the overall BE system is,

$$\rho^m_{B_0E} = \mathcal{D}_{B\to B_0}\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}(\omega^m_A)\right) \tag{3.6.33}$$

$$= \sum_{\hat{m}} \mathrm{Tr}_B\left[\Lambda_B^{\hat{m}}\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\circ\mathcal{E}_{A_0\to A}(|m\rangle\langle m|_{A_0})\right)\right]|\hat{m}\rangle\langle\hat{m}|_{B_0}. \tag{3.6.34}$$

If the communication is successful and private, there exists a state σ_E of the environment system E, such that for every message m, the final state has the form

$$\rho^m_{B_0E} = |m\rangle\langle m|_{B_0}\otimes\sigma_E. \tag{3.6.35}$$

The action of the encoder $\mathcal{E}_{A_0\to A}$ and the decoder $\mathcal{D}_{B\to B_0}$ realizes a superchannel $\Theta_{(A\to B)\to(A_0\to B_0)}$ constructed by local operations. Let $\mathcal{P}_{A\to BE}$ be an arbitrary extension of the quantum channel $\mathcal{N}_{A\to B}$, where the system E can be accessed by an eavesdropper. Note that this extension is different from the extension of channels that we have discussed in the rest of this work, as the system E is not required to be isomorphic to system B.

This can be understood in a purified setting where the eavesdropper can access the environment system E output from the isometric extension $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ [Dev05] of the quantum channel $\mathcal{N}_{A\to B}$. However, we assume Alice's and Bob's laboratories to be secure in this setting and the eavesdropper cannot access any output systems from the encoding or decoding channel used in the protocol. Let $\Upsilon_{(A\to BE)\to(A_0\to B_0E_0)}$ be an arbitrary extension of the superchannel Θ that includes any post-processing that the eavesdropper can perform on their system E. The privacy condition in (3.6.35) implies that for every extended superchannel Υ, and isometric extension $\mathcal{U}^{\mathcal{N}}_{A\to BE}$, there exists a quantum state σ such that,

$$\Upsilon_{(A\to BE)\to(A_0\to B_0E_0)}\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\right) = \overline{\Delta}_{A_0\to B_0}\otimes\mathcal{A}^{\sigma}_{E_0}, \tag{3.6.36}$$

where $\overline{\Delta}_{A_0\to B_0}$ is the completely dephasing channel,

$$\overline{\Delta}_{A_0\to B_0}(\rho_{A_0}) = \sum_k \langle k|\rho_{A_0}|k\rangle |k\rangle\langle k|_{B_0}, \tag{3.6.37}$$

and $\mathcal{A}^{\sigma}_{E_0}$ denotes an appending channel that prepares the state σ on system E_0.

We assume that the eavesdropper only intends to learn about the information being sent from Alice to Bob, and not distort the data. Hence, we can assume that the channel established between Alice, Bob, and the eavesdropper is nonsignaling from the eavesdropper to Bob; i.e.,

$$\mathrm{Tr}_{E_0} \circ \left(\Upsilon\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\right)\right) = \Theta\left(\mathrm{Tr}_E \circ \mathcal{U}^{\mathcal{N}}_{A\to BE}\right) = \Theta\left(\mathcal{N}\right). \tag{3.6.38}$$

Let $\mathrm{Ext}_P(\Theta)$ denote the set of all such extensions of the superchannel Θ.

Now consider a superchannel $\Theta_{(A^n\to B^n)\to(A_0\to B_0)}$, composed of local operations by Alice and Bob, that acts on n instances of a quantum channel $\mathcal{N}_{A\to B}$ to communicate $\log_2 d$ bits of private data from Alice to Bob. An extended superchannel $\Upsilon_{(A\to BE)\to(A_0\to B_0E_0)}$ acts on some isometric extension $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ of the channel $\mathcal{N}_{A\to B}$ such that it lies in the set Ext_P. We define the one-shot zero-error private capacity of a quantum channel $\mathcal{N}_{A\to B}$ as follows:

$$P^{(1)}_{0,\mathrm{LO}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{d\in\mathbb{N},\\ \Theta\in\mathrm{LO}}} \left\{ \begin{array}{c} \log_2 d : \\ \forall\ \Upsilon \in \mathrm{Ext}_P(\Theta)\ \ \exists \sigma \in \mathcal{S}(E_0) \\ \Upsilon\left(\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\right)\right) = \overline{\Delta}_{A_0\to B_0} \otimes \mathcal{A}^{\sigma}_{E_0} \end{array} \right\}, \tag{3.6.39}$$

where $\overline{\Delta}_{A_0\to B_0}$ is a d-dimensional dephasing channel and $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ is an arbitrary isometric extension of the channel $\mathcal{N}_{A\to B}$.

Another quantity of interest is the zero-error private capacity of a channel assisted by one-way LOCC superchannels, where Alice can send classical data of arbitrary size to Bob along with the encoded quantum state. This classical data is naturally not private and can

be copied by the eavesdropper. However, the nonsignaling condition from (3.6.38) still holds. We define the one-shot zero-error private capacity assisted by one-way LOCC superchannels as follows:

$$P^{(1)}_{0,1\text{WL}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{d\in\mathbb{N},\\ \Theta\in 1\text{WL}}} \left\{ \begin{array}{c} \log_2 d : \\ \forall\, \Upsilon \in \text{Ext}_P(\Theta)\ \ \exists \sigma \in \mathcal{S}(E_0) \\ \Upsilon\left(\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\right)\right) = \overline{\Delta}_{A_0\to B_0} \otimes \mathcal{A}^{\sigma}_{E_0} \end{array} \right\}, \tag{3.6.40}$$

where the allowed superchannels are one-way LOCC superchannels instead of superchannels that can be constructed by only local operations.

We can further relax the set of superchannels to be two-extendible. The eavesdropper in this case also has access to a memory system that cannot necessarily be copied owing to its quantum nature. We define the one-shot zero-error private capacity assisted by two-extendible superchannels as follows:

$$P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{d\in\mathbb{N},\\ \Theta\in 2\text{-EXT}}} \left\{ \begin{array}{c} \log_2 d : \\ \forall\, \Upsilon \in \text{Ext}_P(\Theta)\ \ \exists \sigma \in \mathcal{S}(E_0) \\ \Upsilon\left(\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\right)\right) = \overline{\Delta}_{A_0\to B_0} \otimes \mathcal{A}^{\sigma}_{E_0} \end{array} \right\}. \tag{3.6.41}$$

Since the three sets of superchannels in consideration follow the hierarchy,

$$\text{LO} \subseteq \text{1WL} \subseteq \text{2-EXT}, \tag{3.6.42}$$

the respective private capacities obey the following inequalities:

$$P^{(1)}_{0,\text{LO}}(\mathcal{N}_{A\to B}) \leq P^{(1)}_{0,1\text{WL}}(\mathcal{N}_{A\to B}) \leq P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B})\,. \tag{3.6.43}$$

Once again, we can define asymptotic versions of these quantities. The zero-error private capacity of a quantum channel $\mathcal{N}_{A\to B}$ is defined as

$$P_{0,\text{LO}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} P^{(1)}_{0,\text{LO}}(\mathcal{N}^{\otimes n}_{A\to B})\,, \tag{3.6.44}$$

the forward-assisted zero-error private capacity of the channel as

$$P_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} P^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}^{\otimes n}_{A\to B}), \tag{3.6.45}$$

and the zero-error private capacity of the channel assisted by two-extendible superchannels as

$$P_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}). \tag{3.6.46}$$

Since Alice and Bob can always choose a superchannel Θ that acts independently on all instances of the channel $\mathcal{N}_{A\to B}$, we have the following inequalities:

$$P^{(1)}_{0,\mathrm{LO}}(\mathcal{N}_{A\to B}) \leq P_{0,\mathrm{LO}}(\mathcal{N}_{A\to B}), \tag{3.6.47}$$

$$P^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \leq P_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}), \tag{3.6.48}$$

$$P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \leq P_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}). \tag{3.6.49}$$

Private capacity and secret key distillation

The zero-error private capacity of a channel is closely related to its exact distillable key. A secret key of m bits can be established by sending m bits of private data from Alice to Bob. Thus, the number of private bits that can be transmitted using a quantum channel $\mathcal{N}_{A\to B}$ and any superchannel Θ is no larger than the number of bits of a secret key that can be established using the same channel $\mathcal{N}_{A\to B}$ and the superchannel Θ.

In addition, if Alice has the ability to send public classical data to Bob without using the channel $\mathcal{N}_{A\to B}$, the secret key distillation protocol can be converted into a private channel. Alice and Bob can use the one-time-pad scheme to send m bits of private data from Alice to Bob through the public classical channel and consume an m-bit secret key generated from the channel $\mathcal{N}_{A\to B}$.

The above arguments lead to the following conclusion: the one-shot zero-error private capacity of a channel assisted by one-way LOCC superchannels is equal to the one-shot exact one-way distillable key of the channel; that is,

$$P^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) = K^{(1)}_{1\mathrm{WL}}(\mathcal{N}_{A\to B}), \tag{3.6.50}$$

where $K^{(1)}_{1\mathrm{WL}}(\cdot)$ was defined in (3.6.5). Since two-extendible superchannels also allow Alice to send an arbitrary number of classical bits to Bob, the one-shot zero-error private capacity of the channel is equal to the following quantity:

$$P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) = K^{(1)}_{2\text{-EXT}}(\mathcal{N}_{A\to B}), \tag{3.6.51}$$

where $K^{(1)}_{2\text{-EXT}}(\cdot)$ was defined in (3.6.6). Combining the equality in (3.6.51) and the inequality in Proposition 3.12, we conclude the following proposition:

Proposition 3.13 *Given n instances of a quantum channel $\mathcal{N}_{A\to B}$, assisted by one-way LOCC or two-extendible superchannels, the rate at which private bits can be transmitted without error is bounded from above by the min-geometric unextendible entanglement of the channel $\mathcal{N}_{A\to B}$; that is, for all $n \in \mathbb{N}$,*

$$\begin{aligned}\frac{1}{n}P^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}^{\otimes n}_{A\to B}) &\leq \frac{1}{n}P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B})\\ &\leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}).\end{aligned} \tag{3.6.52}$$

Since Proposition 3.13 holds for all values of $n \in \mathbb{N}$, the min-geometric unextendible entanglement of a channel is an upper bound on the zero-error private capacity of the channel, as we state formally in Corollary 3.3 below.

Corollary 3.3 *The zero-error private capacity of a channel $\mathcal{N}_{A\to B}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the min-geometric unextendible entanglement of the channel $\mathcal{N}_{A\to B}$; i.e.,*

$$P_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \leq P_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B})\,. \tag{3.6.53}$$

3.6.4 Zero-error quantum capacity assisted by one-way LOCC

The zero-error quantum capacity of a channel is the maximum rate at which the channel can transmit quantum information with zero error over an arbitrarily large number of channel uses [Shi15] with the assistance of local operations. The notion of zero-error quantum capacity of a channel can be extended to the case where the channel is assisted by one-way LOCC superchannels, which has significance not only from a theoretical perspective but also from a practical viewpoint, given existing state-of-the-art classical networks.

Here we look at the zero-error quantum capacity of a channel assisted by one-way LOCC superchannels. Using one instance of a quantum channel $\mathcal{N}_{A\to B}$ and an arbitrary one-way ideal classical channel, the following channel can be simulated between the two parties:

$$\Theta\left(\mathcal{N}_{A\to B}\right) \coloneqq \sum_{x} \mathcal{D}^{x}_{B\to D} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}^{x}_{C\to A}, \tag{3.6.54}$$

where $\{\mathcal{E}^{x}_{C\to A}\}_x$ is a set of completely-positive maps whose sum is trace preserving and $\{\mathcal{D}^{x}_{B\to D}\}_x$ is a set of quantum channels.

The one-shot zero-error quantum capacity of a channel $\mathcal{N}_{A\to B}$ assisted by one-way

LOCC superchannels is defined as follows:

$$Q^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{d\in\mathbb{N},\\ \Theta\in 1\mathrm{WL}}} \left\{\log_2 d : \Theta(\mathcal{N}) = \mathrm{id}^d_{C\to D}\right\}, \tag{3.6.55}$$

where $\mathrm{id}^d_{C\to D}$ is the d-dimensional identity channel. We can relax the set of allowed superchannels to be the set of two-extendible superchannels, and we can define the one-shot zero-error quantum capacity of a quantum channel assisted by two-extendible superchannels as follows:

$$Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{d\in\mathbb{N},\\ \Theta\in 2\text{-EXT}}} \left\{\log_2 d : \Theta(\mathcal{N}_{A\to B}) = \mathrm{id}^d_{C\to D}\right\}. \tag{3.6.56}$$

Note that the following inequality holds because all one-way LOCC superchannels are two-extendible:

$$Q^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \leq Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}). \tag{3.6.57}$$

The zero-error quantum capacity of a channel assisted by one-way LOCC superchannels can be defined in terms of the one-shot zero-error quantum capacity of the channel assisted by one-way LOCC superchannels as follows:

$$Q_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} Q^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}^{\otimes n}_{A\to B}). \tag{3.6.58}$$

Similarly, the zero-error quantum capacity of the channel assisted by two-extendible superchannels can be defined as follows:

$$Q_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \coloneqq \liminf_{n\to\infty} \frac{1}{n} Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}). \tag{3.6.59}$$

Alice and Bob can always choose a quantum superchannel Θ that acts separately on each instance of the quantum channel $\mathcal{N}_{A\to B}$ as a strategy to simulate an identity channel using multiple instances of the channel $\mathcal{N}_{A\to B}$ and one-way LOCC or two-extendible superchannels. Hence, we have the following inequalities

$$Q^{(1)}_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}) \leq Q_{0,1\mathrm{WL}}(\mathcal{N}_{A\to B}), \tag{3.6.60}$$

$$Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \leq Q_{0,2\text{-EXT}}(\mathcal{N}_{A\to B})\,. \tag{3.6.61}$$

The zero-error quantum capacity of a channel cannot be larger than the zero-error private capacity of the channel in the one-shot or asymptotic setting. This is because a d-dimensional ideal quantum channel can be used to send d-dimensional private data from Alice to Bob as follows: Alice can encode her classical data in a pure d-dimensional quantum state and send it to Bob such that it is protected from any eavesdropper by the no-cloning theorem. Bob can then perform a measurement on the received quantum state in a predetermined basis and deterministically decode d bits of classical data encoded by Alice in the quantum state. Since we only need local operations to transform an ideal quantum channel to an ideal private channel, the following inequalities hold:

$$Q^{(1)}_{0,1\text{WL}}(\mathcal{N}_{A\to B}) \leq P^{(1)}_{0,1\text{WL}}(\mathcal{N}_{A\to B})\,, \tag{3.6.62}$$

$$Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) \leq P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B})\,, \tag{3.6.63}$$

where $P^{(1)}_{0,1\text{WL}}(\mathcal{N}_{A\to B})$ is the one-shot zero-error private capacity of a channel assisted by one-way LOCC superchannels, as defined in (3.6.40), and $P^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B})$ is the one-shot zero-error private capacity of a channel assisted by two-extendible superchannels, as defined in (3.6.41).

Proposition 3.14 *Consider an arbitrary zero-error protocol for quantum communication over a channel $\mathcal{N}_{A\to B}$ assisted by one-way LOCC or two-extendible superchannels, with n the number of channel uses. Then the following upper bound holds for all $n \in \mathbb{N}$:*

$$\frac{1}{n} Q^{(1)}_{0,1\text{WL}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \frac{1}{n} Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B})\,, \tag{3.6.64}$$

where $\widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B})$ is defined in (3.5.98).

Proof: The statement of the proposition follows simply by combining (3.6.57), (3.6.63), and Proposition 3.13. □

Since Proposition 3.14 holds for all $n \in \mathbb{N}$, we conclude the following:

Corollary 3.4 *The zero-error quantum capacity of a quantum channel $\mathcal{N}_{A\to B}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the min-geometric unextendible entanglement of $\mathcal{N}_{A\to B}$:*

$$Q_{0,1\text{WL}}(\mathcal{N}) \leq Q_{0,2\text{-EXT}}(\mathcal{N}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}) . \tag{3.6.65}$$

Proof: This is justified as mentioned above. See Appendix 3.C for an alternate proof. □

Remark 3.6 *It is known that forward classical assistance does not increase the zero-error quantum capacity of a quantum channel [BDSW96, BKN00] (see also [KW20, Lemmas 9.6-9.8]). Thus, the quantum capacity of a quantum channel assisted by one-way LOCC superchannels is the same as the quantum capacity of the channel assisted by local operations.*

Remark 3.7 *The zero-error capacities of quantum channels are known to exhibit superactivation [CCHS10, Shi15]. That is, there exist quantum channels, say $\mathcal{N}^1$ and $\mathcal{N}^2$, such that the zero-error capacity of each channel individually is equal to zero, but the zero-error capacity of the tensor-product channel $\mathcal{N}^1 \otimes \mathcal{N}^2$ is strictly positive.*

Note that the subadditivity of the min-geometric unextendible entanglement implies that $\widehat{E}^{u}_{\min}\left(\mathcal{N}^1 \otimes \mathcal{N}^2\right) \leq \widehat{E}^{u}_{\min}\left(\mathcal{N}^1\right) + \widehat{E}^{u}_{\min}\left(\mathcal{N}^2\right)$, which is an upper bound on the zero-error quantum capacity and the zero-error private capacity of the tensor-product channel $\mathcal{N}^1 \otimes \mathcal{N}^2$. Therefore, if a pair of channels is expected to exhibit superactivation of zero-error private capacity or zero-error

quantum capacity, then at least one of the channels should have a strictly positive min-geometric unextendible entanglement.

3.7 Unextendible entanglement of bipartite quantum channels

In this section, we extend our developments on unextendibility to bipartite quantum channels. Bipartite quantum channels are generalizations of point-to-point channels in the sense that every point-to-point channel can be simulated using some bipartite channel by ignoring the input of Bob and the output of Alice; i.e., for every point-to-point quantum channel $\mathcal{N}_{A\to B'}$, there exists a bipartite quantum channel $\mathcal{M}_{AB\to A'B'}$ such that,

$$\mathcal{N}_{A\to B'} = \mathrm{Tr}_{A'} \circ \mathcal{M}_{AB\to A'B'} \circ \mathrm{Tr}_{B}\,. \tag{3.7.1}$$

Before discussing extensions of bipartite quantum channels, we should first establish what we mean by the marginal of a channel in the multipartite case. A quantum channel $\mathcal{N}_{AB_i\to A'B'_i}$ is a marginal of the channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ if the following condition holds [KDWW19]:

$$\mathrm{Tr}_{B'_{[k]\setminus i}} \circ \mathcal{P}_{AB_{[k]}\to A'B'_{[k]}} = \mathcal{N}_{AB_i\to A'B'_i} \otimes \mathrm{Tr}_{B_{[k]\setminus i}}\,. \tag{3.7.2}$$

The Choi operators of the two channels are related as

$$\mathrm{Tr}_{B'_{[k]\setminus i}}\left[\Gamma^{\mathcal{P}}_{AB_{[k]}A'B'_{[k]}}\right] = \Gamma^{\mathcal{N}}_{AB_iA'B'_i} \otimes I_{B_{[k]\setminus i}}. \tag{3.7.3}$$

Unlike the broadcast channels $\mathcal{P}_{A\to B_{[k]}}$ considered in previous sections of this work, not all multipartite channels have a well defined marginal. In fact, a quantum channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ has a well defined marginal $\mathcal{N}_{AB_i\to A'B'_i}$ if and only if it does not allow systems $B_{[k]\setminus i}$ to send any data, quantum or classical, to systems A' and B'_i. Moreover, if there

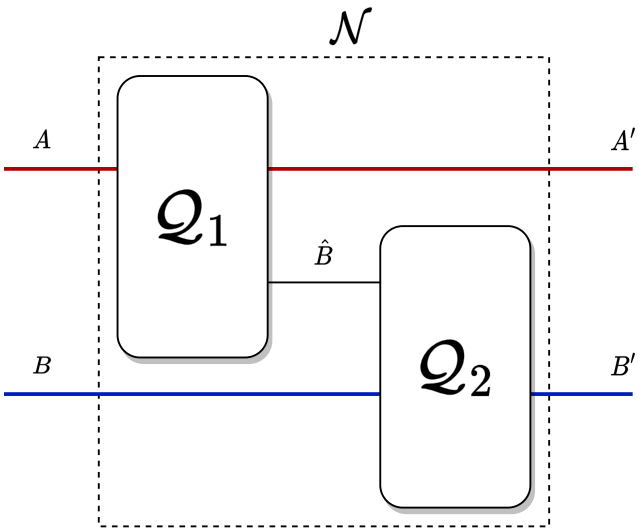


Figure 3.4: Decomposition of a semicausal channel between Alice and Bob that is nonsignaling from Bob to Alice.

exists a marginal channel $\mathcal{N}_{AB_i \to A'B'_i}$ for every $i \in [k]$, the quantum channel $\mathcal{P}_{AB_{[k]} \to A'B'_{[k]}}$ is non-signaling from B_i to A', for every $i \in [k]$.

We restrict our discussion on unextendibility of bipartite quantum channels to semicausal quantum channels between Alice and Bob [BGNP01] that are non-signaling from Bob to Alice. It has been shown that all semicausal channels are semi-localizable [ESW02]. As such, these quantum channels are of the following form (see Figure 3.4):

$$\mathcal{N}_{AB \to A'B'} = \mathcal{Q}^2_{B\hat{B} \to B'} \circ \mathcal{Q}^1_{A \to A'\hat{B}}, \tag{3.7.4}$$

where $\mathcal{Q}^2_{B\hat{B} \to B'}$ and $\mathcal{Q}^1_{A \to A'\hat{B}}$ are quantum channels. This ensures that there always exists an extension of such a channel that is of the form $\mathcal{P}_{AB_{[k]} \to A'B'_{[k]}}$, such that it has a well defined marginal $\mathcal{N}^i_{AB_i \to A'B'_i}$ for every $i \in [k]$. The marginal $\mathcal{N}^i_{AB_i \to A'B'_i}$ can be uniquely obtained from the channel $\mathcal{P}_{AB_{[k]} \to A'B'_{[k]}}$ using the following relation:

$$\mathrm{Tr}_{B'_{[k]\setminus i}} \circ \mathcal{P}_{AB_{[k]} \to A'B'_{[k]}} \circ \mathcal{A}_{B_{[k]\setminus i}} = \mathcal{N}^i_{AB_i \to A'B'_i}, \tag{3.7.5}$$

where $\mathcal{A}_{B_{[k]\setminus i}}$ is a quantum channel that appends an arbitrary quantum state on the systems

$B_{[k]\setminus i}$.

3.7.1 Bipartite k-extendible quantum channels

Let us now define k-extendibility of bipartite quantum channels and superchannels. Multiple definitions of k-extendibility have been proposed for bipartite quantum channels [KDWW19, BBFS21]. In this work, we use the notion of bipartite k-extendible channels presented in [KDWW19, KDWW21].

Definition 3.6 (Bipartite k-extendible channel) *A quantum channel $\mathcal{N}_{AB\to A'B'}$ is k-extendible if there exists a channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ such that the following conditions hold.*

1. *The extended channel is covariant under permutations of the B systems,*

$$\mathcal{W}^{\pi}_{B'_{[k]}} \circ \mathcal{P}_{AB_{[k]}\to A'B'_{[k]}} = \mathcal{P}_{AB_{[k]}\to A'B'_{[k]}} \circ \mathcal{W}^{\pi}_{B_{[k]}} \quad \forall \pi \in \mathcal{S}_k, \tag{3.7.6}$$

   where $\mathcal{W}^{\pi}$ is a permutation unitary channel as defined previously, just after (3.4.5).

2. *The channel $\mathcal{N}_{AB\to A'B'}$ is a marginal of $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$:*

$$\mathrm{Tr}_{B'_{[k]\setminus 1}} \circ \mathcal{P}_{AB_{[k]}\to A'B'_{[k]}} = \mathcal{N}_{AB\to A'B'} \otimes \mathrm{Tr}_{B_{[k]\setminus 1}}. \tag{3.7.7}$$

As a consequence of part 2. of the above definition, it follows that the systems $B_2, B_3, \ldots, B_k$ cannot send any information to the systems A and B_1.

The conditions in (3.7.6) and (3.7.7) can be written as semidefinite constraints on the Choi operator of the quantum channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ as follows [KDWW21, Eqs. (24)–(27)]:

$$\left(\mathcal{W}^{\pi}_{B_{[k]}} \otimes \mathcal{W}^{\pi}_{B'_{[k]}}\right) \Gamma^{\mathcal{P}} = \Gamma^{\mathcal{P}} \quad \forall \pi \in \mathcal{S}_k, \tag{3.7.8}$$

$$\mathrm{Tr}_{B'_{[k]\setminus 1}}\left[\Gamma^{\mathcal{P}}\right] = \Gamma^{\mathcal{N}}_{AB_1A'B'_1} \otimes I_{B_{[k]\setminus 1}}, \tag{3.7.9}$$

where $\Gamma^{\mathcal{N}}_{ABA'B'}$ and $\Gamma^{\mathcal{P}} \equiv \Gamma^{\mathcal{P}}_{AB_{[k]}A'B'_{[k]}}$ are the Choi operators of the quantum channels $\mathcal{N}_{AB\to A'B'}$ and $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$, respectively. It is straightforward to verify that this definition of k-extendibility is consistent with the definition of k-extendibility of point-to-point channels.

It is also worth noting that the unique quantum channel corresponding to a point-to-point superchannel is a bipartite semi-localizable quantum channel. Since the definitions for bipartite k-extendible channels and point-to-point k-extendible superchannels are the same, we can assert that a point-to-point superchannel is k-extendible if and only if the unique bipartite quantum channel associated with it is a k-extendible channel.

The set of bipartite k-extendible quantum channels is a relaxation of the set of bipartite one-way LOCC channels. This can be seen by considering a general bipartite one-way LOCC channel,

$$\mathcal{N}_{AB\to A'B'} = \sum_x \mathcal{E}^x_{A\to A'} \otimes \mathcal{D}^x_{B\to B'}, \tag{3.7.10}$$

where $\left\{\mathcal{E}^x_{A\to A'}\right\}_x$ is a set of completely positive, trace non-increasing maps such that the sum map $\sum_x \mathcal{E}^x_{A\to A'}$ is a quantum channel and $\left\{\mathcal{D}^x_{A\to A'}\right\}_x$ is a set of quantum channels. This is understood to be a one-way LOCC channel as Alice applies the quantum instrument $\left\{\mathcal{E}^x_{A\to A'}\right\}_x$ on her system and sends the classical outcome x to Bob, who then applies the quantum channel $\mathcal{D}^x_{B\to B'}$ on his system based on the classical data he received. We can construct an extension of this channel as follows:

$$\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}} := \sum_x \mathcal{E}^x_{A\to A'} \otimes \mathcal{D}^x_{B_1\to B'_1} \otimes \cdots \otimes \mathcal{D}^x_{B_k\to B'_k}, \tag{3.7.11}$$

because x is classical data that can be copied an arbitrary number of times. Such an extension obeys the permutation covariance and non-signaling conditions stated in (3.7.6) and (3.7.7). Thus, all one-way LOCC bipartite quantum channels are k-extendible for all

$k \geq 2$.

Remark 3.8 *The set of bipartite k-extendible channels as defined in [BBFS21] has been shown to converge to the set of bipartite one-way LOCC channels as $k \to \infty$. However, it is not known if the set of k-extendible channels defined in [KDWW19, KDWW21] converges to the set of bipartite one-way LOCC channels as $k \to \infty$.*

3.7.2 Bipartite k-extendible superchannels

In this section, we discuss the extendibility of bipartite superchannels, and in order to do so, we first establish the notion of marginal superchannels. Let $Q^{\Theta}_{CDA'B' \to C'D'AB}$ and $Q^{\Upsilon}_{CD_{[k]}A'B'_{[k]} \to C'D'_{[k]}AB_{[k]}}$ be the unique quantum channels corresponding to the superchannels $\Theta_{(AB \to A'B') \to (CD \to C'D')}$ and $\Upsilon_{(AB_{[k]} \to A'B'_{[k]}) \to (CD_{[k]} \to C'D'_{[k]})}$, respectively. The superchannel Θ is said to be a marginal of the superchannel Υ if and only if the quantum channel $Q^{\Theta}_{CDA'B' \to C'D'AB}$ is a marginal of the channel $Q^{\Upsilon}_{CD_{[k]}A'B'_{[k]} \to C'D'_{[k]}AB_{[k]}}$; that is,

$$\mathrm{Tr}_{D'_{[k]\setminus i}B_{[k]\setminus i}} \circ Q^{\Upsilon} = Q^{\Theta} \otimes \mathrm{Tr}_{D_{[k]\setminus i}B'_{[k]\setminus i}}. \tag{3.7.12}$$

All bipartite superchannels do not have a well defined marginal. Similar to the case of bipartite channels, we restrict our discussion to such bipartite superchannels $\Theta_{(AB \to A'B') \to (CD \to C'D')}$ for which the associated quantum channel $Q^{\Theta}_{CDA'B' \to C'D'AB}$ is semicausal and does not allow any data to be transmitted from the joint system DB' to the joint system $C'A$. Now that we have defined the marginal of a bipartite superchannel, let us define k-extendible superchannels.

Definition 3.7 (Bipartite k-extendible superchannels) *A bipartite superchannel $\Theta_{(AB \to A'B') \to (CD \to C'D')}$*

is k-extendible if there exists a superchannel $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$ *such that the following conditions hold for the unique quantum channels,* $Q^{\Theta}_{CDA'B'\to C'D'AB}$ *and* $Q^{\Upsilon}_{CD_{[k]}A'B'_{[k]}\to C'D'_{[k]}AB_{[k]}}$*, of the superchannels* Θ *and* Υ*, respectively.*

1. *Permutation covariance:*

$$Q^{\Upsilon}\circ\left(\mathcal{W}^{\pi}_{D_{[k]}}\otimes\mathcal{W}^{\pi}_{B'_{[k]}}\right)=\left(\mathcal{W}^{\pi}_{D'_{[k]}}\otimes\mathcal{W}^{\pi}_{B_{[k]}}\right)\circ Q^{\Upsilon}\quad\forall\pi\in S_k. \tag{3.7.13}$$

2. *Non-signaling:*

$$\mathrm{Tr}_{D'_{[k]\setminus 1}}\circ Q^{\Upsilon}=\mathrm{Tr}_{D'_{[k]\setminus 1}}\circ Q^{\Upsilon}\circ\mathcal{R}_{B'_{[k]\setminus 1}}, \tag{3.7.14}$$

   where $\mathcal{R}$ *is a quantum channel that traces out the input and replaces with an arbitrary quantum state.*

3. *Marginality:*

$$\mathrm{Tr}_{B_{[k]\setminus 1}D'_{[k]\setminus 1}}\circ Q^{\Upsilon}=Q^{\Theta}_{CDA'B'\to C'D'AB}\otimes\mathrm{Tr}_{B'_{[k]\setminus 1}D_{[k]\setminus 1}}. \tag{3.7.15}$$

The conditions in (3.7.13), (3.7.14), and (3.7.15) can be written as semidefinite constraints on the Choi operators of the superchannels Θ and Υ as

$$\left(\mathcal{W}^{\pi}_{D'_{[k]}}\otimes\mathcal{W}^{\pi}_{B_{[k]}}\otimes\mathcal{W}^{\pi}_{D_{[k]}}\otimes\mathcal{W}^{\pi}_{B'_{[k]}}\right)\left(\Gamma^{\Upsilon}\right)=\Gamma^{\Upsilon}\quad\forall\pi\in S_k, \tag{3.7.16}$$

$$\mathrm{Tr}_{D'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]=\mathrm{Tr}_{D'_{[k]\setminus 1}B'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]\otimes\frac{I_{B'_{[k]\setminus 1}}}{|B'|^{k-1}}, \tag{3.7.17}$$

$$\mathrm{Tr}_{B_{[k]\setminus 1}D'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]=\Gamma^{\Theta}\otimes I_{B'_{[k]\setminus 1}D_{[k]\setminus 1}}, \tag{3.7.18}$$

where $|B'|$ is the dimension of the system B' and Γ^{Θ} and Γ^{Υ} are the Choi operators of the quantum channels Q^{Θ} and Q^{Υ}, respectively.

Proposition 3.15 *Let $\Theta_{(AB\to A'B')\to(CD\to C'D')}$ be a k-extendible superchannel with the k-extension $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$. Then each marginal of the channel obtained by acting with the superchannel Υ on a channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ is the same as the channel obtained by acting with the superchannel Θ on the respective marginal of the channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$. That is,*

$$\mathrm{Tr}_{D'_{[k]\setminus i}} \circ (\Upsilon(\mathcal{P})) = \Theta\left(\mathrm{Tr}_{B'_{[k]\setminus i}} \circ \mathcal{P} \circ \mathcal{A}_{B_{[k]\setminus i}}\right) \otimes \mathrm{Tr}_{D_{[k]\setminus i}} \quad \forall i \in [k]. \tag{3.7.19}$$

Proof: See Appendix 3.D. □

Proposition 3.16 *The channel formed by applying a k-extendible superchannel on a k-extendible quantum channel is also a k-extendible quantum channel.*

Proof: See Appendix 3.E. □

Proposition 3.17 *All bipartite superchannels that can be realized by local operations and one-way classical communication are k-extendible for all $k \geq 2$.*

Proof: See Appendix 3.F. □

3.7.3 Unextendible entanglement of bipartite quantum channels

With the notion of k-extendibility established for bipartite quantum channels and superchannels, we can now look for a measure to quantify the unextendibility of a bipartite quantum channel. Let us first define the following set of extensions of a bipartite channel

$\mathcal{N}_{AB\to A'B'}$:

$$\text{Ext}(\mathcal{N}) := \left\{ \begin{array}{c} \mathcal{P}_{AB_1B_2\to A'B'_1B'_2} : \\ \mathcal{N}_{AB\to A'B'} = \text{Tr}_{B'_2} \circ \mathcal{P}_{AB_1B_2\to A'B'_1B'_2} \circ \mathcal{A}_{B_2}, \\ \text{Tr}_{B'_1} \circ \mathcal{P} = \text{Tr}_{B'_1} \circ \mathcal{P} \circ \mathcal{R}_{B_1} \end{array} \right\}, \tag{3.7.20}$$

where $\mathcal{A}$ is a channel that appends an arbitrary state and $\mathcal{R}$ is a channel that traces out the input and replaces it with an arbitrary state. The generalized unextendible entanglement of a bipartite channel is defined as follows.

Definition 3.8 *The generalized unextendible entanglement of a bipartite quantum channel is defined for a generalized divergence between quantum channels,* $\mathbf{D}$*, as follows:*

$$\mathbf{E}^u(\mathcal{N}_{AB\to A'B'}) = \frac{1}{2} \inf_{\mathcal{P}_{AB_1B_2\to A'B'_1B'_2} \in \text{Ext}(\mathcal{N})} \left\{ \begin{array}{c} \mathbf{D}(\mathcal{N}_{AB\to A'B'} \| \mathcal{M}_{AB\to A'B'}) : \\ \mathcal{N}_{AB\to A'B'} = \text{Tr}_{B'_2} \circ \mathcal{P}_{AB_1B_2\to A'B'_1B'_2} \circ \mathcal{A}_{B_2}, \\ \mathcal{M}_{AB\to A'B'} = \text{Tr}_{B'_1} \circ \mathcal{P}_{AB_1B_2\to A'B'_1B'_2} \circ \mathcal{A}_{B_1} \end{array} \right\}, \tag{3.7.21}$$

As is evident from the definition, the minimum value of the generalized unextendible entanglement is achieved for a two-extendible quantum channel. If the underlying divergence is strongly faithful, then the unextendible entanglement of a bipartite quantum channel is equal to zero if and only if the channel is two-extendible. We also find that the action of a two-extendible superchannel on a bipartite quantum channel cannot increase the unextendible entanglement of the said channel.

Theorem 3.7 (Monotonicity) *The generalized unextendible entanglement of a bipartite quantum channel does not increase under the action of a two-extendible superchannel. That is, for an arbitrary bipartite quantum channel* $\mathcal{N}_{AB\to A'B'}$ *and a two-extendible superchannel* $\Theta_{(AB\to A'B')\to(CD\to C'D')}$*,*

$$\mathbf{E}^u(\mathcal{N}_{AB\to A'B'}) \geq \mathbf{E}^u(\Theta(\mathcal{N}_{AB\to A'B'})). \tag{3.7.22}$$

Proof: Monotonicity of generalized unextendible entanglement of bipartite channels under two-extendible superchannels follows from similar arguments as given in the proof of Theorem 3.5. See Appendix 3.G for a complete proof. □

Proposition 3.15 allows us to generalize the statement of Theorem 3.6 to bipartite semicausal channels, which we state as Theorem 3.8.

Theorem 3.8 *The unextendible entanglement of a quantum state $\sigma_{R_C C' C'' R_D D' D''}$, with respect to the partition $R_C C' C'' : R_D D' D''$, that can be established between two parties using a bipartite semicausal channel $\mathcal{N}_{AB\to A'B'}$, a bipartite two-extendible superchannel $\Theta_{(AB\to A'B')\to(CD\to C'C''D'D'')}$, and any two-extendible state $\rho_{R_C C' R_D D'}$, is not greater than the unextendible entanglement of the quantum channel $\mathcal{N}_{AB\to A'B'}$; that is,*

$$\sup_{\rho\in 2\text{-EXT}(R_C C:R_D D)} \mathbf{E}^u(\sigma_{R_C C' C'':R_D D' D''}) \leq \mathbf{E}^u(\mathcal{N}_{AB\to A'B'}), \tag{3.7.23}$$

where 2-EXT$(S_A : S_B)$ *is the set of two-extendible states with respect to systems S_A and S_B, and*

$$\sigma_{R_C C' C'' R_D D' D''} := (\Theta(\mathcal{N}_{AB\to A'B'}))(\rho_{R_C C R_D D}). \tag{3.7.24}$$

Proof: The proof follows the same line of reasoning as the proof of Theorem 3.6. We present a complete proof in Appendix 3.H. □

α-geometric unextendible entanglement of bipartite quantum channels

We have seen that the α-geometric Rényi relative entropies offer several desirable properties when used as the underlying divergence for defining unextendible entanglement

of point-to-point quantum channels. Here we define the α-geometric unextendible entanglement of a bipartite quantum channel $\mathcal{N}_{AB\to A'B'}$ as

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{AB\to A'B'}) \coloneqq \frac{1}{2}\inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})}\sup_{\psi_{RAB}}\left\{\begin{array}{c}\widehat{D}_{\alpha}(\mathcal{N}(\psi_{RAB})\,\|\mathcal{M}(\psi_{RAB})) : \\ \mathcal{N} = \mathrm{Tr}_{B_2'}\circ\mathcal{P}_{AB_1B_2\to A'B_1'B_2'}\circ\mathcal{A}_{B_2}, \\ \mathcal{M} = \mathrm{Tr}_{B_1'}\circ\mathcal{P}_{AB_1B_2\to A'B_1'B_2'}\circ\mathcal{A}_{B_1}\end{array}\right\}, \tag{3.7.25}$$

for all $\alpha \in (0,1)\cup(1,2]$.

Several properties of the α-geometric unextendible entanglement of point-to-point channels hold for the α-geometric unextendible entanglement of bipartite quantum channels as well. Since the input and output systems of point-to-point channels can be considered to have multiple subsystems, the following properties trivially extend from the α-geometric unextendible entanglement of point-to-point quantum channels to the α-geometric unextendible entanglement of bipartite quantum channels.

1. The α-geometric unextendible entanglement of a bipartite channel increases monotonically with α.
2. The smallest quantity in the family of α-geometric unextendible entanglement is induced by the α-geometric Rényi relative entropy when $\alpha \to 0$, and is called the min-geometric unextendible entanglement of the channel,

$$\widehat{E}^{u}_{\min}(\mathcal{N}_{AB\to A'B'}) \coloneqq \lim_{\alpha\to 0^+}\widehat{E}^{u}_{\alpha}(\mathcal{N}_{AB\to A'B'}) \tag{3.7.26}$$

$$= \frac{1}{2}\inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})}\lim_{\alpha\to 0^+}\widehat{D}_{\alpha}\Big(\mathcal{N}\|\,\mathrm{Tr}_{B_1'}\circ\mathcal{P}\circ\mathcal{A}_{B_1}\Big). \tag{3.7.27}$$

3. The α-geometric unextendible entanglement converges to the unextendible entanglement induced by the Belavkin–Staszewski relative entropy as $\alpha \to 1$,

$$\widehat{E}^{u}(\mathcal{N}_{AB\to A'B'}) \coloneqq \lim_{\alpha\to 1}\widehat{E}^{u}_{\alpha}(\mathcal{N}_{AB\to A'B'}) \tag{3.7.28}$$

$$= \frac{1}{2}\inf_{\mathcal{P}\in\mathrm{Ext}(\mathcal{N})}\lim_{\alpha\to 1}\widehat{D}_{\alpha}\Big(\mathcal{N}\|\,\mathrm{Tr}_{B_1'}\circ\mathcal{P}\circ\mathcal{A}_{B_1}\Big). \tag{3.7.29}$$

4. The α-geometric unextendible entanglement is subadditive under tensor products of bipartite quantum channels; that is,

$$\widehat{E}^u_\alpha(\mathcal{N}\otimes\mathcal{M}) \leq \widehat{E}^u_\alpha(\mathcal{N}) + \widehat{E}^u_\alpha(\mathcal{M})\,. \tag{3.7.30}$$

One would expect an unextendible bipartite channel to have the ability to boost the unextendibility of a bipartite state. The α-geometric Rényi relative entropy follows the chain rule $\forall\alpha\in(0,1)\cup(1,2]$ [KW21, Proposition 45],

$$\widehat{D}_\alpha(\mathcal{N}(\rho)\,\|\mathcal{M}(\sigma)) \leq \widehat{D}_\alpha(\mathcal{N}\|\mathcal{M}) + \widehat{D}_\alpha(\rho\|\sigma)\,, \tag{3.7.31}$$

which allows us to quantify the effect of an unextendible bipartite channel on the unextendibility of a bipartite state, as seen from the theorem below.

Theorem 3.9 *A bipartite quantum channel $\mathcal{N}_{AB\to A'B'}$ cannot increase the α-geometric unextendible entanglement of a bipartite state ρ_{AB} by more than the α-geometric unextendible entanglement of the channel itself; that is, for all $\alpha\in(0,1)\cup(1,2]$,*

$$\widehat{E}^u_\alpha(\mathcal{N}_{AB\to A'B'}(\rho_{AB})) \leq \widehat{E}^u_\alpha(\rho_{AB}) + \widehat{E}^u_\alpha(\mathcal{N}_{AB\to A'B'})\,. \tag{3.7.32}$$

Proof: Consider a bipartite quantum channel $\mathcal{N}_{AB\to A'B'}$ and a quantum state ρ_{AB}. Let $\mathcal{P}_{AB_1B_2\to A'B'_1B'_2}$ be an extension of the channel $\mathcal{N}_{AB\to A'B'}$ in the set $\mathrm{Ext}\,(\mathcal{N})$ defined in (3.7.20), and let $\sigma_{AB_1B_2}$ be an arbitrary extension of the quantum state ρ_{AB}. By the definition of α-geometric unextendible entanglement of states,

$$\widehat{E}^u_\alpha(\mathcal{N}_{AB\to A'B'}(\rho_{AB})) \leq \frac{1}{2}\widehat{D}_\alpha\Big(\mathcal{N}(\rho_{AB})\,\|\,\mathrm{Tr}_{B'_1}\circ\mathcal{P}(\sigma)\Big) \tag{3.7.33}$$

$$= \frac{1}{2}\widehat{D}_\alpha\Big(\mathcal{N}(\rho_{AB})\,\|\,\mathrm{Tr}_{B'_1}\circ\mathcal{P}\circ\mathcal{A}_{B_1}(\mathrm{Tr}_{B_1}[\sigma])\Big) \tag{3.7.34}$$

$$\leq \frac{1}{2}\left\{\widehat{D}_\alpha(\rho\big\|\mathrm{Tr}_{B_1}[\sigma]) + \widehat{D}_\alpha\Big(\mathcal{N}\Big\|\mathrm{Tr}_{B'_1}\circ\mathcal{P}\circ\mathcal{A}_{B_1}\Big)\right\}, \tag{3.7.35}$$

where the equality follows from the definition of Ext($\mathcal{N}$) in (3.7.20) and the second inequality follows from the chain rule of α-geometric Rényi relative entropy given in (3.7.31). Since the inequality in (3.7.35) holds for every quantum channel $\mathcal{P}_{AB_1B_2\to A'B_1'B_2'}$ in Ext($\mathcal{N}$) and every extension $\sigma_{AB_1B_2}$ of the state ρ_{AB}, we can take an infimum over all such channels $\mathcal{P}_{AB_1B_2\to A'B_1'B_2'}$ and states $\sigma_{AB_1B_2}$, and conclude (3.7.32). □

3.8 Applications of the unextendible entanglement of bipartite quantum channels

In this section, we discuss some applications of the unextendible entanglement of bipartite quantum channels. Bipartite quantum channels can be used to increase the entanglement in a shared bipartite quantum state, hence increasing the distillable entanglement and distillable key of the state. In Section 3.8.1, we give an upper bound on the expected rate of distilling ebits probabilistically from a bipartite quantum state using a bipartite quantum channel assisted by one-way LOCC or two-extendible superchannels, and in Section 3.8.2, we give an upper bound on the rate of distilling exact secret bits probabilistically from a bipartite quantum state using a bipartite quantum channel assisted by one-way LOCC or two-extendible superchannels.

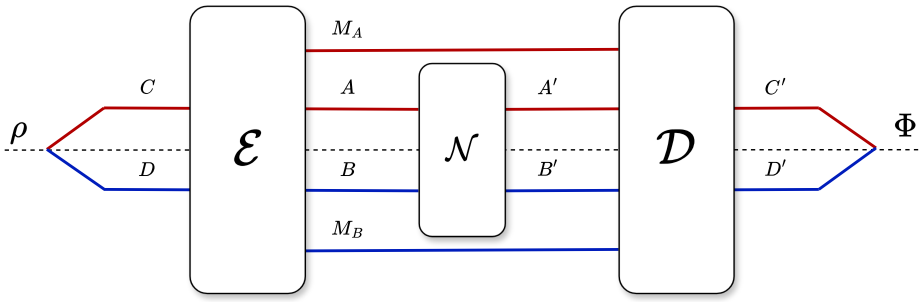


Figure 3.5: Protocol to distill a maximally entangled state $\Phi_{C'D'}$ from a bipartite quantum state ρ_{CD}, a bipartite channel $\mathcal{N}_{AB\to A'B'}$, and one-way LOCC pre-processing and post-processing channels $\mathcal{E}_{CD\to AM_ABM_B}$ and $\mathcal{D}_{A'M_AB'M_B\to C'D'}$, respectively. The dotted line represents the separation between Alice and Bob's labs. All systems above the dotted line are held by Alice and all systems below the dotted line are held by Bob.

3.8.1 One-way distillable entanglement of a quantum state-channel pair

The distillable entanglement of a bipartite quantum state under a restricted set of operations has been a subject of interest in quantum information theory. In quantum communication theory, the number of ebits that can be distilled from an existing bipartite state under local operations and one-way classical communication as well as two-way classical communication is of special interest due to state-of-the-art classical networks available to us.

An upper bound on the probabilistic one-way distillable entanglement of a bipartite quantum state has been established in [WWW24]. In this section, we consider a more general setting where the two distant parties, Alice and Bob, hold a bipartite quantum state ρ_{CD}, and also have access to a semicausal bipartite quantum channel $\mathcal{N}_{AB\to A'B'}$ that is not necessarily simulable by local operations and one-way classical communication. Alice and Bob can encode the available quantum state ρ_{CD} using a one-way LOCC channel $\mathcal{E}_{CD\to AB}$, and then transform the encoded state using the quantum channel $\mathcal{N}_{AB\to A'B'}$ fol-

lowed by a one-way LOCC decoding channel $\mathcal{D}_{A'B'\to C'D'}$ to distill a maximally entangled state (see Figure 3.5). As such, the channel $\mathcal{N}_{AB\to A'B'}$ can be used to boost the amount of entanglement that can be distilled probabilistically, or deterministically, from the shared bipartite state using one-way LOCC.

A simple example of a semicausal channel that is useful for probabilistic distillation of entanglement is the following channel:

$$\mathcal{N}_{A\to A'B}(\rho_{RA}) = p\rho_{RA'} \otimes |e\rangle\langle e|_B + (1-p)\rho_{RB} \otimes |e\rangle\langle e|_{A'}, \tag{3.8.1}$$

where $|e\rangle\langle e|_S$ is the erasure symbol, which is orthogonal to every state in the Hilbert space of system S. This is a channel where Alice and Bob share an erasure channel with erasure probability p, and the output of the complementary channel is received by Alice herself; as such, nothing is lost to the environment. Alice can send one share of a maximally entangled state to Bob using the channel $\mathcal{N}_{A\to A'B}$, and then she can measure if the state she received back was erased or not by applying the POVM $\{\Pi_{A'}, |e\rangle\langle e|_{A'}\}$, where $\Pi_{A'}$ is the projection onto the entire Hilbert space of system A'. If Alice measures her system to be erased, she knows that a maximally entangled state has been established between her and Bob, hence, distilling a maximally entangled state with probability $1-p$.

Probabilistic one-way distillable entanglement

Let us first consider a probabilistic setting in which an entanglement distillation protocol distills a maximally entangled state of Schmidt rank d with some probability p. The expected number of ebits distilled by this protocol is given by $p\log_2 d$. Alice and Bob use one instance of the quantum channel $\mathcal{N}_{AB\to A'B'}$ and a one-way LOCC superchannel $\Theta_{(AB\to A'B')\to(CD\to C'D')}$ to distill a maximally entangled state of Schmidt rank d from a bipartite

quantum state ρ_{CD} with probability p. The action of this protocol can be mathematically described as follows:

$$(\Theta(\mathcal{N}))(\rho) = p|1\rangle\langle 1|_X \otimes \Phi^d_{C'D'} + (1-p)|0\rangle\langle 0|_X \otimes \sigma_{C'D'}, \tag{3.8.2}$$

where system X is held by Alice. We define the probabilistic one-way distillable entanglement of the quantum state-channel pair $(\rho_{CD}, \mathcal{N}_{AB\to A'B'})$ as follows:

$$\widetilde{E}_{D,1\text{WL}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) \coloneqq \sup_{\substack{p\in[0,1], d\in\mathbb{N}, \\ \Theta\in 1\text{WL}}} \left\{ \begin{array}{c} p\log_2 d : \\ (\Theta(\mathcal{N}))(\rho) = p|1\rangle\langle 1|_X \otimes \Phi^d_{C'D'} \\ +(1-p)|0\rangle\langle 0|_X \otimes \sigma_{C'D'}, \\ \sigma \in \mathcal{S}(C'D') \end{array} \right\}. \tag{3.8.3}$$

We can also define the probabilistic two-extendible distillable entanglement of a quantum state-channel pair by relaxing the set of allowed superchannels to the set of two-extendible superchannels:

$$\widetilde{E}_{D,2\text{-EXT}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) \coloneqq \sup_{\substack{p\in[0,1], d\in\mathbb{N}, \\ \Theta\in 2\text{-EXT}}} \left\{ \begin{array}{c} p\log_2 d : \\ (\Theta(\mathcal{N}))(\rho) = p|1\rangle\langle 1|_X \otimes \Phi^d_{C'D'} \\ +(1-p)|0\rangle\langle 0|_X \otimes \sigma_{C'D'}, \\ \sigma \in \mathcal{S}(C'D') \end{array} \right\}. \tag{3.8.4}$$

Since the set of one-way LOCC superchannels lies inside the set of two-extendible superchannels, the following inequality holds for every bipartite state ρ_{CD} and bipartite channel $\mathcal{N}_{AB\to A'B'}$:

$$\widetilde{E}_{D,2\text{-EXT}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) \geq \widetilde{E}_{D,1\text{WL}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}). \tag{3.8.5}$$

Proposition 3.18 *The expected rate at which ebits can be probabilistically distilled from a bipartite quantum state ρ_{CD} and n instances of a quantum channel $\mathcal{N}_{AB\to A'B'}$, assisted by one-way LOCC*

superchannels or two-extendible superchannels, is bounded from above as follows:

$$\frac{1}{n}\widetilde{E}_{D,1\text{WL}}(\rho,\mathcal{N}^{\otimes n}) \leq \frac{1}{n}\widetilde{E}_{D,2\text{-EXT}}(\rho,\mathcal{N}^{\otimes n}) \leq \frac{1}{n}\widehat{E}^{u}(\rho_{CD}) + \widehat{E}^{u}(\mathcal{N}_{AB\to A'B'}), \tag{3.8.6}$$

where $\widehat{E}^{u}(\rho_{CD})$ *is the unextendible entanglement of the quantum state* ρ_{CD} *induced by the Belavkin–Staszewski relative entropy (defined in* (3.5.37)*), and* $\widehat{E}^{u}(\mathcal{N}_{AB\to A'B'})$ *is the unextendible entanglement of the quantum channel* $\mathcal{N}_{AB\to A'B'}$ *induced by the Belavkin–Staszewski relative entropy (defined in* (3.7.29)*).*

Proof: Let ρ_{CD} be a quantum state shared between Alice (holding system C) and Bob (holding system D). Let $\Theta_{(A^nB^n\to A'^nB'^n)\to(CD\to C'D')}$ be a two-extendible superchannel such that it acts on n instances of a quantum channel $\mathcal{N}_{AB\to A'B'}$, and the resultant channel consumes the quantum state ρ_{AB} to generate a maximally entangled state of Schmidt rank d with probability p. This process can be mathematically described as,

$$(\Theta(\mathcal{N}^{\otimes n}))(\rho_{CD}) = p|1\rangle\langle 1|_X \otimes \Phi^{d}_{C'D'} + (1-p)|0\rangle\langle 0|_X \otimes \sigma_{C'D'}, \tag{3.8.7}$$

where $\sigma_{C'D'}$ is an arbitrary bipartite state and system X is held by Alice.

Recall that the α-geometric uenxtendible entanglement of the maximally entangled state $\Phi^{d}_{C'D'}$ is equal to $\log_2 d$ as mentioned in Theorem 3.4. The direct-sum property in Proposition 3.7 then implies that the α-geometric unextendible entanglement of the quantum state described in (3.8.7) is no less than $p\log_2 d$ for all $\alpha \in (1,2]$. Therefore,

$$p\log_2 d \leq \widehat{E}^{u}_{\alpha}(\Theta(\mathcal{N}^{\otimes n})(\rho)) \tag{3.8.8}$$

$$\leq \widehat{E}^{u}_{\alpha}(\Theta(\mathcal{N}^{\otimes n})) + \widehat{E}^{u}_{\alpha}(\rho) \tag{3.8.9}$$

$$\leq n\widehat{E}^{u}_{\alpha}(\mathcal{N}_{AB\to A'B'}) + \widehat{E}^{u}_{\alpha}(\rho_{CD}), \tag{3.8.10}$$

where the second inequality follows from Theorem 3.9, and the final inequality follows from the monotonicity of unextendible entanglement under the action of two-extendible

superchannels (Theorem 3.7) and subadditivity of α-geometric unextendible entanglement under tensor product of quantum channels (Proposition 3.8). We can take the limit $\alpha \to 1$ to get the tightest upper bound using this technique. Since the above inequality is true for all values of p, every dimension d, and every two-extendible superchannel Θ, we can take a supremum over all of these quantities and conclude (3.8.6). □

Exact one-way distillable entanglement

We can consider a special case of the probabilistic one-way distillable entanglement by demanding that the maximally entangled state is distilled deterministically. This means that Alice and Bob use a quantum state ρ_{CD} and n instances of a quantum channel $\mathcal{N}_{AB\to A'B'}$ along with local operations and unbounded forward classical communication from Alice to Bob to deterministically distill the maximum number of ebits possible. We define the exact one-way distillable entanglement of a state-channel pair $(\rho_{CD}, \mathcal{N}_{AB\to A'B'})$ as follows:

$$\widetilde{E}^{e}_{D,1\text{WL}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) := \sup_{d\in\mathbb{N},\Theta\in 1\text{WL}} \left\{ \begin{array}{c} \log_2 d : \\ (\Theta(\mathcal{N}))(\rho) = \Phi^{d}_{C'D'} \end{array} \right\}. \tag{3.8.11}$$

We can relax the set of allowed superchannels to the set of two-extendible superchannels and define the exact two-extendible distillable entanglement of a state-channel pair as follows:

$$\widetilde{E}^{e}_{D,2\text{-EXT}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) := \sup_{d\in\mathbb{N},\Theta\in 2\text{-EXT}} \left\{ \begin{array}{c} \log_2 d : \\ (\Theta(\mathcal{N}))(\rho) = \Phi^{d}_{C'D'} \end{array} \right\}. \tag{3.8.12}$$

Proposition 3.19 *The rate at which ebits can be deterministically distilled from a bipartite quantum state ρ_{CD} and n instances of a quantum channel $\mathcal{N}_{AB\to A'B'}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the following quantity:*

$$\frac{1}{n}\widetilde{E}^{e}_{D,1\text{WL}}(\rho, \mathcal{N}^{\otimes n}) \leq \frac{1}{n}\widetilde{E}^{e}_{D,2\text{-EXT}}(\rho, \mathcal{N}^{\otimes n}) \tag{3.8.13}$$

$$\leq \frac{1}{n}\widehat{E}^{u}_{\min}(\rho_{CD}) + \widehat{E}^{u}_{\min}(\mathcal{N}_{AB\to A'B'})\,, \tag{3.8.14}$$

where $\widehat{E}^{u}_{\min}(\rho_{CD})$ *is the min-unextendible entanglement of the quantum state* ρ_{CD} *(defined in* (3.5.39)*) and* $\widehat{E}^{u}_{\min}(\mathcal{N}_{AB\to A'B'})$ *is the min-geometric unextendible entanglement of the quantum channel* $\mathcal{N}_{AB\to A'B'}$ *(defined in* (3.7.27)*).*

Proof: The proof follows from the same line of reasoning as the proof of Proposition 3.18. Since we do not need the direct-sum property of the α-geometric unextendible entanglement of states in the determinstic distillation case, we can take the limit $\alpha \to 0^{+}$ and arrive at (3.8.14). □

Remark 3.9 *In the asymptotic limit, the expected rate at which perfect ebits can be distilled from a quantum state* ρ_{CD} *and an arbitrarily large number of instances of the quantum channel* $\mathcal{N}_{AB\to A'B'}$*, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the unextendible entanglement of the quantum channel induced by the Belavkin–Staszewski relative entropy, and the rate of exact one-way distillable entanglement is upper bounded by the min-geometric unextendible entanglement of the channel; i.e.,*

$$\liminf_{n\to\infty} \frac{1}{n}\widetilde{E}_{d,1\mathrm{WL}}(\rho, \mathcal{N}^{\otimes n}) \leq \widehat{E}^{u}(\mathcal{N}_{AB\to A'B'})\,, \tag{3.8.15}$$

$$\liminf_{n\to\infty} \frac{1}{n}\widetilde{E}_{d,e,1\mathrm{WL}}(\rho, \mathcal{N}^{\otimes n}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{AB\to A'B'})\,. \tag{3.8.16}$$

The above inequalities follow from the fact that the α*-geometric unextendible entanglement of a quantum state is finite. As we take the limit* $n \to \infty$*, the quantities* $\frac{1}{n}\widehat{E}^{u}(\rho_{CD})$ *and* $\frac{1}{n}\widehat{E}^{u}_{\min}(\rho_{CD})$ *approach zero for every state* ρ_{CD}*, yielding the above inequalities.*

3.8.2 Distillable key of a quantum state-channel pair

In this section we consider the task of distilling secret keys from a bipartite quantum state and multiple instances of an unextendible quantum channel. It has been shown in [WWW24, Corollary 22] that the α-geometric unextendible entanglement of a bipartite quantum state serves as an upper bound on the number of secret bits that can be distilled from the quantum state using one-way LOCC or two-extendible channels for all $\alpha \in (0, 2]$. A no-go theorem for probabilistic secret-key distillation from a bipartite state was given in [SW24] using the unextendible entanglement of the state induced by the min-relative entropy [Dat09]. We extend these results to give an upper bound on the number of exact secret key bits that can be distilled from a bipartite quantum state and an unextendible quantum channel, assisted by local operations and one-way classical communication.

Probabilistic one-way distillable key

Let us first look at the probabilistic setting in which a secret key is established between Alice and Bob using a quantum state ρ_{CD} and a quantum channel $\mathcal{N}_{AB\to A'B'}$ assisted by local operations and one-way classical communication from Alice to Bob. Similar to the formalism in Section 3.6.1, we utilize the fact that distilling a secret key of $\log_2 K$ bits is equivalent to distilling a bipartite private state $\gamma^K_{C'D'C''D''}$ holding $\log_2 K$ bits of secrecy when local operations are allowed for free [HHHO05, HHHO09] (see Section 3.6.1 for details). We define the probabilistic one-way distillable key of a quantum state-channel

pair $(\rho_{CD}, \mathcal{N}_{AB\to A'B'})$ as

$$\widetilde{K}_{\text{1WL}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) := \sup_{\substack{\gamma^K_{C'D'C''D''}\in\mathcal{K},\\ p\in[0,1],\Theta\in\text{1WL}}} \left\{ \begin{array}{c} p\log_2 K : \\ (\Theta(\mathcal{N}))(\rho) = p|1\rangle\langle 1|_X \otimes \gamma^K_{C'D'C''D''} \\ +(1-p)|0\rangle\langle 0|_X \otimes \sigma_{C'D'C''D''}, \\ \sigma \in \mathcal{S}(C'D'C''D'') \end{array} \right\}. \tag{3.8.17}$$

Once again, we can relax the set of allowed superchannels to the set of two-extendible superchannels and define the probabilistic two-extendible distillable key of a quantum state-channel pair as follows:

$$\widetilde{K}_{\text{2-EXT}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) := \sup_{\substack{\gamma^K_{C'D'C''D''}\in\mathcal{K},\\ p\in[0,1],\Theta\in\text{2-EXT}}} \left\{ \begin{array}{c} p\log_2 K : \\ (\Theta(\mathcal{N}))(\rho) = p|1\rangle\langle 1|_X \otimes \gamma^K_{C'D'C''D''} \\ +(1-p)|0\rangle\langle 0|_X \otimes \sigma_{C'D'C''D''}, \\ \sigma \in \mathcal{S}(C'D'C''D'') \end{array} \right\}. \tag{3.8.18}$$

Proposition 3.20 *The expected rate at which secret bits can be probablistically distilled between Alice and Bob from a bipartite state ρ_{CD} and n instances of a bipartite channel $\mathcal{N}_{AB\to A'B'}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above as follows:*

$$\begin{aligned} \frac{1}{n}\widetilde{K}_{\text{1WL}}(\rho, \mathcal{N}^{\otimes n}) &\leq \frac{1}{n}\widetilde{K}_{\text{2-EXT}}(\rho, \mathcal{N}^{\otimes n}) \\ &\leq \frac{1}{n}\widehat{E}^u(\rho_{CD}) + \widehat{E}^u(\mathcal{N}_{AB\to A'B'}). \end{aligned} \tag{3.8.19}$$

Proof: The proof is similar to the proof of Proposition 3.18. The only difference is that we use the fact that the α-geometric unextendible entanglement of a bipartite private state is no less than the number of secret bits held by the private state, for all $\alpha \in (0, 2]$ [WWW24, Corollary 22]. □

Exact one-way distillable key

We now look at a deterministic protocol to distill a secret key from a bipartite state using a quantum channel assisted by local operations and forward classical communication. Alice and Bob use n instances of a bipartite quantum channel $\mathcal{N}_{AB\to A'B'}$ assisted by a one-way LOCC superchannel $\Theta_{(A^nB^n\to A'^mB'^m)\to(CD\to C'D'C''D'')}$ to transform the existing bipartite quantum state ρ_{CD} to a bipartite private state $\gamma^K_{C'D'C''D''}$ holding $\log_2 K$ secret bits:

$$(\Theta(\mathcal{N}^{\otimes n}_{AB\to A'B'}))(\rho_{CD}) = \gamma^K_{C'D'C''D''}. \tag{3.8.20}$$

The exact one-way distillable key of a quantum state-channel pair $(\rho_{CD}, \mathcal{N}_{AB\to A'B'})$ is defined as

$$\widetilde{K}^e_{\text{1WL}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) := \sup_{\substack{\gamma^K_{C'D'C''D''}\in\mathcal{K},\\ \Theta\in\text{1WL}}} \left\{ \begin{array}{c} \log_2 K : \\ (\Theta(\mathcal{N}))(\rho) = \gamma^K_{C'D'C''D''} \end{array} \right\}. \tag{3.8.21}$$

Relaxing the set of allowed superchannels to the set of two-extendible superchannels, we define the the exact two-extendible distillable key of a quantum state-channel pair as follows:

$$\widetilde{K}^e_{\text{2-EXT}}(\rho_{CD}, \mathcal{N}_{AB\to A'B'}) := \sup_{\substack{\gamma^K_{C'D'C''D''}\in\mathcal{K},\\ \Theta\in\text{2-EXT}}} \left\{ \begin{array}{c} \log_2 K : \\ (\Theta(\mathcal{N}))(\rho) = \gamma^K_{C'D'C''D''} \end{array} \right\}. \tag{3.8.22}$$

Proposition 3.21 *The rate at which exact secret bits can be exactly distilled from a quantum state-channel pair, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the following quantity:*

$$\frac{1}{n}\widetilde{K}^e_{\text{1WL}}(\rho, \mathcal{N}^{\otimes n}) \leq \frac{1}{n}\widetilde{K}^e_{\text{2-EXT}}(\rho, \mathcal{N}^{\otimes n}) \tag{3.8.23}$$

$$\leq \frac{1}{n}\widehat{E}^u_{\min}(\rho_{CD}) + \widehat{E}^u_{\min}(\mathcal{N}_{AB\to A'B'}). \tag{3.8.24}$$

Proof: The proof follows from the same arguments used in the proof of Proposition 3.19, and using the fact that the α-geometric unextendible entanglement of a bipartite state holding $\log_2 K$ secret bits is no less than $\log_2 K$ [WWW24, Corollary 22] for all $\alpha \in (0, 2]$. □

Remark 3.10 *Since the α-geometric unextendible entanglement of a quantum state is finite, the expected rate of distilling secret key bits from a quantum state ρ_{CD} probabilistically, using an arbitrarily large number of instances of a quantum channel $\mathcal{N}_{AB\to A'B'}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the unextendible entanglement of the quantum channel $\mathcal{N}_{AB\to A'B'}$ induced by the Belavkin–Staszewski relative entropy. That is,*

$$\liminf_{n\to\infty} \frac{1}{n} \widetilde{K}_{\text{2-EXT}}(\rho_{CD}, \mathcal{N}^{\otimes n}) \leq \widehat{E}^{u}(\mathcal{N}_{AB\to A'B'}) . \tag{3.8.25}$$

Similarly, the rate of distilling secret bits exactly from a quantum state ρ_{CD}, using an arbitrarily large number of instances of a quantum channel $\mathcal{N}_{AB\to A'B'}$, assisted by one-way LOCC or two-extendible superchannels, is bounded from above by the min-geometric unextendible entanglement of the quantum channel $\mathcal{N}_{AB\to A'B'}$. That is,

$$\liminf_{n\to\infty} \frac{1}{n} \widetilde{K}^{e}_{\text{2-EXT}}(\rho_{CD}, \mathcal{N}^{\otimes n}) \leq \widehat{E}^{u}_{\min}(\mathcal{N}_{AB\to A'B'}) . \tag{3.8.26}$$

3.9 Numerical calculations

In this section we present some calculations for the upper bounds proposed in Sections 3.6 and 3.8. It has been shown in [FF21a] that the α-geometric Rényi relative entropy of channels can be calculated using a semidefinite program for $\alpha = 1 + 2^{-\ell}$ with $\ell \in \mathbb{N}$. This allows us to compute an upper bound on the unextendible entanglement of a quantum channel induced by the Belavkin–Staszewski relative entropy since the optimization is over a set of channels expressible by semidefinite constraints.

While a semidefinite program is not known for min-geometric unextendible entanglement of channels, the quantity can be calculated for some special channels. The α-geometric Rényi relative entropy between two quantum channels $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A\to B}$, with Choi operators $\Gamma^{\mathcal{N}}_{AB}$ and $\Gamma^{\mathcal{M}}_{AB}$, respectively, can be calculated for all $\alpha \in (0,1)$ using the following equality from [KW21, Proposition 44]:

$$\widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) = \frac{1}{\alpha-1}\log_2 \lambda_{\min}\left(\mathrm{Tr}_B\left[G_\alpha\left(\Gamma^{\mathcal{M}}_{AB}, \widetilde{\Gamma^{\mathcal{N}}_{AB}}\right)\right]\right), \tag{3.9.1}$$

where $\lambda_{\min}$ denotes the minimum eigenvalue of its argument,

$$G_\alpha(X,Y) := X^{\frac{1}{2}}\left(X^{-\frac{1}{2}}YX^{-\frac{1}{2}}\right)^\alpha X^{\frac{1}{2}}, \tag{3.9.2}$$

$$\widetilde{\Gamma^{\mathcal{N}}_{AB}} := \Gamma^{\mathcal{N}}_{0,0} - \Gamma^{\mathcal{N}}_{0,1}\left(\Gamma^{\mathcal{N}}_{1,1}\right)^{-1}\left(\Gamma^{\mathcal{N}}_{0,1}\right)^\dagger, \tag{3.9.3}$$

$$\Gamma^{\mathcal{N}}_{0,0} := \Pi_{\Gamma^{\mathcal{M}}}\Gamma^{\mathcal{N}}\Pi_{\Gamma^{\mathcal{M}}}, \tag{3.9.4}$$

$$\Gamma^{\mathcal{N}}_{0,1} := \Pi_{\Gamma^{\mathcal{M}}}\Gamma^{\mathcal{N}}\Pi^\perp_{\Gamma^{\mathcal{M}}}, \tag{3.9.5}$$

$$\Gamma^{\mathcal{N}}_{1,1} := \Pi^\perp_{\Gamma^{\mathcal{M}}}\Gamma^{\mathcal{N}}\Pi^\perp_{\Gamma^{\mathcal{M}}}, \tag{3.9.6}$$

$\Pi_{\Gamma^{\mathcal{M}}}$ is the projection onto the support of the $\Gamma^{\mathcal{M}}$, $\Pi^\perp_{\Gamma^{\mathcal{M}}}$ is the projection onto its kernel, and all inverses are taken on the respective support. The min-geometric Rényi relative entropy of channels can then be calculated as follows:

$$\widehat{D}_0(\mathcal{N}\|\mathcal{M}) := \sup_{\psi_{RA}}\lim_{\alpha\to 0^+}\widehat{D}_\alpha(\mathcal{N}(\psi_{RA})\|\mathcal{M}(\psi_{RA})) \tag{3.9.7}$$

$$= \sup_{\psi_{RA}}\inf_{\alpha\in(0,1)}\widehat{D}_\alpha(\mathcal{N}(\psi_{RA})\|\mathcal{M}(\psi_{RA})) \tag{3.9.8}$$

$$= \inf_{\alpha\in(0,1)}\sup_{\psi_{RA}}\widehat{D}_\alpha(\mathcal{N}(\psi_{RA})\|\mathcal{M}(\psi_{RA})) \tag{3.9.9}$$

$$= \inf_{\alpha\in(0,1)}\widehat{D}_\alpha(\mathcal{N}\|\mathcal{M}) \tag{3.9.10}$$

$$= \lim_{\alpha\to 0^+}\widehat{D}_\alpha(\mathcal{N}\|\mathcal{M}), \tag{3.9.11}$$

where the first equality is simply the definition of the min-geometric Rényi relative entropy between channels, the second equality follows from the monotonicity of the α-

geometric Rényi relative entropy in α, the third equality follows from the Mosonyi–Hiai minimax theorem given in [MH11, Corollary A.2], and the final equality follows by using the monotonicity of the α-geometric Rényi relative entropy in α once again. Now using the expression of α-geometric Rényi relative entropy from (3.9.1), we conclude the following equality:

$$\widehat{D}_0(\mathcal{N}\|\mathcal{M}) = -\log_2 \lambda_{\min}\left(\operatorname{Tr}_B\left[\Gamma^{\mathcal{M}}\Pi_\zeta\right]\right), \tag{3.9.12}$$

where Π_ζ is the projection onto the support of $\left(\Gamma^{\mathcal{M}}\right)^{-\frac{1}{2}}\widetilde{\Gamma^{\mathcal{N}}}\left(\Gamma^{\mathcal{M}}\right)^{-\frac{1}{2}}$ and $\widetilde{\Gamma^{\mathcal{N}}}$ is defined in (3.9.3).

Proposition 3.22 *The min-geometric unextendible entanglement of quantum channels with full rank Choi operators is equal to zero.*

Proof: Consider a quantum channel $\mathcal{N}_{A\to B}$ that has a full-rank Choi operator $\Gamma^{\mathcal{N}}_{AB}$. The quantum channel $\mathcal{N}_{A\to B_1}\otimes\mathcal{A}^{\pi}_{B_2}$ is a valid extension of the channel that lies in the set $\operatorname{Ext}(\mathcal{N}_{A\to B})$, where $\mathcal{A}^{\pi}_{B_2}$ is a quantum channel that appends the maximally mixed state on the system B_2, and the system B_2 is isomorphic to the system B. The Choi operator of this channel is $\Gamma^{\mathcal{N}}_{AB_1}\otimes\pi_{B_2}$, where π is the maximally mixed state.

By definition, the min-geometric unextendible entanglement of the channel $\mathcal{N}_{A\to B}$ is bounded from above as follows:

$$\widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}) \leq \frac{1}{2}\widehat{D}_0(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{N}_{A\to B_1}\otimes\mathcal{A}^{\pi}_{B_2}). \tag{3.9.13}$$

The quantum channel $\operatorname{Tr}_{B_1}\circ\mathcal{N}_{A\to B_1}\otimes\mathcal{A}^{\pi}_{B_2}$ is essentially the replacer channel $\mathcal{R}^{\pi}_{A\to B_2}$ that traces out the input and replaces with the maximally mixed state. The Choi operator of this channel is

$$\Gamma^{\mathcal{R}}_{AB_2} = \frac{I_{AB_2}}{|B|}, \tag{3.9.14}$$

where $|B|$ is the dimension of the system B. Since $\Gamma^{\mathcal{R}}_{AB}$ is also full rank, $\operatorname{supp}\left(\Gamma^{\mathcal{N}}\right) \subseteq \operatorname{supp}\left(\Gamma^{\mathcal{M}}\right)$, which further implies that $\widetilde{\Gamma^{\mathcal{N}}} = \Gamma^{\mathcal{N}}$. The positive semidefinite operators $\Gamma^{\mathcal{N}}_{AB}$ and $\Gamma^{\mathcal{R}}_{AB}$ are both full-rank operators. Therefore, $\left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}} \Gamma^{\mathcal{N}} \left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}}$ is also a full-rank operator, and the projection onto the support of $\left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}} \Gamma^{\mathcal{N}} \left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}}$ is the identity operator. That is,

$$\Pi_{\left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}}\Gamma^{\mathcal{N}}\left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}}} = I_{AB}. \tag{3.9.15}$$

The min-geometric Rényi relative entropy between $\mathcal{N}_{A\to B}$ and $\mathcal{R}_{A\to B}$ can be evaluated as follows:

$$\begin{aligned}
\frac{1}{2}\widehat{D}_0(\mathcal{N}\|\mathcal{R}^{\pi}) &= -\log_2 \lambda_{\min}\left(\operatorname{Tr}_B\left[\Gamma^{\mathcal{R}}_{AB}\Pi_{\left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}}\Gamma^{\mathcal{N}}\left(\Gamma^{\mathcal{R}}\right)^{-\frac{1}{2}}}\right]\right) && (3.9.16)\\
&= -\log_2 \lambda_{\min}\left(\operatorname{Tr}_B\left[\frac{I_{AB}}{|B|} I_{AB}\right]\right) && (3.9.17)\\
&= -\log_2 \lambda_{\min}(I_A) && (3.9.18)\\
&= 0. && (3.9.19)
\end{aligned}$$

where the second equality follows from (3.9.14) and (3.9.15). The non-negativity of the min-geometric unextendible entanglement combined with (3.9.13) and (3.9.19) implies that the min-geometric unextendible entanglement of a quantum channel that has a full-rank Choi operator is equal to zero. □

Since the min-geometric unextendible entanglement of a quantum channel serves as an upper bound on the zero-error quantum capacity (Corollary 3.4) and the zero-error private capacity of the channel (Corollary 3.3), we arrive at the following statement:

Corollary 3.5 *The zero-error quantum capacity and the zero-error private capacity of a quantum channel with a full-rank Choi operator is equal to zero in the one-shot as well as the asymptotic setting.*

Another important class of channels for which we can evaluate the min-geometric unextendible entanglement is the class of erasure channels. The action of an erasure channel $\mathcal{E}^p_{A\to B}$ on an arbitrary state ρ_{RA} can be mathematically described as follows:

$$\mathcal{E}^p_{A\to B}(\rho_{RA}) := (1-p)\rho_{RB} + p|e\rangle\langle e|_B \otimes \mathrm{Tr}_A[\rho_{RA}]\,, \tag{3.9.20}$$

where $|e\rangle\langle e|$ is the erasure symbol. We give an upper bound on the α-geometric unextendible entanglement of the erasure channel for $\alpha \in (0,1)\cup(1,2]$ in Appendix 3.J. As a special case, we show that the min-geometric unextendible entanglement of an erasure channel with erasure probability $p > 0$ is equal to zero, which leads us to conclude the following statement:

Proposition 3.23 *The zero-error quantum capacity and the zero-error private capacity of an erasure channel with erasure probability $p > 0$ is equal to zero in the one-shot as well as the asymptotic setting.*

Remark 3.11 *The quantum capacities of erasure channels, with erasure probability less than $\frac{1}{2}$, and a subfamily of depolarizing channels are known to be non-zero [BDS97, DSS98]. However, the zero-error quantum capacity of these channels is equal to zero as shown in Corollary 3.5 and Proposition 3.23. This demonstrates an extreme gap in the zero-error and approximate settings of quantum communication over an erasure or depolarizing channel.*

Let us now look at the α-geometric unextendible entanglement of a channel for $\alpha > 1$, which can be computed using a semidefinite program.

3.9.1 Semidefinite program for α-geometric unextendible entanglement of point-to-point channels

In Section 3.6 we showed that the min-geometric unextendible entanglement of a channel is an upper bound on several operationally relevant quantities corresponding to the channel. However, a semidefinite program to compute the min-geometric unextendible entanglement of an arbitrary channel is not known. The α-geometric unextendible entanglement of the channel serves as a weaker upper bound on all the quantities mentioned in Section 3.6 due to the monotonicity of the α-geometric unextendible entanglement of channels in α (see Proposition 3.9). The α-geometric unextendible entanglement of a channel can be calculated for some values of $\alpha \in (1, 2]$ using a semidefinite program, which we describe in this section.

We make use of the semidefinite program given in [FF21a, Lemma 9] that calculates the following quantity:

$$f_{\mathcal{V}}(\mathcal{N}) := \min_{\mathcal{M}\in\mathcal{V}} \widehat{D}_{\alpha}(\mathcal{N}\|\mathcal{M}), \tag{3.9.21}$$

where $\mathcal{V}$ is a set of channels described by semidefinite constraints. Recall that lower semicontinuity of α-geometric Rényi relative entropy allows us to replace the infimum with a minimum, providing a way to calculate the α-geometric unextendible entanglement of a channel.

We first propose a semidefinite program for calculating the α-geometric unextendible entanglement of a point-to-point quantum channel.

Proposition 3.24 *The α-geometric unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ can be calcu-*

lated, for $\alpha = 1 + 2^{-\ell}$ where $\ell \in \mathbb{N}$, using the following semidefinite program:

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) = 2^{\ell} \min_{\substack{y\in\mathbb{R},\Gamma^{\mathcal{P}}_{AB_1B_2}\geq 0 \\ M_{AB},\{N^i_{AB}\}_{i=0}^{\ell},\in \mathrm{Herm}}} \log_2 y, \tag{3.9.22}$$

subject to the constraints,

$$\mathrm{Tr}_{B_2}\left[\Gamma^{\mathcal{P}}_{AB_1B_2}\right] = \Gamma^{\mathcal{N}}_{AB}, \tag{3.9.23}$$

$$\mathrm{Tr}_{B}\left[M_{AB}\right] \leq y I_A, \tag{3.9.24}$$

$$\mathrm{Tr}_{B_1}\left[\Gamma^{\mathcal{P}}_{AB_1B_2}\right] = N^0_{AB}, \tag{3.9.25}$$

$$\begin{bmatrix} M_{AB} & \Gamma^{\mathcal{N}}_{AB} \\ \Gamma^{\mathcal{N}}_{AB} & N^{\ell}_{AB} \end{bmatrix} \geq 0, \tag{3.9.26}$$

$$\begin{bmatrix} \Gamma^{\mathcal{N}}_{AB} & N^{i}_{AB} \\ N^{i}_{AB} & N^{i-1}_{AB} \end{bmatrix} \geq 0 \quad \forall i \in \{1,2,\ldots,\ell\}, \tag{3.9.27}$$

where $\Gamma^{\mathcal{N}}_{AB}$ is the Choi operator of the channel $\mathcal{N}_{A\to B}$, and B, B_1, and B_2 are isomorphic systems.

The constraints in (3.9.23) and (3.9.25) ensure that $\Gamma^{\mathcal{N}}_{AB}$ and N^0_{AB} are the Choi operators of the marginal channels $\mathrm{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2}$ and $\mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2}$. The constraints in (3.9.24)–(3.9.27) are the semidefinite constraints to calculate the quantity $\min_{\mathcal{P}_{A\to B_1B_2}\in\mathcal{V}} \widehat{D}_{\alpha}(\mathcal{N}_{A\to B}\|\,\mathrm{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2})$ for a set of channels $\mathcal{V}$ defined by semidefinite conditions, given in [FF21a, Lemma 9].

Since ℓ dictates the number of variables in the semidefinite program, we cannot practically use this SDP to calculate $\widehat{E}^{u}_{\alpha}$ for α arbitrarily close to one. We settle for $\ell = 10$ in our calculations to get an upper bound on the unextendible entanglement of a channel induced by the Belavkin–Staszewski relative entropy.

3.9.2 Semidefinite program for α-geometric unextendible entanglement of bipartite channels

The semidefinite program for the α-geometric unextendible entanglement of a channel in Proposition 3.24 can be generalized for bipartite channels $\mathcal{N}_{AB\to A'B'}$ by making the identifications $AB \leftrightarrow A$ and $A'B' \leftrightarrow B$, and modifying the constraints for marginal channels.

Proposition 3.25 *The α-geometric unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ can be calculated, for $\alpha = 1 + 2^{-\ell}$ where $\ell \in \mathbb{N}$, using the following semidefinite program:*

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{AB\to A'B'}) = 2^{\ell} \min_{\substack{y\in\mathbb{R},\Gamma^{\mathcal{P}}_{AB_1B_2A'B'_1B'_2}\geq 0 \\ M_{ABA'B},\{N^i_{ABA'B'}\}_{i=0}^{\ell},\in \mathrm{Herm}}} \log_2 y, \tag{3.9.28}$$

subject to the constraints,

$$\mathrm{Tr}_{B'_2}\left[\Gamma^{\mathcal{P}}_{AB_1B_2A'B'_1B'_2}\right] = \Gamma^{\mathcal{N}}_{ABA'B'} \otimes I_{B_2}, \tag{3.9.29}$$

$$\mathrm{Tr}_{A'B'}\left[M_{ABA'B'}\right] \leq y I_{AB}, \tag{3.9.30}$$

$$\mathrm{Tr}_{B_1B'_1}\left[\Gamma^{\mathcal{P}}_{AB_1B_2A'B'_1B'_2}\right] = N^0_{ABA'B'}, \tag{3.9.31}$$

$$\begin{bmatrix} M_{ABA'B'} & \Gamma^{\mathcal{N}}_{ABA'B'} \\ \Gamma^{\mathcal{N}}_{ABA'B'} & N^{\ell}_{ABA'B'} \end{bmatrix} \geq 0, \tag{3.9.32}$$

$$\begin{bmatrix} \Gamma^{\mathcal{N}}_{ABA'B'} & N^{i}_{ABA'B'} \\ N^{i}_{ABA'B'} & N^{i-1}_{ABA'B'} \end{bmatrix} \geq 0 \quad \forall i \in \{1, 2, \ldots, \ell\}, \tag{3.9.33}$$

where $\Gamma^{\mathcal{N}}_{ABA'B'}$ is the Choi operator of the channel $\mathcal{N}_{A\to B}$ and d_B is the dimension of system B. Systems B_1 and B_2 are isomorphic to the system B, and systems B'_1 and B'_2 are isomorphic to the system B'.

Remark 3.12 *We have used the subadditivity of the α-geometric unextendible entanglement (Proposition 3.8) to obtain a single-letter upper bound on all the operational quantities of a*

quantum channel discussed in Sections 3.6 and 3.8, either in terms of the min-geometric unextendible entanglement of the channel or the unextendible entanglement of the channel induced by the Belavkin–Staszewski relative entropy. However, one can obtain a tighter bound by using the regularized unextendible entanglement of the channel because, for all $n \in \mathbb{N}$,

$$\widehat{E}^{u}(\mathcal{N}_{A\to B}) \geq \frac{1}{n}\widehat{E}^{u}(\mathcal{N}^{\otimes n}_{A\to B}), \tag{3.9.34}$$

$$\widehat{E}^{u}_{\min}(\mathcal{N}_{A\to B}) \geq \frac{1}{n}\widehat{E}^{u}_{\min}(\mathcal{N}^{\otimes n}_{A\to B}). \tag{3.9.35}$$

In practice, direct implementations of the optimizations for these quantities are much harder to calculate with increasing n for arbitrary quantum channels, as the dimensions of the corresponding semidefinite programs increase exponentially with n (however, it could be the case that the approach from [FST22], which incorporates permutational symmetry, could make the computational difficulty of these optimizations grow only polynomially with n). By taking the asymptotic limit of these quantities, an arbitrarily large number of channel uses might be required to estimate it, restricting its usefulness from a practical perspective. Nonetheless, we remark that the regularized unextendible entanglement quantities give a generally tighter bound on the respective operational quantities than the single-letter upper bounds discussed in this section.

3.9.3 Semicausal channel for probabilistic distillation of resource

The channel mentioned in (3.8.1) is a specific case of a semicausal channel where Bob's input system is a trivial system. Alice sends some quantum information to Bob through an erasure channel, but instead of the quantum state being lost to the environment upon erasure, the state is returned to Alice. If the state is successfully transmitted to Bob, Alice receives back the erasure symbol instead.

There exists a simple protocol to probabilistically distill entanglement from this chan-

nel using one-way LOCC. Alice sends one share of a locally prepared maximally entangled state to Bob using the channel. If the state is successfully transmitted to Bob, Alice receives an erasure symbol. Alice can determine if her state is erased or not by performing the POVM $\{\Pi, |e\rangle\langle e|\}$ on the system she received, where Π is the projection onto the entire Hilbert space of her system. If she measures her system to be erased, she knows that a maximally entangled state has been established between herself and Bob, and she can indicate the results of her measurement to Bob, hence, distilling a maximally entangled state probabilistically. If the probability of erasure is p and the channel allows Alice to send a d-dimensional state to Bob, then the probabilistic one-way distillable entanglement of the channel is no less than $(1-p)\log_2 d$. We find that the unextendible entanglement of this channel induced by the Belavkin–Staszewski relative entropy, which is an upper bound on the probabilitic distillable entanglement of the channel, is equal to $(1-p)\log_2 d$ as well, as we state formally in Proposition 3.26.

Proposition 3.26 *Consider a quantum channel that acts on an arbitrary state ρ_{RA} as follows:*

$$\mathcal{N}_{A\to A'B}(\rho_{RA}) = p\rho_{RA'} \otimes |e\rangle\langle e|_B + (1-p)\rho_{RB} \otimes |e\rangle\langle e|_{A'}. \tag{3.9.36}$$

The unextendible entanglement of the channel mentioned above, induced by the Belavkin–Staszewski relative entropy, is equal to $(1-p)\log_2 d$.

Proof: See Appendix 3.I. □

One can consider a less idealistic channel, where the state that Alice sends to Bob is truly erased but Alice receives some information about the erasure process. Let us consider a channel that acts on an arbitrary state ρ_{RA} as follows:

$$\mathcal{N}_{A\to A'B}(\rho_{RA}) := (1-p)\rho_{RB} \otimes \sigma_{A'} + p\pi_R \otimes |e\rangle\langle e|_B \otimes \tau_{A'}, \tag{3.9.37}$$

where π is a maximally mixed state, and $\sigma_{A'}$ and $\tau_{A'}$ are some quantum states.

The probabilistic one-way distillable entanglement of this channel depends on Alice's ability to distinguish between the states σ and τ. Naturally, if σ and τ are orthogonal, then Alice can perfectly distinguish between the two states, and the probabilistic one-way distillable entanglement of the channel will be equal to $(1-p)\log_2 d$. However, if the states are not orthogonal Alice will not be able to perfectly distinguish between the two states, and the number of ebits that can be probabilistically distilled from the channel using one-way LOCC would be smaller than $(1-p)\log_2 d$.

We consider a simple case where Alice receives a single classical bit indicating if the state she sent to Bob was erased or not, where the classical bit also undergoes depolarizing noise. As such,

$$\sigma_{A'} = \mathcal{D}_q(|1\rangle\langle 1|_{A'}), \tag{3.9.38}$$

$$\tau_{A'} = \mathcal{D}_q(|0\rangle\langle 0|_{A'}), \tag{3.9.39}$$

where

$$\mathcal{D}_q(\rho_{A'}) = (1-q)\rho_{A'} + q\pi_{A'}. \tag{3.9.40}$$

In Figure 3.6, we plot the α-geometric unextendible entanglement of the following channel:

$$\widetilde{\mathcal{E}}^{p,q}_{A\to A'B}(\rho_{RA}) := (1-p)\rho_{RB}\otimes\mathcal{D}_q(|1\rangle\langle 1|_{A'}) + p\pi_R\otimes|e\rangle\langle e|_B\otimes\mathcal{D}_q(|0\rangle\langle 0|_{A'}), \tag{3.9.41}$$

for different values of p and q, and $\alpha = 1+2^{-10}$. The code for generating the figures in this paper is available with the arXiv posting.

In the examples considered above, Alice can deduce if the state she sent to Bob was erased by analyzing the state she received from the semicausal channel, which allows Alice and Bob to probabilistically distill resource from such channels using only one-way

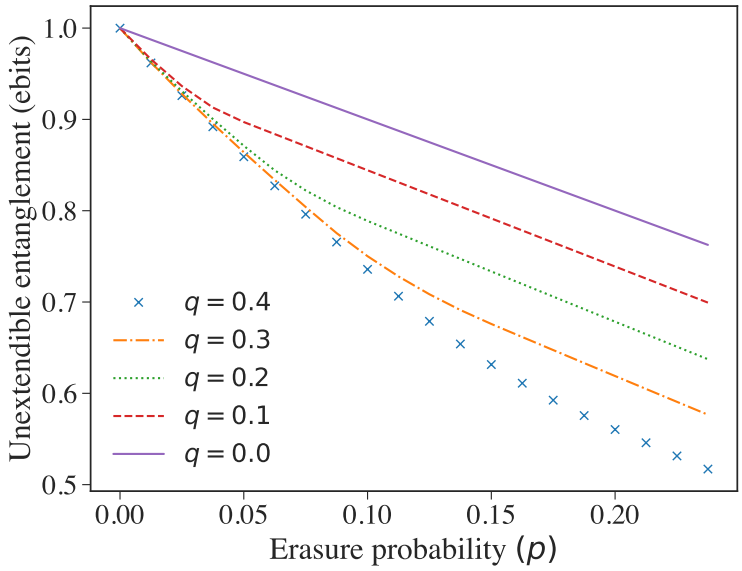


Figure 3.6: Here we plot the α-geometric unextendible entanglement of the channel mentioned in (3.9.41), for $\alpha = 1 + 2^{-10}$. The channel takes a two-dimensional state as input. The α-geometric unextendible entanglement of a channel is an upper bound on the probabilistic one-way distillable entanglement as well as the probabilitic one-way distillable key of the channel for all $\alpha \in (1, 2]$.

LOCC. While the erasure channel and depolarizing channels cannot be used for exact or probabilistic distillation of entanglement or secret keys using only one-way LOCC, it is unclear if these channels cannot be used to boost the probabilistic one-way distillable entanglement or probabilistic one-way distillable key of a bipartite state in the presence of one-way LOCC (see Section 3.8). Nonetheless, we present an analytical upper bound on the α-geometric unextendible entanglement of the erasure channel for all $\alpha \in (1, 2]$, and an analytical expression for the unextendible entanglement of the depolarizing channel induced by the Belavkin–Staszewski relative entropy, in Appendices 3.J and 3.K, respectively.

3.10 Conclusion

3.10.1 Summary

In this work we defined a class of entanglement measures for quantum channels called generalized unextendible entanglement of quantum channels, based on the resource theory of unextendibility. We showed that this quantity does not increase under two-extendible superchannels, and consequently, decreases monotonically under one-way LOCC superchannels as well. This makes the unextendible entanglement of quantum channels a useful quantity for analyzing information-processing tasks that involve transformations of quantum channels assisted by local operations and one-way classical communication.

We found some immediate applications of the unextendible entanglement of quantum channels. The unextendible entanglement of a point-to-point quantum channel, induced by the α-geometric Rényi relative entropy as $\alpha \to 0$, was shown to be an upper bound on the one-way distillable key, one-way distillable entanglement, forward-assisted zero-error quantum capacity, and the forward-assisted zero-error private capacity of the quantum channel. We found this quantity, which we call the min-geometric unextendible entanglement of a channel, to be equal to zero for several important channels such as the erasure channel and all channels with a full-rank Choi operator, indicating that these channels are useless for zero-error quantum and private communication.

The formalism of k-extendibility was extended to bipartite superchannels, and we defined the unextendible entanglement of bipartite semicausal quantum channels. This quantity allowed us to bound the change in unextendibility of a bipartite quantum state

when acted upon by an arbitrary bipartite semicausal quantum channel. Using this formalism we gave upper bounds on the probabilistic one-way distillable entanglement and probabilistic one-way distillable key of a bipartite quantum state when a bipartite quantum channel, not necessarily simulable by local operations and one-way classical communication, is also available.

Finally, we gave a semidefinite program to calculate the unextendible entanglement of a quantum channel induced by the α-geometric Rényi relative entropy for $\alpha = 1 + 2^{-\ell}$, where ℓ is a positive integer, providing a computationally feasible method to calculate the upper bounds on the probabilistic one-way distillable entanglement and probabilistic one-way distillable key of a state-channel pair. We showed some example calculations for this technique, evaluating the α-geometric unextendible entanglement of special erasure channels where one party sends quantum data to a distant party through an erasure channel but also receives some information about the erasure process.

3.10.2 Future directions

There are several future directions to be explored. As was the case in [WWW24], we have restricted all of our measures of unextendibility and applications to two-extendibility. An extension of the measures to k-unextendibility could possibly give tighter bounds on several quantities of interest when using channels assisted by one-way LOCC superchannels. Our formalism also restricts us to the case of zero-error capacities. It will be an interesting direction to allow for arbitrary error in our formalism in order to explore a more general and practical setting.

We have obtained several bounds in terms of the min-geometric Rényi relative entropy

of quantum channels. To the best of our knowledge, no prior work has used this measure as an upper bound on information-theoretic quantities. We believe our approach with min-geometric Rényi relative entropy can be extended to other dynamical resource theories to obtain tighter bounds on several quantities of interest. Given that we have shown the relevance of the min-geometric Rényi relative entropy in our work, we think this motivates developing efficient methods to optimize this quantity with respect to semidefinite constraints.

When multiple uses of a quantum channel are allowed for resource distillation, we restricted the discussion to the independent and identically distributed scenario in which all the quantum channels are used in parallel. A more general case of sequential distillation protocols can be considered. Similar ideas have been pursued in [KW17, BW18, GS20a, FF21a] when positive partial transpose (PPT) channels are allowed for free, and a general treatment for arbitrary resource theories has been considered in [GS20b].

Extending the formalism of unextendibility to bipartite semicausal channels, we gave upper bounds on the probabilistic distillable entanglement and secret key from a bipartite state using one-way LOCC and an unextendible bipartite semicausal channel. It is known that an erasure channel can be used to boost the approximate distillable entanglement of shared bipartite state [WH10]; however, it is still unclear if an erasure channel could boost the one-way exact distillable entanglement or the probabilitic one-way distillable entanglement of the state. In general, it would be interesting to know if channels that cannot be used for zero-error private communication can be used to boost the probabilistic distillable key of a shared bipartite state.

BIBLIOGRAPHY

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[BBC+93] 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(13):1895–1899, March 1993. doi:10.1103/PhysRevLett.70.1895.

[BBFS21] Mario Berta, Francesco Borderi, Omar Fawzi, and Volkher B. Scholz. Semidefinite programming hierarchies for constrained bilinear optimization. *Mathematical Programming*, 194(1-2):781–829, April 2021. arXiv:1810.12197, doi:10.1007/s10107-021-01650-1.

[BCF+96] Howard Barnum, Carlton M. Caves, Christopher A. Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Physical Review Letters*, 76(15):2818–2821, April 1996. arXiv:quant-ph/9511010, doi:10.1103/PhysRevLett.76.2818.

[BDS97] Charles H. Bennett, David P. DiVincenzo, and John A. Smolin. Capacities of quantum erasure channels. *Physical Review Letters*, 78(16):3217–3220, April 1997. arXiv:quant-ph/9701015, doi:10.1103/PhysRevLett.78.3217.

[BDSW96] 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, doi:10.1103/physreva.54.3824.

[BGNP01] David Beckman, Daniel Gottesman, M. A. Nielsen, and John Preskill. Causal and localizable quantum operations. *Physical Review A*, 64(5):052309, October 2001. arXiv:quant-ph/0102043, doi:10.1103/PhysRevA.64.052309.

[BKN00] H. Barnum, E. Knill, and M.A. Nielsen. On quantum fidelities and channel capacities. *IEEE Transactions on Information Theory*, 46(4):1317–1329, 2000. arXiv:quant-ph/9809010v1, doi:10.1109/18.850671.

[BS82] V. P. Belavkin and P. Staszewski. C^*-algebraic generalization of relative entropy and entropy. *Annales de l'I.H.P. Physique théorique*, 37(1):51–58, 1982. URL: http://eudml.org/doc/76163.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, November 1992. doi:10.1103/PhysRevLett.69.2881.

[BW18] Mario Berta and Mark M. Wilde. Amortization does not enhance the max-Rains information of a quantum channel. *New Journal of Physics*, 20(5):053044, 2018. doi:10.1088/1367-2630/aac153.

[CCGFZ99] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller. Creation of entangled states of distant atoms by interference. *Physical Review A*, 59(2):1025–1033, February 1999. arXiv:quant-ph/9810013, doi:10.1103/PhysRevA.59.1025.

[CCHS10] Jianxin Chen, Toby S. Cubitt, Aram W. Harrow, and Graeme Smith. Super-duper-activation of the zero-error quantum capacity. In *2010 IEEE International Symposium on Information Theory*, pages 2695–2697, 2010. doi:10.1109/ISIT.2010.5513780.

[CDP08] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Transforming quantum operations: Quantum supermaps. *Europhysics Letters*, 83(3):30004, July 2008. arXiv:0804.0180, doi:10.1209/0295-5075/83/30004.

[CMW16] Tom Cooney, Milan Mosonyi, and Mark M. Wilde. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. *Communications in Mathematical Physics*, 344(3):797–829, May 2016. arXiv:1408.3373, doi:10.1007/s00220-016-2645-4.

[CS12] Toby S. Cubitt and Graeme Smith. An extreme form of superactivation for quantum zero-error capacities. *IEEE Transactions on Information Theory*, 58(3):1953–1961, 2012. doi:10.1109/TIT.2011.2178157.

[Dat09] Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, 2009. arXiv:0803.2770, doi:10.1109/TIT.2009.2018325.

[Dev05] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005. doi:10.1109/TIT.2004.839515.

[DKQ+23] Dawei Ding, Sumeet Khatri, Yihui Quek, Peter W. Shor, Xin Wang, and Mark M. Wilde. Bounding the forward classical capacity of bipartite quantum channels. *IEEE Transactions on Information Theory*, 69(5):3034–3061, May 2023. doi:10.1109/TIT.2022.3233924.

[Doh14] Andrew C. Doherty. Entanglement and the shareability of quantum states. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424004, October 2014. doi:10.1088/1751-8113/47/42/424004.

[DPS02] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88(18):187904, April 2002. arXiv:quant-ph/0112007, doi:10.1103/PhysRevLett.88.187904.

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69(2):022308, February 2004. arXiv:quant-ph/0308032, doi:10.1103/PhysRevA.69.022308.

[DSS98] David P. DiVincenzo, Peter W. Shor, and John A. Smolin. Quantum-channel capacity of very noisy channels. *Physical Review A*, 57:830–839, February 1998. arXiv:quant-ph/9706061, doi:10.1103/PhysRevA.57.830.

[EGK11] Abbas El Gamal and Young-Han Kim. *Network Information Theory*. Cambridge University Press, 2011. doi:10.1017/CBO9781139030687.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991. doi:10.1103/PhysRevLett.67.661.

[ESW02] T. Eggeling, D. Schlingemann, and R. F. Werner. Semicausal operations are semilocalizable. *Europhysics Letters*, 57(6):782, March 2002. arXiv:quant-ph/0104027, doi:10.1209/epl/i2002-00579-4.

[FF21a] Kun Fang and Hamza Fawzi. Geometric Rényi divergence and its applications in quantum channel capacities. *Communications in Mathematical Physics*, 384(3):1615–1677, May 2021. arXiv:1909.05758, doi:10.1007/s00220-021-04064-4.

[FF21b] Hamza Fawzi and Omar Fawzi. Defining quantum divergences via convex optimization. *Quantum*, 5:387, January 2021. doi:10.22331/q-2021-01-26-387.

[FST22] Omar Fawzi, Ala Shayeghi, and Hoang Ta. A hierarchy of efficient bounds on quantum capacities exploiting symmetry. *IEEE Transactions on Information Theory*, 68(11):7346–7360, 2022. doi:10.1109/TIT.2022.3182101.

[GBP97] M. Grassl, Th. Beth, and T. Pellizzari. Codes for the quantum erasure channel. *Physical Review A*, 56(1):33–38, July 1997. doi:10.1103/PhysRevA.56.33.

[GDAM06] Elloá B. Guedes, Francisco Marcos De Assis, and Rex A. C. Medeiros. *Quantum Zero-Error Information Theory*. Springer, 2106.

[Gha10] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information and Computation*, 10(3):343–360, March 2010. doi:10.26421/QIC10.3-4-11.

[Gou19] Gilad Gour. Comparison of quantum channels by superchannels. *IEEE Transactions on Information Theory*, 65(9):5880–5904, September 2019. arXiv:1808.02607, doi:10.1109/tit.2019.2907989.

[GS20a] Gilad Gour and Carlo Maria Scandolo. Dynamical entanglement. *Physical Review Letters*, 125(18):180505, October 2020. arXiv:2009.12304, doi:10.1103/PhysRevLett.125.180505.

[GS20b] Gilad Gour and Carlo Maria Scandolo. Dynamical resources, 2020. arXiv:2101.01552.

[Gur03] Leonid Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '03, page 10–19, New York, NY, USA, 2003. Association for Computing Machinery. doi:10.1145/780542.780545.

[Hay17] Masahito Hayashi. *Quantum Information Theory: Mathematical Foundation*. Springer, second edition, 2017. doi:10.1007/978-3-662-49725-8.

[HHH99] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review*

A, 60(3):1888–1898, September 1999. arXiv:quant-ph/9807091, doi:10.1103/PhysRevA.60.1888.

[HHHH09] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. arXiv:quant-ph/0702225, doi:10.1103/revmodphys.81.865.

[HHHO05] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, April 2005. doi:10.1103/PhysRevLett.94.160502.

[HHHO09] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189, doi:10.1109/tit.2008.2009798.

[Hol19] Alexander S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. De Gruyter, Berlin, Boston, 2019. doi:10.1515/9783110642490.

[HSR03] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(06):629–641, 2003. doi:10.1142/S0129055X03001709.

[HSW23] Tharon Holdsworth, Vishal Singh, and Mark M. Wilde. Quantifying the performance of approximate teleportation and quantum error correction via symmetric 2-PPT-extendible channels. *Physical Review A*, 107(1):012428, January 2023. arXiv:2207.06931, doi:10.1103/PhysRevA.107.012428.

[JV13] Peter D. Johnson and Lorenza Viola. Compatible quantum correlations: Extension problems for Werner and isotropic states. *Physical Review A*, 88(3):032323, September 2013. arXiv:1305.1342, doi:10.1103/physreva.88.032323.

[KDWW19] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. *Physical Review Letters*, 123(7):070502, August 2019. arXiv:2108.03137, doi:10.1103/physrevlett.123.070502.

[KDWW21] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Resource

theory of unextendibility and nonasymptotic quantum capacity. *Physical Review A*, 104(2):022401, August 2021. arXiv:1803.10710, doi:10.1103/physreva.104.022401.

[Kim08] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, June 2008. arXiv:0806.4195, doi:10.1038/nature07127.

[KO98] J. Korner and A. Orlitsky. Zero-error information theory. *IEEE Transactions on Information Theory*, 44(6):2207–2229, 1998. doi:10.1109/18.720537.

[KW17] Eneet Kaur and Mark M Wilde. Amortized entanglement of a quantum channel and approximately teleportation-simulable channels. *Journal of Physics A: Mathematical and Theoretical*, 51(3):035303, 2017. doi:10.1088/1751-8121/aa9da7.

[KW20] Sumeet Khatri and Mark M. Wilde. Principles of quantum communication theory: A modern approach, 2020. arXiv:2011.04672v1.

[KW21] Vishal Katariya and Mark M. Wilde. Geometric distinguishability measures limit quantum channel estimation and discrimination. *Quantum Information Processing*, 20(2):78, February 2021. doi:10.1007/s11128-021-02992-7.

[LKDW18] Felix Leditzky, Eneet Kaur, Nilanjana Datta, and Mark M. Wilde. Approaches for approximate additivity of the Holevo information of quantum channels. *Physical Review A*, 97(1):012332, January 2018. arXiv:1709.01111, doi:10.1103/PhysRevA.97.012332.

[LLS09] Debbie Leung, Joungkeun Lim, and Peter Shor. Capacity of quantum erasure channel assisted by backwards classical communication. *Physical Review Letters*, 103(24):240505, December 2009. doi:10.1103/PhysRevLett.103.240505.

[LM15] Debbie Leung and William Matthews. On the power of PPT-preserving and non-signalling codes. *IEEE Transactions on Information Theory*, 61(8):4486–4499, 2015. doi:10.1109/TIT.2015.2439953.

[LSW+04] Seth Lloyd, Jeffrey H. Shapiro, Franco N. C. Wong, Prem Kumar, Selim M. Shahriar, and Horace P. Yuen. Infrastructure for the quantum internet. *ACM SIGCOMM Computer Communication Review*, 34(5):9–20, October 2004. doi:10.1145/1039111.1039118.

[LY16] Debbie Leung and Nengkun Yu. Maximum privacy without coherence, zero-error. *Journal of Mathematical Physics*, 57(9):092202, 2016. doi:10.1063/1.4962340.

[Mat13] Keiji Matsumoto. A new quantum version of f-divergence, 2013. arXiv:1311.4722, doi:10.48550/ARXIV.1311.4722.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, May 2001. arXiv:quant-ph/9802025, doi:10.1145/382780.382781.

[MH11] Milán Mosonyi and Fumio Hiai. On the quantum Rényi relative entropies and related capacity formulas. *IEEE Transactions on Information Theory*, 57(4):2474–2487, 2011. arXiv:0912.1286, doi:10.1109/TIT.2011.2110050.

[MLDS+13] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. On quantum Rényi entropies: A new generalization and some properties. *Journal of Mathematical Physics*, 54(12):122203, December 2013. arXiv:1306.3142, doi:10.1063/1.4838856.

[Nie02] Michael A. Nielsen. A simple formula for the average gate fidelity of a quantum dynamical operation. *Physics Letters A*, 303(4):249–252, 2002. URL: https://www.sciencedirect.com/science/article/pii/S0375960102012720, arXiv:quant-ph/0205035, doi:10.1016/S0375-9601(02)01272-0.

[Par70] James L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23–33, March 1970. doi:10.1007/BF00708652.

[PBaHS13] Łukasz Pankowski, Fernando G. S. L. Brandão, Michal Horodecki, and Graeme Smith. Entanglement distillation by extendible maps. *Quantum Information and Computation*, 13(9–10):751–770, September 2013. arXiv:1109.1779, doi:10.26421/QIC13.9-10-2.

[Pet86] Dénes Petz. Quasi-entropies for finite quantum systems. *Reports on Mathematical Physics*, 23(1):57–65, 1986. URL: https://www.sciencedirect.com/science/article/pii/0034487786900674, arXiv:1009.2679, doi:10.1016/0034-4877(86)90067-4.

[PSBZ01] Jian-Wei Pan, Christoph Simon, Časlav Brukner, and Anton Zeilinger. Entan-

glement purification for quantum communication. *Nature*, 410(6832):1067–1070, April 2001. doi:10.1038/35074041.

[PV10] Yury Polyanskiy and Sergio Verdú. Arimoto channel coding converse and Rényi divergence. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1327–1333, 2010. doi:10.1109/ALLERTON.2010.5707067.

[RBL18] Denis Rosset, Francesco Buscemi, and Yeong-Cherng Liang. Resource theory of quantum memories and their faithful verification with minimal assumptions. *Physical Review X*, 8(2):021033, May 2018. arXiv:1710.04710, doi:10.1103/PhysRevX.8.021033.

[RST+18] Filip Rozpedek, Thomas Schiet, Le Phuc Thinh, David Elkouss, Andrew C. Doherty, and Stephanie Wehner. Optimizing practical entanglement distillation. *Physical Review A*, 97(6):062333, June 2018. arXiv:1803.10111, doi:10.1103/PhysRevA.97.062333.

[Sha48] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948. doi:10.1002/j.1538-7305.1948.tb01338.x.

[Sha56] Claude Shannon. The zero error capacity of a noisy channel. *IRE Transactions on Information Theory*, 2(3):8–19, 1956. doi:10.1109/TIT.1956.1056798.

[Shi15] Maksim E. Shirokov. On channels with positive quantum zero-error capacity having vanishing n-shot capacity. *Quantum Information Processing*, 14(8):3057–3074, May 2015. arXiv:1407.8524, doi:10.1007/s11128-015-1014-0.

[SW24] Vishal Singh and Mark M. Wilde. No-go theorem for probabilistic one-way secret-key distillation, 2024. arXiv:2404.01392.

[Ume62] Hisaharu Umegaki. Conditional expectation in an operator algebra. IV. Entropy and information. *Kodai Mathematical Seminar Reports*, 14(2):59 – 85, 1962. doi:10.2996/kmj/1138844604.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. doi:10.1017/9781316848142.

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet:

A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018. doi:10.1126/science.aam9288.

[Wer89] Reinhard F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17(4):359–363, May 1989. doi:10.1007/BF00399761.

[WH10] Mark M. Wilde and Min-Hsiu Hsieh. Entanglement generation with a quantum channel and a shared state. In *2010 IEEE International Symposium on Information Theory*, pages 2713–2717, 2010. arXiv:0904.1175, doi:10.1109/ISIT.2010.5513540.

[Wil17] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, Cambridge, UK, second edition, 2017. doi:10.1017/9781316809976.

[WWW24] Kun Wang, Xin Wang, and Mark M Wilde. Quantifying the unextendibility of entanglement. *New Journal of Physics*, 26(3):033013, mar 2024. arXiv:1911.07433v3, doi:10.1088/1367-2630/ad264e.

[WWY14] 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, July 2014. arXiv:1306.1586, doi:10.1007/s00220-014-2122-x.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982. doi:10.1038/299802a0.

APPENDIX

3.A Proof of Proposition 3.5

In this appendix, we show that the α-geometric unextendible entanglement of quantum states converges to the unextendible entanglement of quantum states induced by the Belavkin–Staszewski relative entropy as $\alpha \to 1$.

Let us first evaluate the α-geometric unextendible entanglement of states when α approaches 1 from above. The α-geometric unextendible entanglement is monotonic in α as is evident from the monotonicity of the underlying divergence, the α-geometric Rényi relative entropy, in α. Therefore,

$$\lim_{\alpha\to 1^+} \widehat{E}^u_\alpha(\rho_{AB}) = \inf_{\alpha\in(1,2]} \widehat{E}^u_\alpha(\rho_{AB}) \tag{3.A.1}$$

$$= \inf_{\alpha\in(1,2]} \frac{1}{2} \inf_{\sigma\in\mathrm{Ext}(\rho)} \widehat{D}_\alpha(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) \tag{3.A.2}$$

$$= \frac{1}{2} \inf_{\sigma\in\mathrm{Ext}(\rho)} \inf_{\alpha\in(1,2]} \widehat{D}_\alpha(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) \tag{3.A.3}$$

$$= \frac{1}{2} \inf_{\sigma\in\mathrm{Ext}(\rho)} \widehat{D}_1(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) \tag{3.A.4}$$

$$= \widehat{E}^u(\rho_{AB})\,. \tag{3.A.5}$$

Now let us evaluate the α-geometric unextendible entanglement when α approaches 1 from below. Once again, using the monotonicity of α-geometric unextendible entanglement in α, we find the following equality:

$$\lim_{\alpha\to 1^-} \widehat{E}^u_\alpha(\rho_{AB}) = \sup_{\alpha\in(0,1)} \widehat{E}^u_\alpha(\rho_{AB}) \tag{3.A.6}$$

$$= \sup_{\alpha\in(0,1)} \frac{1}{2} \inf_{\sigma\in\mathrm{Ext}(\rho)} \widehat{D}_\alpha(\rho\|\operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}])\,. \tag{3.A.7}$$

Since the α-geometric Rényi relative entropy is lower semi-continuous in (ρ, σ) [FF21b, Lemma A.3], and it increases monotonically in α in the range $(0, 2]$, we can employ the Mosonyi–Hiai minimax theorem from [MH11, Corollary A.2] to switch the order of supremum and infimum, obtaining the following equality:

$$\lim_{\alpha \to 1^-} \widehat{E}^u_\alpha(\rho_{AB}) = \frac{1}{2} \inf_{\sigma \in \mathrm{Ext}(\rho)} \sup_{\alpha \in (0,1)} \widehat{D}_\alpha(\rho \| \operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) \tag{3.A.8}$$

$$= \frac{1}{2} \inf_{\sigma \in \mathrm{Ext}(\rho)} \widehat{D}_1(\rho \| \operatorname{Tr}_{B_1}[\sigma_{AB_1B_2}]) \tag{3.A.9}$$

$$= \widehat{E}^u(\rho_{AB}) . \tag{3.A.10}$$

Combining (3.A.5) and (3.A.10), we conclude (3.5.38).

3.B Proof of Proposition 3.11

In this appendix, we show that the α-geometric unextendible entanglement of quantum channels converges to the unextendible entanglement of point-to-point quantum channels induced by the Belavkin–Staszewski relative entropy as $\alpha \to 1$.

Let us first evaluate the limit when α approaches 1 from above. For a given quantum channel $\mathcal{N}_{A\to B}$, let us define the following set of quantum channels:

$$\mathrm{Ext}(\mathcal{N}) := \{\mathcal{P}_{A\to B_1B_2} : \operatorname{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2} = \mathcal{N}_{A\to B}\} . \tag{3.B.1}$$

We know that the unextendible entanglement of channels induced by the α-geometric Rényi relative entropy increases monotonically with α for $\alpha > 0$ [KW21]. Therefore, we can write,

$$\lim_{\alpha \to 1^+} \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) = \inf_{\alpha \in (1,2]} \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \tag{3.B.2}$$

$$= \inf_{\alpha\in(1,2]} \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \tag{3.B.3}$$

$$= \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \inf_{\alpha\in(1,2]} \widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \tag{3.B.4}$$

$$= \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \widehat{D}(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \tag{3.B.5}$$

$$= \widehat{E}^u(\mathcal{N}_{A\to B})\,, \tag{3.B.6}$$

where the first equality is a consequence of monotonicity of α-geometric unextendible entanglement when $\alpha \in (1,2]$ (Proposition 3.9) and the penultimate equality is a consequence of the fact that the α-geometric Rényi relative entropy of channels converges to the Belavkin–Staszewski relative entropy as $\alpha \to 1$ [DKQ+23, Lemma 35].

Now let us evaluate the limit when α approaches 1 from below. By Proposition 3.9, we know that the α-geometric unextendible entanglement increases monotonically for $\alpha \in (0,1)$. Therefore,

$$\lim_{\alpha\to 1^-} \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) = \sup_{\alpha\in(0,1)} \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \tag{3.B.7}$$

$$= \sup_{\alpha\in(0,1)} \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2})\,. \tag{3.B.8}$$

Since the α-geometric Rényi relative entropy of channels $\widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B})$ is lower semi-continuous in $\mathcal{M}_{A\to B}$ [DKQ+23, Lemma 37] and increases monotonically in α in the range $(0,1)$, we can employ the Mosonyi–Hiai minimax theorem from [MH11, Corollary A.2] and establish that

$$\sup_{\alpha\in(0,1)} \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) = \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \sup_{\alpha\in(0,1)} \widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \tag{3.B.9}$$

$$= \inf_{\mathcal{P}_{A\to B_1B_2}\in\mathrm{Ext}(\mathcal{N})} \widehat{D}(\mathcal{N}_{A\to B}\|\operatorname{Tr}_{B_1}\circ\mathcal{P}_{A\to B_1B_2}) \tag{3.B.10}$$

$$= \widehat{E}^u(\mathcal{N}_{A\to B})\,, \tag{3.B.11}$$

where the first equality follows from the Mosonyi–Hiai minimax theorem in [MH11, Corollary A.2], the second equality follows from the fact that α-geometric Rényi relative entropy converges to the Belavkin–Staszewski relative entropy as $\alpha \to 1$, and the final equality follows from the definition of unextendibe entanglement induced by the Belavkin–Staszewski relative entropy. Hence, combining (3.B.6), (3.B.8), and (3.B.11), we conclude (3.5.106).

3.C Proof of Corollary 3.4

In this appendix, we give an alternate proof of Corollary 3.4. Let us begin by evaluating the α-geometric unextendible entanglement of a d-dimensional identity channel.

Proposition 3.27 *The α-geometric unextendible entanglement of a d-dimensional identity channel is equal to $\log_2 d$ for all $\alpha \in (0, 2]$. That is,*

$$\widehat{E}_\alpha^u\left(\mathrm{id}_{A\to B}^d\right) = \log_2 d \qquad \forall \alpha \in (0, 2]. \tag{3.C.1}$$

Proof: Let $\mathcal{P}_{A\to B_1B_2}$ be an extension of the d-dimensional identity channel, i.e.,

$$\mathrm{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2} = \mathrm{id}_{A\to B}^d . \tag{3.C.2}$$

Let $\Gamma_{AB_1B_2}^{\mathcal{P}}$ be the Choi operator of the quantum channel $\mathcal{P}_{A\to B_1B_2}$. Since the Choi operator of the identity channel is the unnormalized maximally entangled state, the Choi operator of the channel $\mathcal{P}_{A\to B_1B_2}$ has the following form:

$$\Gamma_{AB_1B_2}^{\mathcal{P}} = \Gamma_{AB_1} \otimes \sigma_{B_2}, \tag{3.C.3}$$

where Γ_{AB_1} is the unnormalized maximally entangled state, and σ_{B_2} is an arbitrary quantum state. Thus, an arbitrary extension, $\mathcal{P}_{A\to B_1B_2}$, of the identity channel can be expressed as

$$\mathcal{P}_{A\to B_1B_2} = \mathrm{id}^d_{A\to B_1} \otimes \mathcal{A}^{\sigma}_{B_2}, \tag{3.C.4}$$

where $\mathcal{A}^{\sigma}_{B_2}$ is a channel that prepares the state σ_{B_2}.

The two marginals of $\mathcal{P}_{A\to B_1B_2}$ act on an arbitrary quantum state ψ_{RA} as

$$\mathrm{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2}(\psi_{RA}) = \mathrm{id}^d_{A\to B_1}(\psi_{RA}) = \psi_{RB_1}, \tag{3.C.5}$$

and

$$\begin{aligned}\mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2}(\psi_{RA}) &= \mathrm{Tr}_A \otimes \mathcal{A}^{\sigma}_{B_2}(\psi_{RA}) \\ &= \psi_R \otimes \sigma_{B_2}.\end{aligned} \tag{3.C.6}$$

Now consider that

$$\widehat{E}^u_{\alpha}\left(\mathrm{id}^d_{A\to B}\right) = \frac{1}{2} \inf_{\mathcal{P}_{A\to B_1B_2}\in \mathrm{Ext}(\mathrm{id})} \widehat{D}_{\alpha}(\mathrm{id} \,\|\, \mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2}) \tag{3.C.7}$$

$$= \frac{1}{2} \inf_{\sigma_{B_2}} \sup_{\psi_{RA}} \widehat{D}_{\alpha}\left(\psi_{RB_1} \| \psi_R \otimes \sigma_{B_2}\right) \tag{3.C.8}$$

$$= \frac{1}{2} \inf_{\sigma_{B_2}\in\mathcal{S}_+} \sup_{\psi_{RA}} \widehat{D}_{\alpha}\left(\psi_{RB_1} \| \psi_R \otimes \sigma_{B_2}\right), \tag{3.C.9}$$

where $\mathcal{S}_+$ denotes the set of positive definite states, and here we have used the fact that the geometric Rényi relative entropy is lower semi-continuous in the last equality. As shown in [WWW24, Appendix D],

$$\inf_{\sigma_{B_2}\in\mathcal{S}_+} \widehat{D}_{\alpha}(\psi_{RB_1} \| \psi_R \otimes \sigma_{B_2}) = \inf_{\sigma_{B_2}\in\mathcal{S}_+} \log_2 \mathrm{Tr}[\sigma^{-1}_{B_2}]. \tag{3.C.10}$$

The right hand side of the (3.C.10) is independent of ψ_{RA}. Therefore,

$$\widehat{E}^u_{\alpha}\left(\mathrm{id}^d_{A\to B}\right) = \frac{1}{2} \inf_{\sigma_{B_2}\in\mathcal{S}_+} \log_2 \mathrm{Tr}[\sigma^{-1}_{B_2}]. \tag{3.C.11}$$

Let $\{\lambda_i\}_i$ be the eigenvalues of σ_{B_2}, so that this state can be written as

$$\sigma_{B_2} = \sum_{i=1}^{d} \lambda_i |i\rangle\langle i|, \tag{3.C.12}$$

where $\{|i\rangle\}_{i=1}^{d}$ is an eigenbasis of σ_{B_2}. The inverse of this state is

$$\sigma_{B_2}^{-1} = \sum_{i=1}^{d} \lambda_i^{-1} |i\rangle\langle i|. \tag{3.C.13}$$

The α-geometric unextendible entanglement of the identity channel becomes

$$\widehat{E}_\alpha^u\left(\mathrm{id}_{A\to B}^d\right) = \frac{1}{2}\log_2 \inf_{\substack{\{\lambda_i\}_i \\ \sum_i \lambda_i = 1}} \sum_{i=1}^{d} \lambda_i^{-1}, \tag{3.C.14}$$

where the infimum is over every probability distribution $\{\lambda_i\}_i$ with full support. Using the well known arithmetic mean-harmonic mean inequality

$$\frac{d}{\sum_i \lambda_i^{-1}} \leq \frac{\sum_i \lambda_i}{d} = \frac{1}{d}. \tag{3.C.15}$$

Rearranging this inequality then implies that

$$\frac{1}{2}\log_2 \inf_{\substack{\{\lambda_i\}_i \\ \sum_i \lambda_i = 1}} \sum_{i=1}^{d} \lambda_i^{-1} \geq \frac{1}{2}\log_2 d^2. \tag{3.C.16}$$

The inequality above is saturated when all λ_i are equal. Therefore,

$$\widehat{E}_\alpha^u\left(\mathrm{id}_{A\to B}^d\right) = \frac{1}{2}\log_2 d^2 = \log_2 d. \tag{3.C.17}$$

This concludes the proof of Proposition 3.27. □

Now we show that the zero-error quantum capacity of a channel, assisted by one-way LOCC superchannels or two-extendible superchannels, is bounded from above by the min-geometric unextendible entanglement of the channel.

Proof: [Proof of Corollary 3.4] Consider a two-extendible superchannel $\Theta_{(A^n\to B^n)\to(C\to D)}$ that acts on n instances of the channel $\mathcal{N}_{A\to B}$ to exactly simulate the d-dimensional identity channel:

$$\mathrm{id}^d_{C\to D} = \Theta_{(A^n\to B^n)\to(C\to D)}(\mathcal{N}^{\otimes n}_{A\to B})\,. \tag{3.C.18}$$

Equating the α-geometric unextendible entanglement of the identity channel and the simulated channel, the following inequality holds for all $\alpha \in (0,2]$:

$$\widehat{E}^u_\alpha\left(\mathrm{id}^d_{C\to D}\right) = \widehat{E}^u_\alpha(\Theta_{(A^n\to B^n)\to(C\to D)}(\mathcal{N}^{\otimes n}_{A\to B})) \tag{3.C.19}$$

$$\leq \widehat{E}^u_\alpha(\mathcal{N}^{\otimes n}_{A\to B}) \tag{3.C.20}$$

$$\leq n\widehat{E}^u_\alpha(\mathcal{N}_{A\to B})\,, \tag{3.C.21}$$

where the first inequality comes from the monotonicity of the unextendible entanglement under the action of two-extendible superchannels (Theorem 3.5) and the second inequality comes from the subadditivity of the α-geometric unextendible entanglement (Proposition 3.8).

Using (3.C.21) and Proposition 3.27, we arrive at the following inequality:

$$\widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \geq \frac{\log_2 d}{n} = \frac{1}{n}Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B})\,, \tag{3.C.22}$$

where we arrive at the equality after recalling the definition of $Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}_{A\to B})$ from (3.6.56). Since the inequality holds for all $\alpha \in (0,2]$, we can take the limit $\alpha \to 0$ to get the tightest inequality in (3.C.22), owing to the monotonicity of the α-geometric unextendible entanglement in α. Moreover, (3.C.22) holds for every positive integer n, which leads to the following inequality:

$$Q_{0,2\text{-EXT}}(\mathcal{N}_{A\to B}) = \frac{1}{n}Q^{(1)}_{0,2\text{-EXT}}(\mathcal{N}^{\otimes n}_{A\to B}) \leq \widehat{E}^u_{\min}(\mathcal{N}_{A\to B})\,. \tag{3.C.23}$$

The zero-error quantum capacity of a channel assisted by two-extendible superchannels

is never less than the zero-error quantum capacity of the channel assisted by one-way LOCC superchannels, which concludes the proof. □

3.D Proof of Proposition 3.15

Consider an arbitrary quantum channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ where all systems in the set $\{B_i\}_{i=1}^k$ are isomorphic to each other, and all systems in the set $\left\{B'_i\right\}_{i=1}^k$ are isomorphic to each other. Let $\Theta_{(AB\to A'B')\to(CD\to C'D')}$ be a k-extendible superchannel with the k-extension $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$. Let $\mathcal{N}^i_{AB_i\to A'B'_i}$ be a marginal of the channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ such that,

$$\mathcal{N}^i_{AB_i\to A'B'_i} = \mathrm{Tr}_{B'_{[k]\setminus i}} \circ \mathcal{P}_{AB_{[k]}\to A'B'_{[k]}} \circ \mathcal{A}_{B_{[k]\setminus i}}, \tag{3.D.1}$$

The Choi operator of the channel $\Upsilon(\mathcal{P})$, using the propagation rule stated in (3.3.12), is,

$$\Gamma^{\Upsilon(\mathcal{P})} = \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^T \Gamma^{\Upsilon}\right], \tag{3.D.2}$$

where $\Gamma^{\mathcal{P}}_{AB_{[k]}A'B'_{[k]}}$ is the Choi operator of the quantum channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$, and $\Gamma^{\Upsilon}_{AB_{[k]}A'B'_{[k]}CD_{[k]}C'D'_{[k]}}$ is the Choi operator of the superchannel $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$. The Choi operator of the channel $\mathcal{N}^i_{AB_i\to A'B'_i}$ is related to the Choi operator of the channel $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ as

$$\Gamma^{\mathcal{N}_i}_{AB_iA'B'_i} \otimes I_{B_{[k]\setminus i}} = \mathrm{Tr}_{B'_{[k]\setminus i}}\left[\Gamma^{\mathcal{P}}_{AB_{[k]}A'B'_{[k]}}\right], \tag{3.D.3}$$

since the former is a marginal of the latter. Now consider the Choi operator of the channel $\mathrm{Tr}_{D'_{[k]\setminus i}} \circ (\Upsilon(\mathcal{P}))$,

$$\mathrm{Tr}_{D'_{[k]\setminus i}}\left[\Gamma^{\Upsilon(\mathcal{P})}\right] = \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}D'_{[k]\setminus i}}\left[\left(\Gamma^{\mathcal{P}}\right)^T \Gamma^{\Upsilon}\right] \tag{3.D.4}$$

$$= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^T \mathrm{Tr}_{D'_{[k]\setminus i}}\left[\Gamma^{\Upsilon}\right]\right] \tag{3.D.5}$$

$$= \frac{1}{|B'|^{k-1}} \operatorname{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^T \operatorname{Tr}_{D'_{[k]\setminus i}B'_{[k]\setminus i}}\left[\Gamma^{\Upsilon}\right] \otimes I_{B'_{[k]\setminus i}}\right] \tag{3.D.6}$$

$$= \frac{1}{|B'|^{k-1}} \operatorname{Tr}_{AB_{[k]}A'B'_i}\left[\left(\operatorname{Tr}_{B'_{[k]\setminus i}}\left[\Gamma^{\mathcal{P}}\right]\right)^T \operatorname{Tr}_{D'_{[k]\setminus i}B'_{[k]\setminus i}}\left[\Gamma^{\Upsilon}\right]\right] \tag{3.D.7}$$

$$= \frac{1}{|B'|^{k-1}} \operatorname{Tr}_{AB_{[k]}A'B'_i}\left[\left(\Gamma^{\mathcal{N}_i} \otimes I_{B_{[k]\setminus i}}\right)^T \operatorname{Tr}_{D'_{[k]\setminus i}B'_{[k]\setminus i}}\left[\Gamma^{\Upsilon}\right]\right] \tag{3.D.8}$$

$$= \frac{1}{|B'|^{k-1}} \operatorname{Tr}_{AB_iA'B'_i}\left[\left(\Gamma^{\mathcal{N}_i}\right)^T \operatorname{Tr}_{B_{[k]\setminus i}D'_{[k]\setminus i}B'_{[k]\setminus i}}\left[\Gamma^{\Upsilon}\right]\right] \tag{3.D.9}$$

$$= \frac{1}{|B'|^{k-1}} \operatorname{Tr}_{AB_iA'B'_i}\left[\left(\Gamma^{\mathcal{N}_i}\right)^T \operatorname{Tr}_{B'_{[k]\setminus i}}\left[\Gamma^{\Theta} \otimes I_{B'_{[k]\setminus i}D_{[k]\setminus i}}\right]\right] \tag{3.D.10}$$

$$= \operatorname{Tr}_{AB_iA'B'_i}\left[\left(\Gamma^{\mathcal{N}_i}\right)^T \Gamma^{\Theta}\right] \otimes I_{D_{[k]\setminus i}} \tag{3.D.11}$$

$$= \Gamma^{\Theta(\mathcal{N}_i)} \otimes I_{D_{[k]\setminus i}}, \tag{3.D.12}$$

where the third equality is a consequence of (3.7.17), the fifth equality is a consequence of (3.D.3), the seventh equality is a consequence of (3.7.18) and the final equality is arrived at by using the propagation rule again. Since the above equalities are true for all $i \in [k]$, we conclude (3.7.19).

3.E Proof of Proposition 3.16

In this appendix, we show that the action of a bipartite k-extendible superchannel on a bipartite k-extendible quantum channel results in a k-extendible quantum channel.

Let $\mathcal{N}_{AB\to A'B'}$ be a k-extendible quantum channel with a k-extension $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$, and $\Theta_{(AB\to A'B')\to(CD\to C'D')}$ be a k-extendible superchannel with a k-extension $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$. Let $\Gamma^{\mathcal{N}}_{ABA'B'}$ and $\Gamma^{\mathcal{P}}_{AB_{[k]}A'B'_{[k]}}$ be the respective Choi operators of the channels $\mathcal{N}_{AB\to A'B'}$ and $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$, and let $\Gamma^{\Theta}_{ABA'B'CDC'D'}$ and $\Gamma^{\Upsilon}_{AB_{[k]}A'B'_{[k]}CD_{[k]}C'D'_{[k]}}$ be the respective Choi operators of the superchannels $\Theta_{(AB\to A'B')\to(CD\to C'D')}$ and $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$.

The Choi operator of the channel $\Theta(\mathcal{N})$ can be evaluated using the propagation rule, stated in (3.3.12), as

$$\Gamma^{\Theta(\mathcal{N})}_{CDC'D'} = \mathrm{Tr}_{ABA'B'}\left[\left(\Gamma^{\mathcal{N}}_{ABA'B'}\right)^{T}\Gamma^{\Theta}_{ABA'B'CDC'D'}\right]. \tag{3.E.1}$$

Consider the Choi operator of the quantum channel $\Upsilon(\mathcal{P})$,

$$\Gamma^{\Upsilon(\mathcal{P})}_{CD_{[k]}C'D'_{[k]}} = \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T}\Gamma^{\Upsilon}\right]. \tag{3.E.2}$$

Let us first show that $\Theta(\mathcal{N})$ is a marginal of the channel $\Upsilon(\mathcal{P})$. The non-signaling condition for $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ and $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$ from (3.7.9) and (3.7.17), respectively, implies

$$\begin{aligned}
\mathrm{Tr}_{D'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon(\mathcal{P})}\right] &= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}D'_{[k]\setminus 1}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T}\Gamma^{\Upsilon}\right] && (3.E.3)\\
&= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T}\mathrm{Tr}_{D'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]\right] && (3.E.4)\\
&= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T}\left(\mathrm{Tr}_{D'_{[k]\setminus 1}B'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]\otimes\frac{I_{B'_{[k]\setminus 1}}}{|B'|^{k-1}}\right)\right] && (3.E.5)\\
&= \frac{1}{|B'|^{k-1}}\mathrm{Tr}_{AB_{[k]}A'B'_{1}}\left[\left(\mathrm{Tr}_{B'_{[k]\setminus 1}}\Gamma^{\mathcal{P}}\right)^{T}\mathrm{Tr}_{D'_{[k]\setminus 1}B'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]\right] && (3.E.6)\\
&= \frac{1}{|B'|^{k-1}}\mathrm{Tr}_{AB_{[k]}A'B'_{1}}\left[\left(\Gamma^{\mathcal{N}}\otimes I_{B_{[k]\setminus 1}}\right)^{T}\mathrm{Tr}_{D'_{[k]\setminus 1}B'_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]\right] && (3.E.7)\\
&= \frac{1}{|B'|^{k-1}}\mathrm{Tr}_{AB_{1}A'B'_{1}}\left[\left(\Gamma^{\mathcal{N}}\right)^{T}\mathrm{Tr}_{D'_{[k]\setminus 1}B'_{[k]\setminus 1}B_{[k]\setminus 1}}\left[\Gamma^{\Upsilon}\right]\right] && (3.E.8)\\
&= \mathrm{Tr}_{AB_{1}A'B'_{1}}\left[\left(\Gamma^{\mathcal{N}}\right)^{T}\left(\Gamma^{\Theta}\otimes I_{D_{[k]\setminus 1}}\right)\right] && (3.E.9)\\
&= \Gamma^{\Theta(\mathcal{N})}_{CD_{1}C'D'_{1}}\otimes I_{D_{[k]\setminus 1}}, && (3.E.10)
\end{aligned}$$

where the first equality follows from the propagation rule stated in (3.3.12), the third equality follows from the non-signaling condition for k-extensions of sueprchannels given in (3.7.17), the fifth equality follows from the non-signaling condition for k-extensions of quantum channels given in (3.7.9), the penultimate equality follows from the marginality condition for bipartite k-extendible superchannels given in (3.7.18), and the final equality follows once again by using the propagation rule. Equation (3.E.10) implies that $\Theta(\mathcal{N})$ is a marginal of the channel $\Upsilon(\mathcal{P})$ which follows the non-signaling condition given in (3.7.9).

Now let us test the quantum channel $\Upsilon(\mathcal{P})$ for permutation covariance. Since $\mathcal{P}_{AB_{[k]}A'B'_{[k]}}$ is a k-extension of the quantum channel $\mathcal{N}_{AB\to A'B'}$, it obeys the permutation covariance condition given in (3.7.6); that is,

$$\left(W^{\pi}_{B_{[k]}} \otimes W^{\pi}_{B'_{[k]}}\right)\Gamma^{\mathcal{P}}\left(W^{\pi\dagger}_{B_{[k]}} \otimes W^{\pi\dagger}_{B'_{[k]}}\right) = \Gamma^{\mathcal{P}}, \tag{3.E.11}$$

where W^{π} is the unitary corresponding to the permutation π in the symmetric group S_k. Let us define the following unitary:

$$U^{\pi}_{B_{[k]}B'_{[k]}} := W^{\pi}_{B_{[k]}} \otimes W^{\pi}_{B'_{[k]}}, \tag{3.E.12}$$

so that the permutation condition for $\mathcal{P}_{AB_{[k]}\to A'B'_{[k]}}$ can be written as,

$$\Gamma^{\mathcal{P}} = U^{\pi}_{B_{[k]}B'_{[k]}}\,\Gamma^{\mathcal{P}}\,U^{\pi\dagger}_{B_{[k]}B'_{[k]}}. \tag{3.E.13}$$

Let us also define a unitary V^{π} in a similar fashion,

$$V^{\pi}_{D'_{[k]}B_{[k]}D_{[k]}B'_{[k]}} := W^{\pi}_{D'_{[k]}} \otimes W^{\pi}_{B_{[k]}} \otimes W^{\pi}_{D_{[k]}} \otimes W^{\pi}_{B'_{[k]}}. \tag{3.E.14}$$

The permutation covariance condition for k-extendible superchannels given in (3.7.16) can then be written as,

$$\Gamma^{\Upsilon} = V^{\pi}_{D'_{[k]}B_{[k]}D_{[k]}B'_{[k]}}\,\Gamma^{\Upsilon}\,V^{\pi\dagger}_{D'_{[k]}B_{[k]}D_{[k]}B'_{[k]}}. \tag{3.E.15}$$

Note that $(W^{\pi})^T = W^{\pi\dagger}$ since the permutation unitary is completely real. This implies the following equality:

$$\left(\Gamma^{\mathcal{P}}\right)^T\Gamma^{\Upsilon} = \left(U^{\pi}_{B_{[k]}B'_{[k]}}\,\Gamma^{\mathcal{P}}\,U^{\pi\dagger}_{B_{[k]}B'_{[k]}}\right)^T V^{\pi}\Gamma^{\Upsilon}V^{\pi\dagger} \tag{3.E.16}$$

$$= U^{\pi}_{B_{[k]}B'_{[k]}}\left(\Gamma^{\mathcal{P}}\right)^T U^{\pi\dagger}_{B_{[k]}B'_{[k]}}\,V^{\pi}\Gamma^{\Upsilon}V^{\pi\dagger} \tag{3.E.17}$$

$$= U^{\pi}_{B_{[k]}B'_{[k]}}\left(\Gamma^{\mathcal{P}}\right)^T U^{\pi\dagger}_{D_{[k]}D'_{[k]}}\,\Gamma^{\Upsilon}V^{\pi\dagger}. \tag{3.E.18}$$

Using the above equality in the expression for the Choi operator of the channel $\Upsilon(\mathcal{P})$,

$$\Gamma^{\Upsilon(\mathcal{N})}_{CD_{[k]}C'D'_{[k]}} = \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^T\Gamma^{\Upsilon}\right] \tag{3.E.19}$$

$$= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[U^{\pi}_{B_{[k]}B'_{[k]}}\left(\Gamma^{\mathcal{P}}\right)^{T} U^{\pi\dagger}_{D_{[k]}D'_{[k]}}\Gamma^{\Upsilon}V^{\pi\dagger}\right] \tag{3.E.20}$$

$$= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T} U^{\pi\dagger}_{D_{[k]}D'_{[k]}}\Gamma^{\Upsilon}V^{\pi\dagger}U^{\pi}_{B_{[k]}B'_{[k]}}\right] \tag{3.E.21}$$

$$= \mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T} U^{\pi\dagger}_{D_{[k]}D'_{[k]}}\Gamma^{\Upsilon}U^{\pi}_{D_{[k]}D'_{[k]}}\right] \tag{3.E.22}$$

$$= U^{\pi\dagger}_{D_{[k]}D'_{[k]}}\left(\mathrm{Tr}_{AB_{[k]}A'B'_{[k]}}\left[\left(\Gamma^{\mathcal{P}}\right)^{T}\Gamma^{\Upsilon}\right]\right)U^{\pi}_{D_{[k]}D'_{[k]}} \tag{3.E.23}$$

$$= U^{\pi\dagger}_{D_{[k]}D'_{[k]}}\left(\Gamma^{\Upsilon(\mathcal{N})}_{CD_{[k]}C'D'_{[k]}}\right)U^{\pi}_{D_{[k]}D'_{[k]}}, \tag{3.E.24}$$

where we have used the cyclicity of trace to arrive at the third equality. Thus, the quantum channel $\Upsilon(\mathcal{P})$ follows the permutation covariance condition given in (3.7.6).

Since $\Upsilon(\mathcal{P})$ is an extension of the quantum channel $\Theta(\mathcal{N})$ that follows the permutation covariance condition given in (3.7.6), and the non-signaling condition given in (3.7.7), we conclude that $\Theta(\mathcal{N})$ is a k-extendible channel.

3.F Proof of Proposition 3.17

In this section, we show that every bipartite one-way LOCC superchannel is k-extendible for all $k \geq 2$ by constructing an explicit extension of an arbitrary bipartite one-way LOCC superchannel.

In a bipartite one-way LOCC superchannel $\Theta_{(AB\to A'B')\to(CD\to C'D')}$, both the pre-processing and post-processing channels are bipartite one-way LOCC channels. Therefore, we can write the pre-processing channel as follows:

$$\mathcal{E}^{\Theta}_{CD\to AM_ABM_B} := \sum_x \mathcal{E}^{A,x}_{C\to AM_A}\otimes\mathcal{E}^{B,x}_{D\to BM_B}, \tag{3.F.1}$$

where systems C, A and M_A are held by Alice, and systems D, B and M_B are held by Bob. In the above, $\left\{\mathcal{E}^{A,x}_{C\to AM_A}\right\}_x$ is a set of CP maps and $\left\{\mathcal{E}^{B,x}_{D\to BM_B}\right\}_x$ is a set of quantum channels

such that $\mathcal{E}^{\Theta}_{CD\to AM_ABM_B}$ is a quantum channel. Similarly, we can write the post-processing channel as follows:

$$\mathcal{D}^{\Theta}_{A'M_AB'M_B\to C'D'} \coloneqq \sum_y \mathcal{D}^{A,y}_{A'M_A\to C'} \otimes \mathcal{D}^{B,y}_{B'M_B\to D'}, \tag{3.F.2}$$

where systems A', C' and M_A are held by Alice, and systems D', B' and M_B are held by Bob. The set $\left\{\mathcal{D}^{A,y}_{A'M_A\to C'}\right\}_y$ is a set of CP maps and $\left\{\mathcal{D}^{B,y}_{B'M_B\to D'}\right\}_y$ is a set of quantum channels such that $\mathcal{D}^{\Theta}_{A'M_AB'M_B\to C'D'}$ is a quantum channel.

One can define a superchannel $\Upsilon_{(AB_{[k]}\to A'B'_{[k]})\to(CD_{[k]}\to C'D'_{[k]})}$ with the following pre-processing channel:

$$\mathcal{E}^{\Upsilon}_{CD_{[k]}\to AM_AB_{[k]}M_{B_{[k]}}} \coloneqq \sum_x \mathcal{E}^{A,x}_{C\to AM_A} \otimes \mathcal{E}^{B,x}_{D_1\to B_1M_{B_1}} \otimes \cdots \otimes \mathcal{E}^{B,x}_{D_k\to B_kM_{B_k}}. \tag{3.F.3}$$

The post-processing channel associated with the superchannel Υ can be defined as follows:

$$\mathcal{D}^{\Upsilon}_{A'M_AB'_{[k]}M_{B_{[k]}}\to C'D'_{[k]}} \coloneqq \sum_y \mathcal{D}^{A,y}_{A'M_A\to C'} \otimes \mathcal{D}^{B,y}_{B'_1M_{B_1}\to D'_1} \otimes \cdots \otimes \mathcal{D}^{B,y}_{B'_kM_{B_k}\to D'_k}. \tag{3.F.4}$$

It is straightforward to verify that the superchannel Θ is a marginal of the superchannel Υ, and the quantum channels Q^{Θ} and Q^{Υ} unique to the superchannels Θ and Υ respectively, follow the conditions given in (3.7.13), (3.7.14), and (3.7.15). Therefore, Υ is a valid k-extension of the superchannel Θ. Since such a two-extension can be constructed for every one-way LOCC superchannel Θ, we conclude that every one-way LOCC superchannel is k-extendible for all $k \geq 2$.

3.G Proof of Theorem 3.7

In this appendix, we show that the unextendible entanglement of bipartite channels decreases under the action of two-extendible superchannels.

Let $\Theta_{(AB\to A'B')\to(CD\to C'D')}$ be an arbitrary two-extendible superchannel. Let $\mathcal{P}_{AB_1B_2\to A'B_1'B_2'}$ be an arbitrary extension of the channel $\mathcal{N}_{AB\to A'B'}$ such that

$$\mathcal{N}_{AB\to A'B'} = \mathrm{Tr}_{B_2'} \circ \mathcal{P}_{AB_1B_2\to A'B_1'B_2'} \circ \mathcal{A}_{B_2}, \tag{3.G.1}$$

where $\mathcal{A}_{B_2}$ is a quantum channel that appends an arbitrary quantum state to the system B_2. The generalized divergernce between the channels $\mathcal{N}_{AB\to A'B'}$ and $\mathrm{Tr}_{B_1'} \circ \mathcal{P}_{AB_1B_2\to A'B_1'B_2'} \circ \mathcal{A}_{B_1}$ obeys the following inequality:

$$\begin{aligned}
\mathbf{D}\left(\mathcal{N} \middle\| \mathrm{Tr}_{B_1'} \circ \mathcal{P} \circ \mathcal{A}_{B_1}\right) &= \mathbf{D}\left(\mathrm{Tr}_{B_2'} \circ \mathcal{P} \circ \mathcal{A}_{B_2} \middle\| \mathrm{Tr}_{B_1'} \circ \mathcal{P} \circ \mathcal{A}_{B_1}\right) && \text{(3.G.2)}\\
&\geq \mathbf{D}\left(\Theta\left(\mathrm{Tr}_{B_2'} \circ \mathcal{P} \circ \mathcal{A}_{B_2}\right) \middle\| \Theta\left(\mathrm{Tr}_{B_1'} \circ \mathcal{P} \circ \mathcal{A}_{B_1}\right)\right) && \text{(3.G.3)}\\
&= \mathbf{D}\left(\mathrm{Tr}_{D_2'} \circ (\Upsilon(\mathcal{P})) \circ \mathcal{A}_{D_2} \middle\| \mathrm{Tr}_{D_1'} \circ (\Upsilon(\mathcal{P})) \circ \mathcal{A}_{D_1}\right) && \text{(3.G.4)}\\
&\geq 2\mathbf{E}^u\left(\mathrm{Tr}_{D_2'} \circ (\Upsilon(\mathcal{P})) \circ \mathcal{A}_{D_2}\right) && \text{(3.G.5)}\\
&= 2\mathbf{E}^u\left(\Theta\left(\mathrm{Tr}_{B_2'} \circ \mathcal{P} \circ \mathcal{A}_{B_2}\right)\right) && \text{(3.G.6)}\\
&= 2\mathbf{E}^u(\Theta(\mathcal{N})), && \text{(3.G.7)}
\end{aligned}$$

where the first inequality follows from the data-processing inequality for generalized channel divergence of quantum channels (Theorem 3.3), the second equality follows from Proposition 3.15, and the second inequality follows from the definition of the generalized unextendible entanglement of quantum channels. Since the above inequality holds for all quantum channels $\mathcal{P}_{AB_1B_2\to A'B_1'B_2'}$ that lie in the set $\mathrm{Ext}(\mathcal{N})$ defined in (3.7.20), we conclude the statement of Theorem 3.7.

3.H Proof of Theorem 3.8

In this appendix we present the proof of Theorem 3.8.

Let $\rho_{R_C C R_D D}$ be an arbitrary two-extendible state. This means that there exists an extension $\tau_{R_C C R_{D_1} D_1 R_{D_2} D_2}$ of the state $\rho_{R_C C R_D D}$ with the following marginals:

$$\mathrm{Tr}_{R_{D_1} D_1}[\tau] = \mathrm{Tr}_{R_{D_2} D_2}[\tau] = \rho_{R_C C R_D D}, \tag{3.H.1}$$

where system R_{D_1} is isomorphic to R_{D_2} and system D_1 is isomorphic to D_2.

Let $\Theta_{(AB\to A'B')\to(CD\to C'C''D'D'')}$ be a two-extendible superchannel, and let $\mathcal{N}_{AB\to A'B'}$ be an arbitrary semicausal channel. Let us define the following quantum state:

$$\sigma_{R_C C' C'' R_D D' D''} := \Theta(\mathcal{N}_{AB\to A'B'})(\rho_{R_C C R_D D}). \tag{3.H.2}$$

Let $\mathcal{P}_{AB_1B_2\to A'B'_1B'_2}$ be an arbitrary extension of the channel $\mathcal{N}_{AB\to A'B'}$; that is,

$$\mathrm{Tr}_{B'_2} \circ \mathcal{P}_{AB_1B_2\to A'B'_1B'_2} = \mathcal{N}_{AB_1\to A'B'_1} \otimes \mathrm{Tr}_{B_2}. \tag{3.H.3}$$

Proposition 3.15 implies that there exists a superchannel $\Upsilon_{(AB_1B_2\to A'B'_1B'_2)\to(CD_1D_2\to C'D'_1D'_2)}$ such that the following equalities hold:

$$\mathrm{Tr}_{D'_2} \circ (\Upsilon(\mathcal{P})) = \Theta(\mathcal{N}) \otimes \mathrm{Tr}_{D_2}, \tag{3.H.4}$$

$$\mathrm{Tr}_{D'_1} \circ (\Upsilon(\mathcal{P})) = \Theta\Big(\mathrm{Tr}_{B'_1} \otimes \mathcal{P}\Big) \circ \mathrm{Tr}_{D_1}. \tag{3.H.5}$$

Consider the following state:

$$\mathrm{Tr}_{R_{D_2} D'_2} \circ (\Upsilon(\mathcal{P}))(\tau) = \Big(\Theta(\mathcal{N}) \otimes \mathrm{Tr}_{R_{D_2} D_2}\Big)(\tau) \tag{3.H.6}$$

$$= \Theta(\mathcal{N})(\rho_{R_C C R_D D}) \tag{3.H.7}$$

$$= \sigma_{R_C C' C'' R_D D' D''}, \tag{3.H.8}$$

where the first equality follows from Proposition 3.15, the second equality follows from the fact that τ is a two-extension of ρ, and the final equality follows from the definition

of the state σ. The above equality implies that $\Upsilon(\mathcal{P})(\tau)$ is an extension of the state σ. By definition of the unextendible entanglement of states, the following inequality holds:

$$\mathbf{E}^u(\sigma) \leq \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}\Big(\sigma \Big\| \mathrm{Tr}_{R_{D_1}D_1'} \circ (\Upsilon(\mathcal{P}))(\tau)\Big), \tag{3.H.9}$$

where $\mathrm{Ext}(\mathcal{N})$ is the set of all extensions of the channel $\mathcal{N}$ as defined in (3.7.20). Using (3.H.5) we arrive at the following equality:

$$\begin{aligned}\mathrm{Tr}_{R_{D_1}D_1'} \circ (\Upsilon(\mathcal{P}))(\tau) &= \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big(\mathrm{Tr}_{R_{D_1}D_1}[\tau]\Big) &(3.H.10)\\ &= \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big(\rho_{R_C C R_D D}\Big), &(3.H.11)\end{aligned}$$

where the second equality follows from the fact that τ is a two-extension of ρ. As such, the following inequality holds for all two-extendible states $\rho_{R_C C R_D D}$:

$$\mathbf{E}^u(\sigma) \leq \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}\Big(\Theta(\mathcal{N})(\rho) \Big\| \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big(\rho\Big)\Big). \tag{3.H.12}$$

For brevity, let us denote the set of two-extendible states with respect to the partition $R_C C : R_D D$ as 2-$\mathrm{EXT}_{\mathrm{RCD}}$ and the set of all states on systems $R_C C R_D D$ as $\mathcal{S}_{\mathrm{RCD}}$. Supremizing over all two-extendible states in 2-$\mathrm{EXT}_{\mathrm{RCD}}$,

$$\begin{aligned}\sup_{\rho\in 2\text{-}\mathrm{EXT}_{\mathrm{RCD}}} \mathbf{E}^u(\sigma_{R_C C' C'' : R_D D' D''}) &\leq \sup_{\rho\in 2\text{-}\mathrm{EXT}_{\mathrm{RCD}}} \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}\Big(\Theta(\mathcal{N})(\rho) \Big\| \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big(\rho\Big)\Big) &(3.H.13)\\ &\leq \sup_{\rho\in \mathcal{S}_{\mathrm{RCD}}} \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}\Big(\Theta(\mathcal{N})(\rho) \Big\| \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big(\rho\Big)\Big) &(3.H.14)\\ &\leq \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \sup_{\rho\in \mathcal{S}_{\mathrm{RCD}}} \frac{1}{2}\mathbf{D}\Big(\Theta(\mathcal{N})(\rho) \Big\| \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big(\rho\Big)\Big) &(3.H.15)\\ &= \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}\Big(\Theta(\mathcal{N}) \Big\| \Theta\Big(\mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big)\Big) &(3.H.16)\\ &\leq \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2}\mathbf{D}\Big(\mathcal{N} \Big\| \mathrm{Tr}_{B_1'} \circ \mathcal{P}\Big) &(3.H.17)\\ &= \mathbf{E}^u(\mathcal{N}), &(3.H.18)\end{aligned}$$

where the second inequality follows from the fact that the set 2-$\mathrm{EXT}_{\mathrm{RCD}}$ is contained inside the set $\mathcal{S}_{\mathrm{RCD}}$. The third inequality is a consequence of the max-min inequality, the

first equality follows from the definition of generalized divergence of channels, the last inequality follows from the data-processing inequality for generalized divergence of channels, and the last equality follows from the definition of the generalized unextendible entanglement of channels.

Therefore, we conclude the statement of Theorem 3.8.

3.I Proof of Proposition 3.26

In this appendix, we compute the Belavkin–Staszewski induced unextendible entanglement of the channel whose action on an arbitrary state ρ_{RA} is defined as follows:

$$\mathcal{N}_{A\to A'B}(\rho_{RA}) = p\rho_{RA'} \otimes |e\rangle\langle e|_B + (1-p)\rho_{RB} \otimes |e\rangle\langle e|_{A'}, \tag{3.I.1}$$

for some $p \in [0,1]$.

We first establish a lower bound on the unextendible entanglement of the channel induced by the Belavkin–Staszewski relative entropy.

Note that Alice can find out if she received the erased state or not by performing the POVM $\{\Pi_{A'}, |e\rangle\langle e|_{A'}\}$ on her system. She can convey the results of the measurement to Bob via one-way classical communication, which is assumed available for free. Alice and Bob can then replace the erased state with a maximally mixed state, and Alice holds the flag indicating the result from the POVM. As such, Alice and Bob can transform the output state given in (3.I.1) into the following state using a one-way LOCC $\mathcal{L}^{\rightarrow}_{A'B\to A'BX_A}$:

$$(\mathcal{L}^{\rightarrow}_{A'B\to A'BX_A} \circ \mathcal{N})(\rho_{RA}) = p\rho_{RA'} \otimes \pi_B \otimes |0\rangle\langle 0|_{X_A} + (1-p)\rho_{RB} \otimes \pi_{A'} \otimes |1\rangle\langle 1|_{X_A}, \tag{3.I.2}$$

where π is the maximally mixed state.

Let us choose the input state ρ_{RA} to be Φ^d_{RA}, a maximally entangled state of Schmidt rank d. Here we assume that system R is held by Alice. Using Proposition 3.7, we have the following equality:

$$\widehat{E}^u\Big((\mathcal{L}^{\rightarrow} \circ \mathcal{N})\left(\Phi^d_{RA}\right)\Big) = p\widehat{E}^u\left(\Phi^d_{RA'} \otimes \pi_B\right) + (1-p)\widehat{E}^u\left(\Phi^d_{RB} \otimes \pi_A\right). \tag{3.I.3}$$

The state $\Phi^d_{RA'} \otimes \pi_B$ is a separable state with respect to the partition $RA' : B$; therefore,

$$\widehat{E}^u\left(\Phi^d_{RA'} \otimes \pi_B\right) = 0. \tag{3.I.4}$$

It is easy to see that the unextendible entanglement induced by the Belavkin–Staszewski relative entropy of the state $\Phi^d_{RB} \otimes \pi_A$ is equal to $\log_2 d$, by means of the following reasoning:

$$\begin{aligned}
\log_2 d &= \widehat{E}^u\left(\Phi^d_{R:B}\right) && (3.I.5)\\
&= \widehat{E}^u\left(\mathrm{Tr}_{A'}\left[\Phi^d_{RB} \otimes \pi_{A'}\right]\right) && (3.I.6)\\
&\leq \widehat{E}^u\left(\Phi^d_{RB} \otimes \pi_{A'}\right) && (3.I.7)\\
&\leq \widehat{E}^u\left(\Phi^d_{RB}\right) + \widehat{E}^u(\pi_{A'}) && (3.I.8)\\
&= \widehat{E}^u\left(\Phi^d_{R:B}\right), && (3.I.9)
\end{aligned}$$

where the first equality follows from (3.5.49), the first follows from the monotonicity of unextendible entanglement under local operations, the second inequality follows from the subadditivity of the uenxtendible entanglement induced by the Belavkin–Staszewski relative entropy (see (3.5.48)), and the last equality follows from the fact that the unextendible entanglement induced by the Belavkin–Staszewski relative entropy is equal to zero for two-extendible states. Therefore,

$$\widehat{E}^u\Big((\mathcal{L}^{\rightarrow} \circ \mathcal{N})\left(\Phi^d_{RA}\right)\Big) = (1-p)\log_2 d. \tag{3.I.10}$$

Since $\mathcal{L}^{\rightarrow}_{A'B\to A'BX_A}$ is an instance of a two-extendible superchannel, Theorem 3.8 implies the following inequality:

$$\widehat{E}^u(\mathcal{N}_{A\to A'B}) \geq (1-p)\log_2 d. \tag{3.I.11}$$

Now let us establish an upper bound on the unextendible entanglement of the channel induced by the Belavkin–Staszewski relative entropy of the channel.

Consider the following extension of the channel $\mathcal{N}_{A\to A'B}$:

$$\mathcal{P}_{A\to A'B_1B_2} = \mathcal{N}_{A\to A'B_1} \otimes \mathcal{A}^{\pi}_{B_2}, \tag{3.I.12}$$

where $\mathcal{A}^{\pi}_{B_2}$ is a channel that appends a maximally mixed state on system B_2, and systems B_1 and B_2 are isomorphic to each other. Let us define the following channel:

$$\mathcal{M}_{A\to A'B_2} = \mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to A'B_1B_2}. \tag{3.I.13}$$

The Choi operators of the two relevant marginals of the channel $\mathcal{P}_{A\to A'B_1B_2}$ are as follows:

$$\Gamma^{\mathcal{N}}_{AA'B_1} = p\Gamma_{AA'} \otimes |e\rangle\langle e|_{B_1} + (1-p)\Gamma_{AB_1} \otimes |e\rangle\langle e|_{A'}, \tag{3.I.14}$$

$$\Gamma^{\mathcal{M}}_{AA'B_2} = p\Gamma_{AA'} \otimes \pi_{B_2} + (1-p)I_A \otimes \pi_{B_2} \otimes |e\rangle\langle e|_{A'}, \tag{3.I.15}$$

where Γ is the unnormalized maximally entangled operator. Note that the erasure symbol is orthogonal to every quantum state in the Hilbert space of the system. Hence, the identity operator, I_A, acts on the subspace orthogonal to $|e\rangle\langle e|_A$.

The Belavkin–Staszewski relative entropy between the channels $\mathcal{N}_{A\to A'B}$ and $\mathcal{M}_{A\to A'B}$ can be calculated using their Choi operators as follows [FF21a]:

$$\widehat{D}(\mathcal{N}_{A\to A'B}\|\mathcal{M}_{A\to A'B}) = \left\| \mathrm{Tr}_{A'B}\left[\left(\Gamma^{\mathcal{N}}_{AA'B}\right)^{1/2} (\log_2 Q_{AA'B}) \left(\Gamma^{\mathcal{N}}_{AA'B}\right)^{1/2} \right] \right\|_{\infty}, \tag{3.I.16}$$

where

$$Q_{AA'B} = \left(\Gamma^{\mathcal{N}}_{AA'B}\right)^{1/2} \left(\Gamma^{\mathcal{M}}_{AA'B}\right)^{-1} \left(\Gamma^{\mathcal{N}}_{AA'B}\right)^{1/2}. \tag{3.I.17}$$

We can write $\Gamma^{\mathcal{M}}_{AA'B}$ as a linear combination of orthogonal projectors as follows:

$$\Gamma^{\mathcal{M}}_{AA'B} = p\Phi^{d}_{RA'} \otimes I_B + \frac{1-p}{d} I_{RB} \otimes |e\rangle\langle e|_{A'}. \tag{3.I.18}$$

Therefore,

$$\left(\Gamma^{\mathcal{M}}_{AA'B}\right)^{-1} = \frac{1}{p}\Phi^{d}_{RA'} \otimes I_B + \frac{d}{1-p} I_{RB} \otimes |e\rangle\langle e|_{A'}. \tag{3.I.19}$$

Similarly, $\Gamma^{\mathcal{N}}_{AA'B}$ can be written as a linear combination of orthogonal projectors as follows:

$$\Gamma^{\mathcal{N}}_{AA'B_1} = pd\Phi^{d}_{RA'} \otimes |e\rangle\langle e|_B + (1-p)d\Phi^{d}_{RB} \otimes |e\rangle\langle e|_{A'}. \tag{3.I.20}$$

Following simple linear algebra, we find that

$$Q_{AA'B} = d^2\Phi^{d}_{RB} \otimes |e\rangle\langle e|_{A'}, \tag{3.I.21}$$

and consequently,

$$\log_2 Q_{AA'B} = 2\log_2 d\ \Phi^{d}_{RB} \otimes |e\rangle\langle e|_{A'}. \tag{3.I.22}$$

Substituting this value into (3.I.16), we evaluate the Belavkin–Staszewski relative entropy between $\mathcal{N}_{A\to A'B}$ and $\mathcal{M}_{A\to A'B}$ to be equal to $(1-p)\log_2 d$; that is,

$$\widehat{D}(\mathcal{N}_{A\to A'B}\|\mathcal{M}_{A\to A'B}) = 2(1-p)\log_2 d. \tag{3.I.23}$$

By the definition of the unextendible entanglement of channels,

$$\widehat{E}^{u}(\mathcal{N}_{A\to A'B}) \leq \frac{1}{2}\widehat{D}(\mathcal{N}_{A\to A'B}\|\mathcal{M}_{A\to A'B}) \tag{3.I.24}$$

$$= (1-p)\log_2 d. \tag{3.I.25}$$

Combining (3.I.11) and (3.I.25), we conclude that

$$\widehat{E}^{u}(\mathcal{N}_{A\to A'B}) = (1-p)\log_2 d. \tag{3.I.26}$$

3.J Unextendible entanglement of erasure channels

In this section we find analytical and numerical upper bounds on the unextendible entanglement of the erasure channel. An erasure channel erases the input state with some

probability p and is defined as follows [GBP97]:

$$\mathcal{E}^{p}_{A\to B}(Y) = (1-p)Y + p|e\rangle\langle e|\,\mathrm{Tr}[Y], \tag{3.J.1}$$

where $|e\rangle\langle e|$ is the erasure symbol, orthogonal to all input states. The Choi operator of this channel is as follows:

$$\Gamma^{\mathcal{E}}_{AB} = (1-p)\,\Gamma_{AB} + pI_A \otimes |e\rangle\langle e|_B. \tag{3.J.2}$$

Erasure channels are of special interest in the context of quantum communication because there exists a well known protocol to distill a maximally entangled state using this channel, assisted by local operations and two-way classical communication. Alice sends one share of a locally prepared maximally entangled state of Schmidt rank d to Bob through an erasure channel. Bob performs the projective measurement $\left\{\sum_{i=0}^{d-1}|i\rangle\langle i|, |e\rangle\langle e|\right\}$ on the state he received, thus, finding out if the quantum state sent by Alice was erased or not. Bob can convey this classical information back to Alice using a classical channel, hence, establishing a maximally entangled state between the two parties which can be used for quantum communication or private communication tasks.

The protocol mentioned above can be used to probabilistically distill $\log_2 d$ ebits from a d-dimensional erasure channel with probability $1-p$, where p is the erasure probability of the channel. However, it requires Bob to send back classical data to Alice. We will see that one cannot distill any entanglement from the erasure channel with the assistance of one-way LOCC superchannels only, as the min-geometric unextendible entanglement of the erasure channel is equal to zero (Proposition 3.29). See also [LLS09] for a further study of the assisted quantum capacities of the erasure channel.

The proposition below provides an upper bound on the unextendible entanglement of the erasure channel induced by the Belavkin–Staszewski relative entropy.

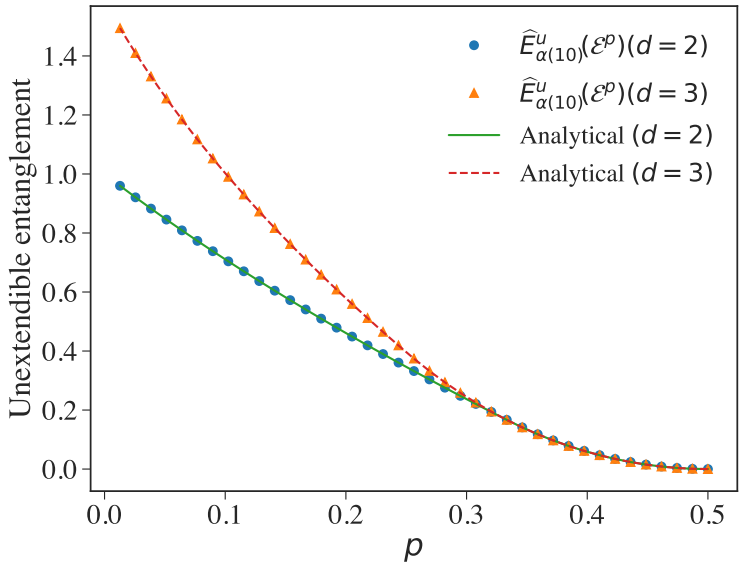


Figure 3.7: Here we plot the upper bounds on the unextendible entanglement of the two-dimensional and the three-dimensional erasure channel induced by the Belavkin–Staszewski relative entropy using the analytical expression given in Proposition 3.28. We also plot the numerical values of the α-geometric unextendible entanglement calculated for $\alpha = 1 + 2^{-10}$ using the semidefinite program given in Proposition 3.24.

Proposition 3.28 *The unextendible entanglement of a d-dimensional erasure channel with erasure probability $p \leq 1/2$, induced by the Belavkin–Staszewski relative entropy, is bounded from above by*

$$\widehat{E}^u\left(\mathcal{E}^p_{A\to B}\right) \leq (1-p)\log_2 d - \frac{1}{2}\log_2\left((d^2-1)p+1\right) \tag{3.J.3}$$

for all $p \in \left[0, \frac{1}{d+1}\right]$, and by

$$\widehat{E}^u\left(\mathcal{E}^p_{A\to B}\right) \leq \frac{1}{2}(1-p)\log_2\left(\frac{1-p}{p}\right) + \frac{1}{2}p\log_2\left(\frac{p}{1-p}\right) \tag{3.J.4}$$

for all $p \in \left(\frac{1}{d+1}, \frac{1}{2}\right]$.

Proof: First, we note that an erasure channel is two-extendible if the erasure probability is greater than 1/2. Hence, the unextendible entanglement of such erasure channels, induced by the Belavkin–Staszewski relative entropy, is equal to zero.

Now consider the extension $\mathcal{P}_{A\to B_1B_2}$ of the erasure channel $\mathcal{E}^p_{A\to B}$ with the Choi operator,

$$\Gamma^{\mathcal{P}}_{AB_1B_2} \coloneqq p\Gamma_{AB_2} \otimes |e\rangle\langle e|_{B_1} + (1-p-dx)\,\Gamma_{AB_1} \otimes |e\rangle\langle e|_{B_2} + x\Gamma_{AB_1} \otimes \Pi_{B_2}, \tag{3.J.5}$$

where

$$\Pi \coloneqq |0\rangle\langle 0| + \cdots + |d-1\rangle\langle d-1| \tag{3.J.6}$$

is the projection onto all possible states of the input space. This operator is positive semidefinite for all $x \in [0, (1-p)/d]$. The two marginals of this channel are described by the Choi operators,

$$\Gamma^{\mathcal{N}}_{AB} = \mathrm{Tr}_{B_2}\left[\Gamma^{\mathcal{P}}_{AB_1B_2}\right] = (1-p)\,\Gamma_{AB} + p\Pi_A \otimes |e\rangle\langle e|_B, \tag{3.J.7}$$

and

$$\Gamma^{\mathcal{M}}_{AB} = \mathrm{Tr}_{B_1}\left[\Gamma^{\mathcal{P}}_{AB_1B_2}\right] \tag{3.J.8}$$

$$= p\Gamma_{AB} + (1-p-dx)\,\Pi_A \otimes |e\rangle\langle e|_B + x\Pi_A \otimes \Pi_B. \tag{3.J.9}$$

Note that $\Gamma^{\mathcal{N}}_{AB}$ is the Choi operator of the erasure channel with erasure probability p, justifying the claim that $\mathcal{P}_{A\to B_1B_2}$ is an extension of the said erasure channel.

By definition,

$$\widehat{E}^u\left(\mathcal{E}^p_{A\to B}\right) \leq \frac{1}{2}\widehat{D}\left(\mathcal{E}^p_{A\to B}\middle\|\, \mathrm{Tr}_{B_2} \circ \mathcal{P}_{A\to B_1B_2}\right), \tag{3.J.10}$$

where $\widehat{D}(\cdot\|\cdot)$ is the Belavkin–Staszewski relative entropy between channels. This quantity has a closed-form expression in terms of the Choi operators of the two channels [FF21a],

$$\widehat{D}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) = \left\|\mathrm{Tr}_B\left[\left(\Gamma^{\mathcal{N}}_{AB}\right)^{1/2}(\log_2 Q_{AB})\left(\Gamma^{\mathcal{N}}_{AB}\right)^{1/2}\right]\right\|_\infty, \tag{3.J.11}$$

where

$$Q_{AB} = \left(\Gamma^{\mathcal{N}}_{AB}\right)^{1/2}\left(\Gamma^{\mathcal{M}}_{AB}\right)^{-1}\left(\Gamma^{\mathcal{N}}_{AB}\right)^{1/2}. \tag{3.J.12}$$

The Choi operator $\Gamma_{AB}^{\mathcal{M}}$ can be written as

$$\Gamma_{AB}^{\mathcal{M}} = (pd + x)\,\Phi_{AB}^{d} + x\left(\Pi_A \otimes \Pi_B - \Phi_{AB}^{d}\right) + (1 - p - dx)\,\Pi_A \otimes |e\rangle\langle e|_B, \tag{3.J.13}$$

where Φ_{AB}^{d} is the maximally entangled state of Schmidt rank d. Since we have written $\Gamma_{AB}^{\mathcal{M}}$ as a linear combination of orthogonal projections, we can conclude

$$\left(\Gamma_{AB}^{\mathcal{M}}\right)^{-1} = \frac{1}{pd + x}\Phi_{AB}^{d} + \frac{1}{x}\left(\Pi_A \otimes \Pi_B - \Phi_{AB}^{d}\right) + \frac{1}{1 - p - dx}\Pi_A \otimes |e\rangle\langle e|_B. \tag{3.J.14}$$

From the above, we conclude that

$$\left(\Gamma_{AB}^{\mathcal{N}}\right)^{1/2} (\log_2 Q_{AB}) \left(\Gamma_{AB}^{\mathcal{N}}\right)^{1/2} = (1 - p)\, d \log_2\left(\frac{d\,(1 - p)}{pd + x}\right)\Phi_{AB}^{d} + p \log_2\left(\frac{p}{1 - p - dx}\right)\Pi_A \otimes |e\rangle\langle e|_B. \tag{3.J.15}$$

This allows us to evaluate the quantity in (3.J.11) to be

$$\widehat{D}(\mathcal{N}_{A\to B} \| \mathcal{M}_{A\to B}) = (1 - p) \log_2\left(\frac{d\,(1 - p)}{pd + x}\right) + p \log_2\left(\frac{p}{1 - p - dx}\right). \tag{3.J.16}$$

This quantity is minimized for

$$x = \frac{(1 - p)^2 - p^2 d^2}{d}. \tag{3.J.17}$$

The Choi operator $\Gamma_{AB}^{\mathcal{M}}$ is required to be a positive semidefinite operator. This in turn requires x to be non-negative. Therefore, we choose

$$x = \frac{(1 - p)^2 - p^2 d^2}{d}, \tag{3.J.18}$$

if $p \leq \frac{1}{d+1}$, and $x = 0$ otherwise. Using these values of x in (3.J.16) and rearranging, we arrive at the upper bound given in Proposition 3.28. □

In Figure 3.7, we plot the α-geometric unextendible entanglement of the channel, for $\alpha = 1 + 2^{-10}$, against the analytical upper bound on the unextendible entanglement of the channel induced by the Belavkin–Staszewski relative entropy.

We also evaluate an upper bound on the α-geometric unextendible entanglement of the erasure channel and find an analytical expression given in the proposition below. In the limit $\alpha \to 0^+$, this quantity is equal to zero. This finding, combined with Corollaries 3.4 and 3.3, implies that both the zero-error quantum and private capacities of the erasure channel are equal to zero.

Proposition 3.29 *For all $\alpha \in (0,1) \cup (1,2]$, the α-geometric unextendible entanglement of a d-dimensional erasure channel with erasure probability $p \leq 1/2$ is bounded from above by*

$$\widehat{E}^u_\alpha\left(\mathcal{E}^p_{A\to B}\right) \leq \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(\begin{array}{c}\frac{1}{d}\left[d\left(1-p\right)\right]^\alpha\left(pd+x\right)^{1-\alpha}\\ +p^\alpha\left(1-p-dx\right)^{1-\alpha}\end{array}\right) \tag{3.J.19}$$

for all $p \in \left[0, \frac{1}{d^{1/\alpha}+1}\right]$, and where

$$x = \frac{1-p-pdk}{k+d}, \tag{3.J.20}$$

$$k = \frac{d^{2/\alpha}p}{d\left(1-p\right)}. \tag{3.J.21}$$

For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}^u_\alpha\left(\mathcal{E}^p_{A\to B}\right) \leq \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(\left(1-p\right)^\alpha p^{1-\alpha} + p^\alpha\left(1-p\right)^{1-\alpha}\right). \tag{3.J.22}$$

As such, for all $p \in (0, 1/2]$,

$$\widehat{E}^u_{\min}\left(\mathcal{E}^p_{A\to B}\right) = 0. \tag{3.J.23}$$

Proof: Here we follow the same approach used in the proof of Proposition 3.28. Let us first recall from [KW21, Proposition 44] that the geometric Rényi relative entropy of channels can be written explicitly as

$$\widehat{D}_\alpha(\mathcal{N}\|\mathcal{M}) = \frac{1}{\alpha-1}\log_2\widehat{Q}_\alpha(\mathcal{N}\|\mathcal{M}), \tag{3.J.24}$$

where

$$\widehat{Q}_\alpha(\mathcal{N}\|\mathcal{M}) := \left\| \mathrm{Tr}_B\left[\left(\Gamma^{\mathcal{M}}\right)^{1/2} \left[\left(\Gamma^{\mathcal{M}}\right)^{-1/2} \Gamma^{\mathcal{N}} \left(\Gamma^{\mathcal{M}}\right)^{-1/2} \right]^\alpha \left(\Gamma^{\mathcal{M}}\right)^{1/2} \right] \right\|_\infty \tag{3.J.25}$$

when $\alpha \in (1, 2]$ and

$$\widehat{Q}_\alpha(\mathcal{N}\|\mathcal{M}) := \lambda_{\min}\left(\mathrm{Tr}_B\left[\left(\Gamma^{\mathcal{M}}\right)^{1/2} \left[\left(\Gamma^{\mathcal{M}}\right)^{-1/2} \Gamma^{\mathcal{N}} \left(\Gamma^{\mathcal{M}}\right)^{-1/2} \right]^\alpha \left(\Gamma^{\mathcal{M}}\right)^{1/2} \right] \right) \tag{3.J.26}$$

when $\alpha \in (0, 1)$, with both expressions above holding under the assumption that $\mathrm{supp}(\Gamma^{\mathcal{N}}) \subseteq \mathrm{supp}(\Gamma^{\mathcal{M}})$. Now using the expressions in (3.J.7) and (3.J.9), we find that

$$\begin{aligned} &\left(\Gamma^{\mathcal{M}}\right)^{1/2} \left[\left(\Gamma^{\mathcal{M}}\right)^{-1/2} \Gamma^{\mathcal{N}} \left(\Gamma^{\mathcal{M}}\right)^{-1/2} \right]^\alpha \left(\Gamma^{\mathcal{M}}\right)^{1/2} \\ &\qquad = \left[d\,(1-p)\right]^\alpha (pd + x)^{1-\alpha}\, \Phi_{AB}^d + p^\alpha\, (1 - p - dx)^{1-\alpha}\, \Pi_A \otimes |e\rangle\langle e|_B. \end{aligned} \tag{3.J.27}$$

This in turn implies that

$$\widehat{D}_\alpha(\mathcal{N}\|\mathcal{M}) = \frac{1}{\alpha - 1} \log_2 \begin{pmatrix} \frac{1}{d}\left[d\,(1-p)\right]^\alpha (pd + x)^{1-\alpha} \\ + p^\alpha\, (1 - p - dx)^{1-\alpha} \end{pmatrix}. \tag{3.J.28}$$

This quantity is minimized for the choice

$$x = \frac{1 - p - pdk}{k + d}, \tag{3.J.29}$$

where $k = \frac{d^{2/\alpha} p}{d(1-p)}$. In order for $\Gamma^{\mathcal{M}}$ to be positive semidefinite, it is required that $x \geq 0$, which is the same as $p \leq \frac{1}{d^{1/\alpha}+1}$. So when this condition holds, we choose x as above, and otherwise choose $x = 0$. In the latter case, we find that

$$\frac{1}{\alpha - 1} \log_2 \begin{pmatrix} \frac{1}{d}\left[d\,(1-p)\right]^\alpha (pd + x)^{1-\alpha} \\ + p^\alpha\, (1 - p - dx)^{1-\alpha} \end{pmatrix} = \frac{1}{\alpha - 1} \log_2 \left(\frac{1}{d}\left[d\,(1-p)\right]^\alpha (pd)^{1-\alpha} + p^\alpha\, (1-p)^{1-\alpha} \right) \tag{3.J.30}$$

$$= \frac{1}{\alpha - 1} \log_2 \left((1-p)^\alpha\, p^{1-\alpha} + p^\alpha\, (1-p)^{1-\alpha} \right). \tag{3.J.31}$$

This leads to the inequalities in (3.J.19) and (3.J.22).

To establish the limit when $\alpha \to 0^+$, we simply set $x = 0$ and then take the limit as $\alpha \to 0^+$, leading to

$$\lim_{\alpha \to 0^+} \frac{1}{\alpha - 1} \log_2 \left((1-p)^\alpha \, p^{1-\alpha} + p^\alpha \, (1-p)^{1-\alpha} \right) = - \log_2 \left((1-p)^0 \, p^1 + p^0 \, (1-p)^1 \right) = 0. \quad (3.J.32)$$

This completes the proof. □

3.K Unextendible entanglement of depolarizing channels

Depolarizing channels are commonly used to model noise in quantum circuits. The d-dimensional depolarizing channel $\mathcal{D}_p$ is a completely positive trace-preserving map when the parameter $p \in \left[0, \frac{d^2}{d^2-1}\right]$, and it acts on a quantum state ρ as

$$\mathcal{D}_p(\rho) = (1-p)\,\rho + p\pi, \quad (3.K.1)$$

where $\pi \coloneqq I/d$ is the d-dimensional maximally mixed state. The Choi operator of a depolarizing channel $\mathcal{D}_p$ is,

$$\Gamma_{AB}^{\mathcal{D}_p} = (1-p)\Gamma_{AB} + p I_A \otimes \pi_B. \quad (3.K.2)$$

The Choi operator can be written as a linear combination of orthogonal projectors as

$$\Gamma_{AB}^{\mathcal{D}_p} = d\left(F\Phi_{AB}^d + (1-F)\frac{I_{AB} - \Phi_{AB}^d}{d^2-1} \right), \quad (3.K.3)$$

where

$$F \coloneqq 1 - p + \frac{p}{d^2}. \quad (3.K.4)$$

Since the Choi operator of the depolarizing channel is a full-rank operator for $p > 0$, the min-geometric unextendible entanglement of this channel is equal to zero, which implies that the zero-error quantum capacity and the zero-error private capacity of this

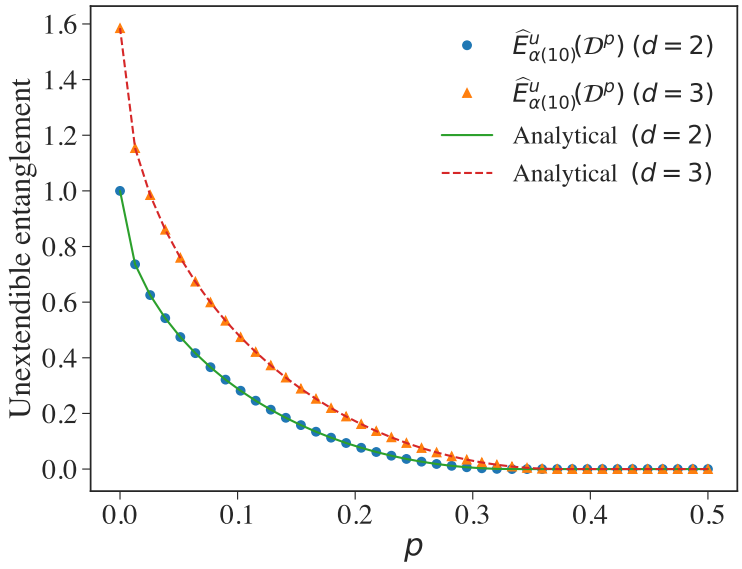


Figure 3.8: Here we plot the unextendible entanglement of the two-dimensional and the three-dimensional depolarizing channel induced by the Belavkin–Staszewski relative entropy using the analytical expression given in Proposition 3.30. We also plot the numerical values of the α-geometric unextendible entanglement calculated for $\alpha = 1 + 2^{-10}$ using the semidefinite program given in Proposition 3.24.

channel, assisted by one-way LOCC or two-extendible superchannels, are also equal to zero (see Corollary 3.5).

The extendibility of isotropic states has been studied in [JV13], and since the Choi operator of the depolarizing channel is a scaled isotropic state, we can find an analytical expression for the α-geometric unextendible entanglement of the channel. Let us first look at the extremities. Since a point-to-point quantum channel is two-extendible if and only if its Choi state is two-extendible, the d-dimensional depolarizing channel is two-extendible for $p \geq \frac{d}{2(d+1)}$ [JV13, Theorem III.8] (also see [KDWW21, Lemma 3]). This implies that the α-geometric unextendible entanglement of a depolarizing channel with $p \geq \frac{d}{2(d+1)}$ is equal to zero. For $p = 0$, the depolarizing channel is the same as the identity channel; hence, the α-geometric unextendible entanglement in this case is equal to one.

Proposition 3.30 *The unextendible entanglement of the d-dimensional depolarizing channel, with parameter* $p < \frac{d}{2(d+1)}$*, induced by the Belavkin–Staszewski relative entropy is*

$$\widehat{E}^{u}(\mathcal{D}^{p}) = \frac{1}{2}\left[F \log_2\left(\frac{F}{F'}\right) + (1-F)\log_2\left(\frac{1-F}{1-F'}\right)\right], \tag{3.K.5}$$

where $F = 1 - p + \frac{p}{d^2}$ *and*

$$F' := \max\left\{\frac{2F-1}{d^2} + \frac{2\sqrt{(d^2-1)(1-F)F}}{d^2} - F + 1, F\right\}. \tag{3.K.6}$$

Proof: Consider a d-dimensional depolarizing channel $\mathcal{D}^{p}_{A\to B}$ with parameter p as defined in (3.K.1). The Choi operator of this channel is

$$\Gamma^{\mathcal{D}^p}_{AB} = d\left(F\Phi^{d}_{AB} + (1-F)\frac{I_{AB} - \Phi^{d}_{AB}}{d^2-1}\right), \tag{3.K.7}$$

where

$$F = 1 - p + \frac{p}{d^2}. \tag{3.K.8}$$

The depolarizing channel does not change under the action of a twirling superchannel; that is,

$$\mathcal{T}_{AB}\left(\mathcal{D}^{p}_{A\to B}\right) = \int dU\, \mathcal{U}_B \circ \mathcal{D}^{p}_{A\to B} \circ \mathcal{U}^{\dagger}_A = \mathcal{D}^{p}_{A\to B}, \tag{3.K.9}$$

where $\mathcal{U}$ is the unitary channel corresponding to the unitary U and acts as $\mathcal{U}(\cdot) = U(\cdot)U^{\dagger}$ and the integration is taken over the Haar measure. Twirling an arbitrary point-to-point quantum channel results in a depolarizing channel [HHH99, Nie02].

Let $\mathcal{P}_{A\to B_1B_2}$ be a extension of $\mathcal{D}^{p}_{A\to B}$ lying in the set $\mathrm{Ext}(\mathcal{D}^{p})$. Consider the following tripartite twirling superchannel:

$$\mathcal{T}_{AB_1B_2}(\mathcal{P}_{A\to B_1B_2}) := \int dU\, \mathcal{U}_{B_1} \circ \mathcal{U}_{B_2} \circ \mathcal{P}_{A\to B_1B_2} \circ \mathcal{U}^{\dagger}_A. \tag{3.K.10}$$

The quantum channel $\mathcal{T}_{AB_1B_2}(\mathcal{P}_{A\to B_1B_2})$ also lies in the set $\mathrm{Ext}(\mathcal{D}^{p})$ since

$$\mathrm{Tr}_{B_2} \circ \mathcal{T}_{AB_1B_2}(\mathcal{P}) = \mathcal{T}_{AB_1}(\mathrm{Tr}_{B_2} \circ \mathcal{P}) = \mathcal{D}^{p}_{A\to B_1}, \tag{3.K.11}$$

which follows from the trace-preserving nature of the channel $\mathcal{U}_{B_2}$. Moreover, the other marginal of this channel is also a depolarizing channel, with some parameter p' as shown below:

$$\mathrm{Tr}_{B_1} \circ \mathcal{T}_{AB_1B_2}(\mathcal{P}) = \mathcal{T}_{AB_2}(\mathrm{Tr}_{B_1} \circ \mathcal{P}) = \mathcal{D}^{p'}_{A\to B_2}. \tag{3.K.12}$$

As stated above, twirling a quantum channel is a valid superchannel, and the generalized divergence between two quantum channels decreases upon twirling due to the data-processing inequality. This implies that

$$\mathbf{D}(\mathrm{Tr}_{B_2} \circ \mathcal{T}(\mathcal{P}_{A\to B_1B_2}) \,\|\, \mathrm{Tr}_{B_1} \circ \mathcal{T}(\mathcal{P}_{A\to B_1B_2})) = \mathbf{D}\Big(\mathcal{T}\Big(\mathcal{D}^{p}_{A\to B}\Big) \| \mathcal{T}(\mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2})\Big) \tag{3.K.13}$$

$$\leq \mathbf{D}\Big(\mathcal{D}^{p}_{A\to B} \| \,\mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2}\Big). \tag{3.K.14}$$

This further implies that

$$\inf_{\mathcal{P}_{A\to B_1B_2}\in \mathrm{Ext}(\mathcal{D}^p)} \mathbf{D}\Big(\mathcal{D}^{p}_{A\to B} \| \,\mathrm{Tr}_{B_1} \circ \mathcal{T}(\mathcal{P}_{A\to B_1B_2})\Big) \leq \inf_{\mathcal{P}_{A\to B_1B_2}\in \mathrm{Ext}(\mathcal{D}^p)} \mathbf{D}\Big(\mathcal{D}^{p}_{A\to B} \| \,\mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2}\Big), \tag{3.K.15}$$

and hence, we only need to consider the extensions $\mathcal{P}_{A\to B_1B_2} \in \mathrm{Ext}(\mathcal{D}^p)$ that are invariant under the tripartite twirl $\mathcal{T}_{AB_1B_2}$ when computing the unextendible entanglement of the channel. Since the marginals of such channels are always depolarizing channels, we can write,

$$\mathbf{E}^u\Big(\mathcal{D}^{p}_{A\to B}\Big) = \inf_{\mathcal{P}\in \mathrm{Ext}(\mathcal{N})} \frac{1}{2} \left\{ \begin{array}{c} \mathbf{D}\Big(\mathcal{D}^{p}_{A\to B} \| \mathcal{D}^{p'}_{A\to B}\Big) : \\ \mathcal{P}_{A\to B_1B_2} = \mathcal{T}(\mathcal{P}_{A\to B_1B_2}), \\ \mathcal{D}^{p'}_{A\to B} = \mathrm{Tr}_{B_1} \circ \mathcal{P}_{A\to B_1B_2} \end{array} \right\}. \tag{3.K.16}$$

The Belavkin–Staszewski relative entropy between two depolarizing channels $\mathcal{D}^{p}_{A\to B}$ and $\mathcal{D}^{p'}_{A\to B}$, using the analytical expression given in [FF21a, Theorem 3], evaluates to the following quantity:

$$\widehat{D}\Big(\mathcal{D}^{p} \| \mathcal{D}^{p'}\Big) = F \log_2\left(\frac{F}{F'}\right) + (1-F)\log_2\left(\frac{1-F}{1-F'}\right), \tag{3.K.17}$$

where

$$F = 1 - p + \frac{p}{d^2}, \tag{3.K.18}$$

$$F' = 1 - p' + \frac{p'}{d^2}. \tag{3.K.19}$$

Let ζ_{AB}^F denote an isotropic state with parameter F:

$$\zeta_{AB}^F := F\Phi_{AB}^d + (1-F)\frac{I_{AB} - \Phi_{AB}^d}{d^2 - 1}. \tag{3.K.20}$$

Since the Choi operator of the depolarizing channel is an isotropic state with a scaling factor (see (3.K.7)), the following two statements are equivalent:

1. There exists a quantum channel $\mathcal{P}_{A\to B_1B_2}$ with the depolarizing channels, $\mathcal{D}_{A\to B_1}^p$ and $\mathcal{D}_{A\to B_2}^{p'}$, as its marginals.
2. There exists a quantum state $\tau_{AB_1B_2}$ with the isotropic states, $\zeta_{AB_1}^F$ and $\zeta_{AB_2}^{F'}$, as its marginals, where F and F' are given in (3.K.18) and (3.K.19), respectively.

Therefore, we can compute the unextendible entanglement of a depolarizing channel, using the measure induced by the Belavkin–Staszewski relative entropy as follows:

$$\widehat{E}^u\left(\mathcal{D}_{A\to B}^p\right) = \inf_{F'\in[0,1]} \left\{ \begin{array}{c} \widehat{D}\left(\mathcal{D}^p \| \mathcal{D}^{p'}\right) : \\ \tau_{AB_1B_2} \in \mathcal{S}(AB_1B_2) \\ \mathrm{Tr}_{B_2}[\tau] = \zeta_{AB_1}^F, \mathrm{Tr}_{B_1}[\tau] = \zeta_{AB_2}^{F'}, \\ F = 1 - p + \frac{p}{d^2}, F' = 1 - p' + \frac{p'}{d^2} \end{array} \right\}. \tag{3.K.21}$$

Moreover, the infimum can be replaced with a minimum due to the lower-semicontinuity of the Belavkin–Staszewski relative entropy.

It has been shown in [JV13, Corollary III.4] that there exists a quantum state $\tau_{AB_1B_2}$ with marginals ζ_{AB}^F and $\zeta_{AB}^{F'}$ if and only if F and F' lie in the convex hull of the ellipse

$$\frac{(F + F' - 1)^2}{1/d^2} + \frac{(F - F')^2}{(d^2-1)/d^2} = 1, \tag{3.K.22}$$

and the point $(F, F') = (0, 0)$. Rewriting the equation of ellipse in the form of a quadratic equation in F',

$$(F + F' - 1)^2 + \frac{(F - F')^2}{d^2 - 1} = \frac{1}{d^2} \tag{3.K.23}$$

$$\Rightarrow \quad (F')^2 \left(1 + \frac{1}{d^2 - 1}\right) + F' \left(2(F - 1) - \frac{2F}{d^2 - 1}\right) + (F - 1)^2 + \frac{F^2}{d^2 - 1} - \frac{1}{d^2} = 0. \tag{3.K.24}$$

Let F'_{hi} and F'_{lo} be the two solutions of this quadratic equation such that $F'_{\text{hi}} \geq F'_{\text{lo}}$. Since (F, F') can reside anywhere in the convex hull of the ellipse and the point $(0, 0)$, the largest value F' can take for a fixed value of F lies on the boundary of the ellipse, and hence, is the larger of the two solutions of the quadratic equation in (3.K.24) which is F'_{hi}. Solving (3.K.24), we find that

$$F'_{\text{hi}} = \frac{2F - 1}{d^2} + \frac{2\sqrt{(d^2 - 1)(1 - F)F}}{d^2} - F + 1. \tag{3.K.25}$$

The Belavkin–Staszewski relative entropy between two depolarizing channels as given in (3.K.17) is minimized when F' is the closest to F. Therefore, the optimal value of F' is achieved by $\max\left\{F'_{\text{hi}}, F\right\}$. Hence, we can substitute this optimal value of F' in (3.K.17) and (3.K.21) to arrive at the following analytical expression for the unextendible entanglement of the depolarizing channel, using the measure induced by the Belavkin–Staszewski relative entropy:

$$\widehat{E}^u\left(\mathcal{D}^p_{A\to B}\right) = \frac{1}{2} \left\{ \begin{array}{c} F \log_2\left(\frac{F}{F'}\right) + (1 - F) \log_2\left(\frac{1-F}{1-F'}\right) : \\ F' = \max\left\{\frac{2F-1}{d^2} + \frac{2\sqrt{(d^2-1)(1-F)F}}{d^2} - F + 1, F\right\}, \\ F = 1 - p + \frac{p}{d^2} \end{array} \right\}. \tag{3.K.26}$$

This completes the proof. □

In Figure 3.8 we plot the α-geometric unextendible entanglement of the two-dimensional and three-dimensional depolarizing channels for $\alpha = 1 + 2^{-10}$, with respect to

the prameter p. We also plot the analytical expression for the unextendible entanglement of the depolarizing channel induced by the Belavkin–Staszewski relative entropy given in Proposition 3.30.

CHAPTER 4

EXTENDIBILITY LIMITS QUANTUM-SECURED COMMUNICATION AND KEY DISTILLATION[1]

4.1 Abstract

Secret-key distillation from quantum states and channels is a central task of interest in quantum information theory, as it facilitates private communication over a quantum network. Here, we study the task of secret-key distillation from bipartite states and point-to-point quantum channels using local operations and one-way classical communication (one-way LOCC). We employ the resource theory of unextendible entanglement to study the transformation of a bipartite state under one-way LOCC, and we obtain several efficiently computable upper bounds on the number of secret bits that can be distilled from a bipartite state using one-way LOCC channels; these findings apply not only in the one-shot setting but also in some restricted asymptotic settings. We extend our formalism to private communication over a quantum channel assisted by forward classical communication. We obtain efficiently computable upper bounds on the one-shot forward-assisted private capacity of a channel, thus addressing a question in the theory of quantum-secured communication that has been open for some time now. Our formalism also provides upper bounds on the rate of private communication when using a large number of channels in such a way that the error in the transmitted private data decreases exponentially with the number of channel uses. Moreover, our bounds can be computed using semidefinite programs, thus providing a computationally feasible method to understand

[1] V. Singh and M. M. Wilde, "Extendibility limits quantum-secured communication and key distillation", accepted in *Reports on Progress in Physics*, https://iopscience.iop.org/article/10.1088/1361-6633/adcd28

the limits of private communication over a quantum network.

4.2 Introduction

4.2.1 Motivation

The existence of a quantum network facilitates the distribution of secret keys between distant parties [BB84, Eke91], which ensures secure communication by means of the one-time pad protocol. However, realizing an ideal quantum network can be very expensive. This motivates an in-depth study of the number of secret bits that can be established with the available resources, which, in the context of the quantum internet, are partially entangled states and quantum channels.

Our ability to distill secret keys from a bipartite state or a quantum channel depends on the operations that we can perform. The three most common settings studied in any non-local resource distillation task are as follows: local operations, local operations with one-way classical communication, and local operations with two-way classical communication. Here we consider the task of secret-key distillation from bipartite states and point-to-point channels in the presence of local operations and one-way classical communication. In what follows, we first discuss our contributions on understanding secret-key distillation from states, and thereafter we discuss our related contributions for channels.

4.2.2 Secret-key distillation from states

The task of distilling secret keys from a bipartite state using local operations and one-way classical communication, abbreviated as one-way LOCC, has been studied extensively in the past [DW05, RR12, KKGW21]. From an information-theoretic perspective, the main quantities of interest are the one-shot, one-way distillable key of a state and the asymptotic one-way distillable key of the state. The one-shot, one-way distillable key of a state is roughly defined as the maximum number of "approximate" secret bits that can be distilled from a state using a one-way LOCC channel with respect to a fixed error parameter, and the asymptotic one-way distillable key of the state is the maximum rate at which secret bits can be distilled from an arbitrarily large number of independent and identically distributed copies of the state when using one-way LOCC channels.

Computing the one-shot, one-way distillable key and the asymptotic one-way distillable key is a challenging task. Lower bounds on the one-way distillable key in the one-shot regime, as well as the asymptotic regime, have been found in previous works [DW05, RR12, KKGW21]. Upper bounds on the one-shot distillable key of a state when using two-way LOCC have been found in terms of the smooth-min relative entropy of entanglement [WTB17] and the squashed entanglement [Chr06, CEH+07, CSW12, Wil16]. Naturally, these quantities also bound the one-shot, one-way distillable key from above. However, computing the smooth-min relative entropy of entanglement of a state is related to the NP-hard problem of optimizing over the set of separable states [Gur03, Gha10], and the squashed entanglement is not even known to be computable in the Turing sense, due to it involving an optimization over a state having a system of unbounded size. Moreover, the aforementioned quantities bound the one-shot distillable key of a state, which is expected to be larger than the one-shot, one-way distillable key of the state in general,

leaving room for significant improvement in the estimation of the latter quantity.

In this work, we invoke the framework of unextendibility to obtain upper bounds on the one-shot, one-way distillable key of a state, which can be computed by means of a semidefinite program. As such, to the best of our knowledge, ours is the first general upper bound on this quantity that is efficiently computable, in contrast to the smooth-min relative entropy of entanglement and the squashed entanglement. We also give an upper bound on the maximum rate at which secret bits can be distilled from an arbitrarily large number of i.i.d. copies of a state when using one-way LOCC channels, provided that the error in distillation decreases exponentially with the number of copies of the resource state.

4.2.3 Private communication over channels

The one-shot setting of private communication has been the subject of several studies [RR11, WTB17, Wil17, RSW17, KKGW21]. In the context of private communication, we are interested in the maximum number of private bits that can be sent through a quantum channel when using some freely available operations, which can be local operations and classical communication, local operations with only forward-classical communication, or local operations only. The corresponding quantities are called the one-shot two-way-assisted private capacity, the one-shot forward-assisted private capacity, and the one-shot unassisted private capacity, respectively. In the presence of forward-classical assistance, the task of secret-key distillation is equivalent to the task of private communication, which allows us to immediately extend our understanding of secret-key distillation from channels to private communication.

Finding efficiently computable upper bounds on the one-shot private capacity of a channel has remained an unsolved problem since early works on private capacity [CWY04, DW05]. Several upper bounds on the one-shot, two-way-assisted private capacity have been obtained [TGW14, WTB17, QSW18]. However, none of them are known to be efficiently computable. Even in the asymptotic regime, computable upper bounds on the unassisted private capacity and two-way-assisted private capacity are known only for qubit channels [FF21].

Here we contribute to this growing body of knowledge by giving upper bounds on the one-shot forward-assisted private capacity of a channel, which can be computed efficiently using a semidefinite program. We also give a semidefinite computable upper bound on the maximum rate at which private bits can be transmitted through a quantum channel when the error in transmission is required to decay exponentially with the number of channel uses.

4.2.4 Methods used in this work

The resource theory of unextendible entanglement developed in [WWW24] serves as the primary mathematical framework in our investigation. The set of free states in the resource theory of unextendible entanglement is a state-dependent set comprising of all symmetric extensions of the state in question. The set of two-extendible channels serves as the set of free operations, which was defined in [KDWW19, KDWW21]. All one-way LOCC channels are two-extendible channels, which makes the resource theory of unextendible entanglement useful for the analysis of private communication with one-way LOCC.

The unextendible entanglement of quantum channels was defined in [SW24b], which is the primary mathematical framework that we use to investigate private communication through a quantum channel assisted by one-way LOCC. In this resource theory, the set of free channels is a channel-dependent set, which consists of channels that are symmetrically-*compatible* with the channel in question, where compatible channels were defined in [HMZ16]. The set of free operations are two-extendible superchannels, which form a semidefinite relaxation of the set of one-way LOCC superchannels originally considered in [LM15, RBL18].

In the past, the unextendible entanglement of states has been used to study the *exact* and *probabilistic* distillation of secret keys from states using one-way LOCC channels in [WWW24, SW24a], and the unextendible entanglement of channels has been used to study zero-error private communication through channels in [SW24b]. By using the resource theory of unextendible entanglement to study "approximate" secret-key distillation from states and channels, we demonstrate that this resource theory can be used to study more practical settings in which an arbitrarily small error is allowed in resource distillation.

4.2.5 Summary of results and organization of the paper

The main contributions of our paper are as follows: We give upper bounds on the one-shot, one-way distillable key of a bipartite state and on the one-shot, forward-assisted private capacity of point-to-point quantum channels. As mentioned previously, to the best of our knowledge, these are the first efficiently computable upper bounds on these quantities. Extending our results to the asymptotic setting, we give upper bounds on the maximum rate of distilling secret keys from i.i.d. copies of a bipartite state or channel

Setting	Divergence used for upper bound	Reference
One-shot setting	Smooth-min relative entropy	Theorem 4.2
Simplified bounds for one-shot setting	Smooth-min relative entropy	Corollary 4.1 and Corollary 4.2
n-Shot setting	Sandwiched Rényi relative entropy	Corollary 4.3
Asymptotic setting	Umegaki relative entropy	Theorem 4.3

Table 4.1: A list of our results for secret-key distillation from a bipartite state when using one-way LOCC channels, in the one-shot and asymptotic settings.

Setting	Divergence used for upper bound	Reference
One-shot setting	Smooth-min relative entropy	Theorem 4.4
Simplified bounds for one-shot setting	Smooth-min relative entropy	Corollary 4.4
n-shot setting	Geometric Rényi relative entropy	Corollary 4.5
Asymptotic setting	Belavkin–Staszewski relative entropy	Theorem 4.5

Table 4.2: A list of our results for forward-assisted private communication from point-to-point quantum channels in the one-shot and asymptotic settings.

when using one-way LOCC, albeit in a particular setting in which the error in distillation is required to decay exponentially with the number of copies of the resource. Several of our bounds can be computed using semidefinite programs, adding to their practical relevance. Finally, with this work, we demonstrate the power of the resource theory of unextendible entanglement in studying resource distillation. Prior to our work here, it was unclear how to apply this concept to the setting of approximate key distillation and left as an open question since [WWW24].

In Table 4.1, we present a brief summary of our results on one-way secret-key distillation from bipartite states, and in Table 4.2, we give a brief summary of our results on forward-assisted private communication over channels. We note here that the Python codes used for calculating the semidefinite programs and producing the plots in this paper are available with the arXiv posting.

An outline of our paper is as follows:

- Section 4.3: Definitions and notations used in the paper, along with basic facts about quantum states, channels, and superchannels.
- Section 4.4: Discussion on secret-key distillation from bipartite states using one-way LOCC channels, and definition of the one-shot, one-way distillable key of a state, which is the primary quantity of interest.
- Section 4.5: Review of the concepts of two-extendibility and the unextendible entanglement of states. Discussion on the unextendible entanglement of states induced by smooth-min relative entropy and α-sandwiched Rényi relative entropy, which are the primary ingredients in the main result obtained for one-way secret-key distillation from bipartite states.
- Section 4.6: Main results on one-way secret-key distillation from an arbitrary bipartite state. Numerical demonstration of the upper bounds on the one-shot, one-way distillable key of isotropic states using semidefinite programs.
- Section 4.7: Discussion of private communication over quantum channels using one-way LOCC superchannels. Review of the unextendible entanglement of channels induced by smooth-min relative entropy and α-geometric Rényi relative entropy. Main results on one-way private communication over an arbitrary channel.

Demonstrating the upper bound on the one-shot, forward-assisted private capacity of the erasure channel using analytical expressions.

4.3 Notation and Preliminaries

In this section, we review background material on the three major elements that we use in the rest of the work: quantum states, channels, and superchannels.

4.3.1 Quantum states and channels

A quantum state ρ_A is a positive semidefinite, unit-trace operator acting on a Hilbert space $\mathcal{H}_A$. We denote the set of all linear operators acting on the Hilbert space $\mathcal{H}_A$ by $\mathcal{L}(A)$ and the set of all quantum states acting on this Hilbert space by $\mathcal{S}(A)$. A bipartite quantum state ρ_{AB} acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is called separable if it can be written as

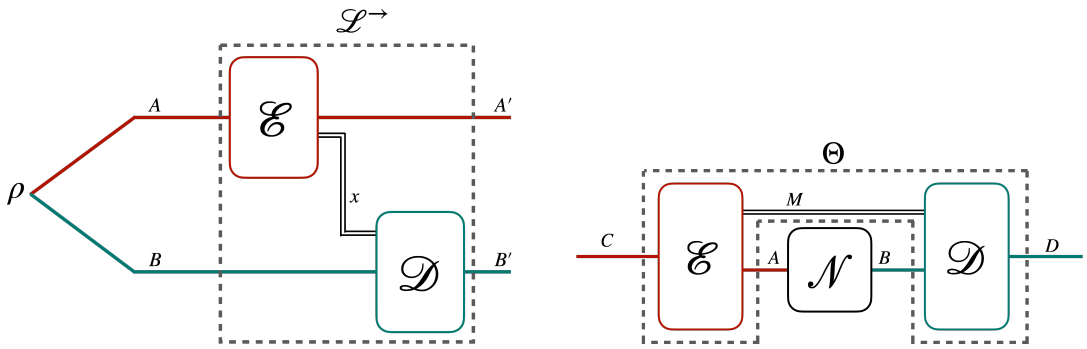
$$\rho_{AB} = \sum_{x \in \mathcal{X}} p(x) \sigma_A^x \otimes \tau_B^x, \tag{4.3.1}$$

where $\{p(x)\}_{x \in \mathcal{X}}$ is a probability distribution and $\{\sigma_A^x\}_{x \in \mathcal{X}}$ and $\{\tau_B^x\}_{x \in \mathcal{X}}$ are sets of states. Any quantum state that is not separable is said to be entangled. The maximally entangled state vector in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is denoted as follows:

$$|\Phi^d\rangle_{AB} \coloneqq \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A |i\rangle_B, \tag{4.3.2}$$

where $\{|i\rangle\}_{i=0}^{d-1}$ is an orthonormal basis and d is the Schmidt rank of the state. We denote the correponding density operator as $\Phi_{AB}^d \equiv |\Phi^d\rangle\langle\Phi^d|_{AB}$.

A quantum channel $\mathcal{N}_{A \to B}$ is a completely positive (CP) and trace-preserving (TP) linear map that takes an operator acting on the Hilbert space $\mathcal{H}_A$ as input and outputs an



(a) One-way LOCC channel (b) One-way LOCC superchannel

Figure 4.1: (a) Schematic diagram of a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'}$, as defined in (4.3.5), acting on a bipartite state ρ_{AB}. (b) Schematic diagram of a one-way LOCC superchannel $\Theta_{(A\to B)\to(C\to D)}$, defined in (4.3.6) with M being a classical system, acting on a channel $\mathcal{N}_{A\to B}$.

operator acting on the Hilbert space $\mathcal{H}_B$. We denote the Choi operator of a channel $\mathcal{N}_{A\to B}$ by $\Gamma^{\mathcal{N}}_{RB}$, which is defined as follows:

$$\Gamma^{\mathcal{N}}_{RB} \coloneqq \mathcal{N}_{A\to B}\left(d\Phi^{d}_{RA}\right), \tag{4.3.3}$$

where Φ^{d}_{RA} is the maximally entangled state of Schmidt rank d and system R is isomorphic to system A. The normalized Choi operator is called the Choi state of the channel, and it is defined as follows:

$$\Phi^{\mathcal{N}}_{RB} \coloneqq \mathcal{N}_{A\to B}\left(\Phi^{d}_{RB}\right). \tag{4.3.4}$$

An important class of channels that is central to our work consists of one-way LOCC channels. We use the symbol $\mathcal{L}^{\rightarrow}$ for a one-way LOCC channel.

A one-way LOCC channel is a quantum channel that acts on a bipartite state, and it can be physically described by the following sequence of operations: Say Alice and Bob share a bipartite state ρ_{AB}. Alice applies a quantum instrument $\left\{\mathcal{E}^{x}_{A\to A'}\right\}_{x\in\mathcal{X}}$ on her system, where x is a classical label corresponding to the outcome of the instrument. She sends the classical label x to Bob through an ideal classical channel. Bob then applies a quantum

channel $\mathcal{D}^x_{B\to B'}$ based on the label x that he received from Alice (see Figure 4.1a). A one-way LOCC channel can be mathematically described as follows:

$$\mathcal{L}^{\rightarrow}_{AB\to A'B'} = \sum_{x\in\mathcal{X}} \mathcal{D}^x_{A\to B} \otimes \mathcal{E}^x_{A\to A'}, \tag{4.3.5}$$

where $\left\{\mathcal{E}^x_{A\to A'}\right\}_{x\in\mathcal{X}}$ is a quantum instrument and $\left\{\mathcal{D}^x_{B\to B'}\right\}_{x\in\mathcal{X}}$ is a set of quantum channels.

4.3.2 Quantum superchannels

A quantum superchannel $\Theta_{(A\to B)\to(C\to D)}$ is a linear map that transforms a quantum channel to another quantum channel. Since quantum channels are completely positive and trace-preserving maps, a superchannel is a completely CPTP-preserving map (see Definition 4.1 for a formal definition). It can be perceived as a mathematical model for any physical transformation a quantum channel can undergo, as long as the resulting map is also a quantum channel. Quantum superchannels were introduced in [CDP08] and further investigated in [Gou19], both of which provide a detailed discussion. Here, we include a brief discussion on superchannels relevant to this work.

Definition 4.1 (Superchannel) *Let $\mathcal{T}_{A\to B} : \mathcal{L}(A) \to \mathcal{L}(B)$ be a linear map. Let the space of all such maps be denoted by $\mathbb{L}^{AB}$. A linear map $\Theta_{(A\to B)\to(C\to D)} : \mathbb{L}^{AB} \to \mathbb{L}^{CD}$ is a superchannel if*

1. *It is completely CP preserving; i.e., $(\mathrm{id}_{(E)\to(E)} \otimes \Theta_{(A\to B)\to(C\to D)})(\mathcal{T}_{EA\to EB})$ is a CP map if $\mathcal{T}_{EA\to E'B}$ is a CP map, for all possible dimensions of system E.*
2. *It is TP preserving; i.e., $\Theta_{(A\to B)\to(C\to D)}(\mathcal{T}_{A\to B})$ is a TP map if $\mathcal{T}_{A\to B}$ is a TP map.*

According to the fundamental theorem of superchannels [CDP08], every superchannel can be decomposed into a pre-processing channel $\mathcal{E}_{C\to MA}$ and a post-processing channel

$\mathcal{D}_{MB\to D}$ connected by a memory system M. That is, for every superchannel $\Theta_{(A\to B)\to(C\to D)}$, there exist $\mathcal{E}_{C\to MA}$ and $\mathcal{D}_{MB\to D}$ such that

$$\Theta_{(A\to B)\to(C\to D)}(\mathcal{N}_{A\to B}) = \mathcal{D}_{MB\to D} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}_{C\to MA}. \tag{4.3.6}$$

Quantum superchannels are a powerful tool in analyzing communication tasks over a quantum channel, as any communication protocol can be modeled as a superchannel.

A special class of superchannels that is relevant to this work is the class of one-way LOCC superchannels. This is the set of superchannels that can be simulated by local operations and forward classical communication (see Figure 4.1b). In particular, if system M in (4.3.6) is set to be a classical system, then every superchannel $\Theta_{(A\to B)\to(C\to D)}$ that has the form given in (4.3.6) is a one-way LOCC superchannel.

4.4 One-way secret-key distillation

In principle, the existence of a quantum network ensures unconditional secret key distribution [BB84, Eke91]. Alice and Bob can often manipulate a shared entangled state by means of local operations to obtain a maximally classically-correlated state that is completely independent of the system of any eavesdropper. The maximally-classically correlated state can then be used as a key to encrypt some classical data that Alice intends to send to Bob using the one-time-pad scheme. Since the eavesdropper is independent of the key shared between Alice and Bob, it is impossible for them to decode the encrypted data irrespective of their computational power. The state thus established between Alice, Bob, and an eavesdropper is called a tripartite key state, and it can be expressed in the

following form:

$$\tau_{ABE} = \frac{1}{K} \sum_{i=0}^{k-1} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes \sigma_E, \tag{4.4.1}$$

where σ_E is an arbitrary quantum state.

In general, the task of secret-key distillation is a three party problem due to the involvement of the eavesdropper. However, a crucial discovery was made in [HHHO05, HHHO09], establishing an equivalence between the tripartite scenario and a bipartite scenario involving the concept of a *private state*. In the next section, we briefly review the structure of bipartite private states, which plays an important role in this work.

4.4.1 Bipartite private states

A bipartite private state $\gamma^k_{ABA'B'}$ is the most general form of a quantum state that furnishes a secret key of $\log_2 k$ bits upon local measurements of systems A and B. Therefore, to establish a secret key whose secrecy is ensured by the laws of quantum mechanics, one needs to establish a bipartite private state.

It was shown in [HHHO05, HHHO09] that a private state $\gamma^k_{ABA'B'}$ holding $\log_2 k$ secret key bits can always be written in the following form:

$$\gamma^k_{ABA'B} = V_{ABA'B'} \left(\Phi^k_{AB} \otimes \tau_{A'B'} \right) V^\dagger_{ABA'B'}, \tag{4.4.2}$$

where Φ^k_{AB} is a maximally entangled state of Schmidt rank k, the operator $\tau_{A'B'}$ is an arbitrary bipartite state, and $V_{ABA'B'}$ is called a twisting unitary, defined as follows:

$$V_{ABA'B'} = \sum_{i=0}^{k-1} |i\rangle\langle i|_A \otimes I_B \otimes U^i_{A'B'}, \tag{4.4.3}$$

with $U^i_{A'B'}$ being some unitary operator. The private state in (4.4.2) can then be written more explicitly as follows:

$$\gamma^k_{ABA'B} = \sum_{i,j=0}^{k-1} |i\rangle\langle j|_A \otimes |i\rangle\langle j|_B \otimes U^i_{A'B'} \tau_{A'B'} \left(U^j_{A'B'}\right)^\dagger . \tag{4.4.4}$$

Systems A and B are said to be the key systems, and systems A' and B' are said to be the shield systems.

4.4.2 One-shot, one-way distillable key of a state

Let us now consider the task of distilling secret keys from a bipartite state shared between two parties using local operations and one-way classical communication. Since the distillation of a secret key is equivalent to the distillation of a bipartite private state, we consider the task of distilling a private state from bipartite resource state using one-way LOCC channels. However, distilling private states exactly, or even probabilistically, is a very restrictive task [SW24a], and one must relax this setting to allow for any practical distillation of secret keys.

The task of distilling approximate secret keys using one-way LOCC channels has been a subject of significant interest in several prior works [DW05, RR12, KKGW21] (see Figure 4.2 for a schematic diagram). The error in distillation of secret keys from a state ρ_{AB} using a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ is measured by the infidelity, defined as

$$p_{\text{err}}(\mathcal{L}^{\rightarrow};\rho_{AB}) := \inf_{\gamma^k_{A'B'A''B''}} \left(1 - F\left(\gamma^k_{A'B'A''B''}, \mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}(\rho_{AB})\right)\right), \tag{4.4.5}$$

where the infimum is over all bipartite private states holding $\log_2 k$ secret bits and $F(\cdot,\cdot)$ denotes the fidelity between two states, which is defined as follows:

$$F(\rho,\sigma) := \left(\text{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right]\right)^2 . \tag{4.4.6}$$

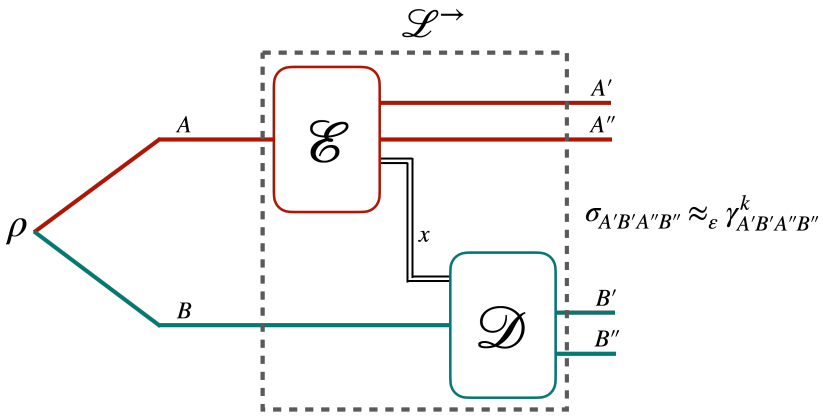


Figure 4.2: Schematic diagram of approximate distillation of a bipartite private state $\gamma^k_{A'B'A''B''}$ from a state ρ_{AB} using a one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$, where the error in distillation, denoted by ε, is defined in (4.4.5).

The reason for choosing infidelity to be the metric of error is motivated from the 'γ^k-privacy test' [HHH+08b, HHH+08a] (see [KW24, Section 15.1.3] for a detailed discussion. The γ^k-privacy test is a POVM $\left\{\Pi^{\gamma}_{ABA'B'}, I_{ABA'B'} - \Pi^{\gamma}_{ABA'B'}\right\}$, where

$$\Pi^{\gamma}_{ABA'B'} := V_{ABA'B'}\left(\Phi^k_{AB} \otimes I_{A'B'}\right) V^{\dagger}_{ABA'B'}, \tag{4.4.7}$$

The one-shot, one-way distillable key of a state is the quantity that describes the number of bits of secret key that can be established between two parties holding a resource state ρ_{AB}, with some error tolerance ε, when using one-way LOCC channels.

Definition 4.2 (One-shot, one-way distillable key) *For $\varepsilon \in [0,1]$, the one-shot, one-way distillable key of a state ρ_{AB} is defined as follows:*

$$K^{\varepsilon,\rightarrow}_{D}(\rho_{AB}) := \sup_{\substack{k\in\mathbb{N},\gamma^k_{A'B'A''B''},\\ \mathcal{L}^{\rightarrow}\in 1\text{WL}}} \left\{ \begin{array}{c} \log_2 k : \\ F\left(\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}(\rho_{AB}), \gamma^k_{A'B'A''B''}\right) \geq 1-\varepsilon \end{array} \right\}, \tag{4.4.8}$$

where 1WL *stands for the set of all one-way LOCC channels.*

In the above definition, the supremum is over every positive integer k, every private state $\gamma^k_{A'B'A''B''}$ holding $\log_2 k$ secret key bits, and every one-way LOCC channel

$\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$.

4.5 Two-extendibility

In this section we review the concepts of two-extendibility for states and channels. The resource theory of k-extendibility was developed in [KDWW19, KDWW21] as a semidefinite relaxation of the resource theory of entanglement, and the resource theory of two-extendibility is a special case when $k = 2$. A state-dependent resource theory of extendibility was developed in [WWW24], which is the framework that we employ to study the task of secret-key distillation with one-way LOCC channels.

4.5.1 Two-extendible states and channels

Let us first discuss two-extendible states [DPS04], also known as *symmetrically extendible states* [Wer89], *two-shareable states* [Yan06], and *anti-degradable states* [LDS18].

Definition 4.3 (Two-extendible state) *A bipartite state ρ_{AB} is said to be two-extendible if there exists a state ω_{ABE} such that the following conditions hold:*

$$\operatorname{Tr}_E[\omega_{ABE}] = \rho_{AB}, \tag{4.5.1}$$

and

$$W_{BE}(\omega_{ABE})W^{\dagger}_{BE} = \omega_{ABE}, \tag{4.5.2}$$

where the unitary swap operator W is defined as follows:

$$W_{BE} \coloneqq \sum_{k,k'=0}^{d-1} |k\rangle\langle k'|_B \otimes |k'\rangle\langle k|_E. \tag{4.5.3}$$

Note that the system E should be isomorphic to the system B for (4.5.1) and (4.5.2) to hold. The state ω_{ABE} is said to be a two-extension of the state ρ_{AB} if the conditions in (4.5.1) and (4.5.2) are met.

Remark 4.1 *All bipartite separable states are two-extendible. Consider an arbitrary bipartite separable state* $\rho_{AB} \coloneqq \sum_{x\in\mathcal{X}} p(x)\sigma_A^x \otimes \tau_B^x$, *where* $\{p(x)\}_{x\in\mathcal{X}}$ *is a probability distribution and* $\left\{\sigma_A^x\right\}_{x\in\mathcal{X}}$ *and* $\left\{\tau_B^x\right\}_{x\in\mathcal{X}}$ *are sets of quantum states. One can always construct the following two-extension of* ρ_{AB}*:*

$$\omega_{ABE} \coloneqq \sum_{x\in\mathcal{X}} p(x)\sigma_A^x \otimes \tau_B^x \otimes \tau_E^x, \tag{4.5.4}$$

which shows that all bipartite separable states are two-extendible. However, all two-extendible states are not separable. A simple example is the following isotropic state [HH99]:

$$\zeta_{AB} = \frac{5}{8}\Phi_{AB} + \frac{1}{8}\left(I_{AB} - \Phi_{AB}\right) = \frac{1}{2}\Phi_{AB} + \frac{1}{8}I_{AB}, \tag{4.5.5}$$

where A and B are two-dimensional systems, Φ_{AB} *is a two-qubit maximally entangled state, and* I_{AB} *is the identity operator. This state is two-extendible with the following two-extension:*

$$\omega_{ABE} = \frac{1}{4}\Phi_{AB} \otimes I_E + \frac{1}{4}\Phi_{AE} \otimes I_B, \tag{4.5.6}$$

but ζ_{AB} *has non-zero distillable entanglement [HH99], and hence, it is not a separable state.*

A family of semidefinite relaxations of one-way LOCC channels was developed in [KDWW19, KDWW21], called k-extendible channels. The set of k-extendible channels serves as the set of free channels in [KDWW19, KDWW21]. Setting $k = 2$, we obtain the set of two-extendible channels, which serves as the set of free operations in the state-dependent resource theory of unextendibility developed in [WWW24]. Here we briefly discuss the idea of two-extendible channels.

Definition 4.4 (Two-extendible channel) *A bipartite channel $\mathcal{N}_{AB\to A'B'}$ is said to be two-extendible if there exists a channel $\mathcal{P}_{ABE\to A'B'E'}$ such that the following conditions hold:*

$$\mathrm{Tr}_{E'} \circ \mathcal{P}_{ABE\to A'B'E'} = \mathcal{N}_{AB\to A'B'} \otimes \mathrm{Tr}_{E}, \tag{4.5.7}$$

and

$$\mathcal{W}_{B'E'} \circ \mathcal{P}_{ABE\to A'B'E'} = \mathcal{P}_{ABE\to A'B'E'} \circ \mathcal{W}_{BE}, \tag{4.5.8}$$

where $\mathcal{W}_{BE} := W_{BE}(\cdot)W_{BE}^{\dagger}$ with W_{BE} defined in (4.5.3). The conditions in (4.5.7) and (4.5.8) are known as the channel extension condition and the permutation covariance condition, respectively.

The channel $\mathcal{P}_{ABE\to A'B'E'}$ is said to be a two-extension of $\mathcal{N}_{AB\to A'B'}$ if the channel extension and permutation covariance conditions, mentioned in (4.5.7) and (4.5.8) respectively, hold.

If a channel $\mathcal{N}_{AB\to A'B'}$ is two-extendible, then it is non-signaling from B to A [HSW23, Appendix A]; that is,

$$\mathrm{Tr}_{B'} \circ \mathcal{N}_{AB\to A'B'} = \mathrm{Tr}_{B'} \circ \mathcal{N}_{AB\to A'B'} \circ \mathcal{R}_{B}^{\pi}, \tag{4.5.9}$$

where $\mathcal{R}_{B}^{\pi}$ is a channel that traces out the input and replaces it with a maximally mixed state. Moreover, all one-way LOCC channels are two-extendible, as can be seen from a simple construction. An arbitrary one-way LOCC channel can be written in the following form:

$$\mathcal{N}_{AB\to A'B'} = \sum_{x\in\mathcal{X}} \mathcal{E}^{x}_{A\to A'} \otimes \mathcal{F}^{x}_{B\to B'}, \tag{4.5.10}$$

where $\left\{\mathcal{E}^{x}_{A\to A'}\right\}_{x\in\mathcal{X}}$ is a quantum instrument and $\left\{\mathcal{F}^{x}_{B\to B'}\right\}_{x\in\mathcal{X}}$ is a set of quantum channels. A two-extension of this channel can be constructed as follows:

$$\mathcal{P}_{ABE\to A'B'E'} = \sum_{x\in\mathcal{X}} \mathcal{E}^{x}_{A\to A'} \otimes \mathcal{F}^{x}_{B\to B'} \otimes \mathcal{F}^{x}_{E\to E'}. \tag{4.5.11}$$

Hence, every one-way LOCC channel is two-extendible.

On the contrary, all two-extendible channels cannot be simulated by local operations and one-way classical communication. Consider the example of a bipartite channel that traces out the input and replaces it with the state mentioned in (4.5.6), which can be mathematically represented as follows:

$$\mathcal{N}_{AB\to A'B'}(\cdot) = \mathrm{Tr}[\cdot]\left(\frac{1}{2}\Phi_{AB} + \frac{1}{2}\frac{I_{AB}}{4}\right). \tag{4.5.12}$$

Since this channel is capable of taking a separable state as input and establishing an entangled state, it is not a one-way LOCC channel. However, one can construct the following two-extension of the channel:

$$\mathcal{P}_{ABE\to A'B'E'}(\cdot) \coloneqq \mathrm{Tr}[\cdot]\left(\frac{1}{4}\Phi_{A'B'}\otimes I_{E'} + \frac{1}{4}\Phi_{A'E'}\otimes I_{B'}\right). \tag{4.5.13}$$

Therefore, the channel defined in (4.5.12) is an example of a two-extendible channel that is not a one-way LOCC channel.

4.5.2 Unextendible entanglement of states

Let $\mathbb{R}$ denote the field of real numbers. A generalized divergence [PV10] is a functional $\mathbf{D}\colon \mathcal{S}(A)\times\mathcal{S}(A)\to\mathbb{R}\cup\{+\infty\}$, such that, for arbitrary states $\rho_A,\sigma_A\in\mathcal{S}(A)$ and an arbitrary channel $\mathcal{N}_{A\to B}$, the data-processing inequality holds

$$\mathbf{D}(\rho_A\|\sigma_A) \geq \mathbf{D}(\mathcal{N}_{A\to B}(\rho_A)\|\mathcal{N}_{A\to B}(\sigma_A))\,. \tag{4.5.14}$$

Some examples of divergences that commonly appear in quantum information theory are the quantum relative entropy [Ume62], Petz-Rényi relative entropies [Pet86], sandwiched Rényi relative entropies [MLDS+13, WWY14], and geometric Rényi relative entropies [Mat13, FF21].

The generalized unextendible entanglement of a bipartite state has been defined in [WWW24]. We include a short discussion on the topic for necessary development.

Definition 4.5 ([WWW24]) *The generalized unextendible entanglement of a bipartite state ρ_{AB}, induced by a generalized divergence* $\mathbf{D}$ *between states, is defined as*

$$\mathbf{E}^u(\rho_{AB}) \coloneqq \inf_{\omega_{ABE}\in\mathcal{S}(ABE)} \frac{1}{2}\Big\{\mathbf{D}(\rho_{AB}\|\operatorname{Tr}_B[\omega_{ABE}]) : \operatorname{Tr}_E[\omega_{ABE}] = \rho_{AB}\Big\}, \tag{4.5.15}$$

where the optimization is over every state ρ_{ABE} that is an extension of the state ρ_{AB}. We also adopt the following alternative notations sometimes because they can be helpful to make the bipartition $A|B$ clear:

$$\mathbf{E}^u(A;B)_\rho \equiv \mathbf{E}^u(\rho_{A:B}) \equiv \mathbf{E}^u(\rho_{AB}). \tag{4.5.16}$$

Let us define the following set of extensions of a bipartite state ρ_{AB}:

$$\operatorname{Ext}(\rho_{AB}) \coloneqq \{\omega_{ABE} : \operatorname{Tr}_{BE}[\omega_{ABE}] = \rho_{AB}\}, \tag{4.5.17}$$

where E is isomorphic to B. This allows us to write the generalized unextendible entanglement of ρ_{AB}, induced by the generalized divergence $\mathbf{D}$, as

$$\mathbf{E}^u(\rho_{AB}) = \inf_{\omega_{ABE}\in\operatorname{Ext}(\rho_{AB})} \frac{1}{2}\mathbf{D}(\rho_{AB}\|\operatorname{Tr}_E[\omega_{ABE}]). \tag{4.5.18}$$

Alternatively, one can define the set of state-dependent free states as follows:

$$\mathcal{F}(\rho_{AB}) \coloneqq \{\operatorname{Tr}_B[\omega_{ABE}] : \omega_{ABE} \in \operatorname{Ext}(\rho_{AB})\}. \tag{4.5.19}$$

The generalized unextendible entanglement of the state ρ_{AB} can then be written as follows:

$$\mathbf{E}^u(\rho_{AB}) = \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2}\mathbf{D}(\rho_{AB}\|\sigma_{AB}). \tag{4.5.20}$$

Theorem 4.1 ([WWW24]) *The generalized unextendible entanglement of bipartite state does not increase under the action of a two-extendible channel. That is,*

$$\mathbf{E}^u(\rho_{AB}) \geq \mathbf{E}^u(\mathcal{N}_{AB\to A'B'}(\rho_{AB}))\,, \tag{4.5.21}$$

where $\mathcal{N}_{AB\to A'B'}$ is a two-extendible channel.

Proof: See Theorem 2 in [WWW24]. □

A direct consequence of Theorem 4.1 is that the generalized unextendible entanglement of a bipartite state does not increase under the action of one-way LOCC channels.

The generalized unextendible entanglement provides a framework for quantifying the unextendibility of a bipartite state ρ_{AB} with respect to the system B. A different measure for unextendibility was considered in [KDWW19, KDWW21], where the divergence was measured from the fixed set of two-extendible states. However, in Definition 4.5, the divergence is measured by means of a set of states that depend on the input state itself. Although both measures are equal to the minimal possible value of $\mathbf{D}$ when ρ_{AB} is two-extendible, they are not equal in general.

The unextendible entanglement is a measure of entanglement between two systems, and as such, it is expected to obtain its maximum value for the maximally entangled state. This is indeed the case, as is evident from the following argument. An arbitrary bipartite state ρ_{AB} can be established between Alice and Bob with the help of a maximally entangled state $\Phi^d_{A_0B_0}$ of sufficiently large Schmidt rank and a one-way LOCC channel, where $\dim(A_0) = \dim(B_0) = \min\{\dim(A), \dim(B)\}$. A simple protocol to perform this transformation is as follows: Alice prepares the state $\rho_{AA'}$ locally. We can assume $\dim(A') \leq \dim(A)$ without loss of generality. She uses the maximally entangled state $\Phi^d_{A_0B_0}$ to implement

the teleportation protocol and send the state on system A' to Bob, thus establishing the state ρ_{AB} between Alice and Bob. The aforementioned protocol can be mathematically represented as the following one-way LOCC channel [KW24, Chapter 5]:

$$\mathcal{L}^{\rho,\rightarrow}_{A_0B_0\rightarrow AB}\left(\Phi^d_{A_0B_0}\right) = \sum_{x,z=0}^{d-1} \mathrm{Tr}_{A_0A'}\left[\Phi^{z,x}_{A_0A'} W^{z,x}_{B_0} \left(\rho_{AA'} \otimes \Phi_{A_0B_0}\right) \left(W^{z,x}_{B_0}\right)^\dagger\right], \tag{4.5.22}$$

where $\{W^{z,x}\}_{z,x}$ is the set of Heisenberg–Weyl operators and $\Phi^{z,x}_{A_0A'} := W^{z,x}_{A_0}\Phi^d_{A_0A'}(W^{z,x}_{A_0})^\dagger$. Since the generalized unextendible entanglement of a bipartite state does not increase under the action of a one-way LOCC channel, the following inequality holds for every state ρ_{AB}:

$$\mathbf{E}^u(\rho_{AB}) = \mathbf{E}^u\left(\mathcal{L}^{\rho,\rightarrow}_{A_0B_0\rightarrow AB}\left(\Phi^d_{A_0B_0}\right)\right) \leq \mathbf{E}^u\left(\Phi^d_{A_0B_0}\right), \tag{4.5.23}$$

where $\mathcal{L}^{\rho,\rightarrow}_{A_0B_0\rightarrow AB}$ is the channel defined in (4.5.22) and $d := \min\{\dim(A), \dim(B)\}$.

Smooth-min unextendible entanglement

The unextendible entanglement of states was studied in detail in [WWW24] for several different underlying divergences, with applications in finding efficiently computable upper bounds on the probabilistic and exact one-way distillable entanglement and key of a state. A stronger no-go theorem for probabilistic key distillation was obtained in [SW24a] using the min-relative entropy as the underlying divergence for the unextendible entanglement. In this work, we are specifically interested in the unextendible entanglement of a state induced by the smooth-min relative entropy to understand the limits of one-shot approximate distillable key of a bipartite state using one-way LOCC channels. As a special case of (4.5.15), we define the smooth min-unextendible entanglement as follows:

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) := \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2} D^\varepsilon_{\min}(\rho_{AB}\|\sigma_{AB}), \tag{4.5.24}$$

where the set $\mathcal{F}(\rho_{AB})$ was defined in (4.5.19) and

$$D^\varepsilon_{\min}(\rho\|\sigma) := -\log_2 \inf_{0\leq\Lambda\leq I} \{\mathrm{Tr}[\Lambda\sigma] : \mathrm{Tr}[\Lambda\rho] \geq 1-\varepsilon\} \tag{4.5.25}$$

is the smooth-min relative entropy [BD10, BD11], also known as the hypothesis testing relative entropy [WR12].

We will often use the following quantity in our discussions:

$$J^{\varepsilon}_{\min}(\rho_{AB}) := 2^{-2E^{u,\varepsilon}_{\min}(\rho_{AB})}, \tag{4.5.26}$$

which we will abbreviate as $J^{\varepsilon}_{\min}$ when the state it acts upon is obvious from the context. The quantity $J^{\varepsilon}_{\min}(\rho_{AB})$ can alternatively be written as follows:

$$J^{\varepsilon}_{\min}(\rho_{AB}) = \sup_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \inf_{0\leq\Lambda\leq I} \{\mathrm{Tr}[\Lambda\sigma] : \mathrm{Tr}[\Lambda\rho] \geq 1-\varepsilon\}. \tag{4.5.27}$$

The set $\mathcal{F}(\rho_{AB})$ is a convex set of quantum states, and the set $\{\Lambda : 0 \leq \Lambda \leq I : \mathrm{Tr}[\Lambda\rho] \geq 1-\varepsilon\}$ is a convex set of measurement operators for a fixed state ρ. Therefore, using Sion's minimax theorem [Sio58], we can interchange the supremum and infimum to arrive at the following equality:

$$J^{\varepsilon}_{\min}(\rho_{AB}) = \inf_{0\leq\Lambda\leq I} \sup_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \{\mathrm{Tr}[\Lambda\sigma] : \mathrm{Tr}[\Lambda\rho] \geq 1-\varepsilon\}. \tag{4.5.28}$$

The above equality gives an interpretation for the quantity $J^{\varepsilon}_{\min}(\rho_{AB})$ in the hypothesis testing setting. Given a quantum state ρ_{AB} and an arbitrary state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$, the quantity $J^{\varepsilon}_{\min}(\rho_{AB})$ denotes the minimum type-II error probability in the worst case when the type-I error probability is guaranteed to be less than ε. Note that the quantity $J^{\varepsilon}_{\min}$ decreases monotonically with increasing smooth-min unextendible entanglement. As such, $J^{\varepsilon}_{\min}$ is smaller for highly entangled states and larger for weakly entangled states, and the minimum value is achieved for the maximally entangled state due to (4.5.23).

Proposition 4.1 *The unextendible entanglement of a maximally entangled state with Schmidt rank d is equal to the following:*

$$E^{u,\varepsilon}_{\min}\left(\Phi^{d}_{AB}\right) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \tag{4.5.29}$$

Proof: See Appendix 4.A. □

Proposition 4.2 *The smooth-min unextendible entanglement of a state ρ_{AB} is bounded as follows:*

$$-\frac{1}{2}\log_2(1-\varepsilon) \leq E_{\min}^{u,\varepsilon}(\rho_{AB}) \leq \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), \tag{4.5.30}$$

where $d \coloneqq \min\{\dim(A), \dim(B)\}$ with $\dim(A)$ and $\dim(B)$ being the dimensions of system A and B, respectively.

Consequently,

$$\frac{1-\varepsilon}{d^2} \leq J^{\varepsilon}(\rho_{AB}) \leq 1-\varepsilon. \tag{4.5.31}$$

Proof: See Appendix 4.B. □

The smooth-min unextendible entanglement of a bipartite state can be computed using a semidefinite program (see Appendix 4.H).

α-Sandwiched unextendible entanglement

Another quantity that is relevant to this work is the α-sandwiched unextendible entanglement [WWW24], which is defined as follows:

$$\widetilde{E}_{\alpha}^{u}(\rho_{AB}) \coloneqq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2}\widetilde{D}_{\alpha}(\rho_{AB}\|\sigma_{AB}) \qquad \forall \alpha \in (1,\infty)\,, \tag{4.5.32}$$

where

$$\widetilde{D}_{\alpha}(\rho\|\sigma) \coloneqq \frac{1}{\alpha-1}\log_2 \operatorname{Tr}\left[\left(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right)^{\alpha}\right] \tag{4.5.33}$$

is the α-sandwiched Rényi relative entropy [MLDS+13, WWY14]. The α-sandwiched unextendible entanglement was defined for all $\alpha \in (0,1)\cup(1,\infty)$ in [WWW24], but we restrict

our development here to $\alpha \in (1, \infty)$, due to technical reasons that will become apparent in Section 4.6.

Consider the special case when $\alpha \to \infty$. It was shown in [MLDS+13, Theorem 5] that the α-sandwiched relative entropy is equal to the max-relative entropy [Dat09] when $\alpha \to \infty$; that is,

$$D_{\max}(\rho\|\sigma) = \lim_{\alpha\to\infty} \widetilde{D}_\alpha(\rho\|\sigma)\,. \tag{4.5.34}$$

Corresponding to the max-relative entropy, the max-unextendible entanglement is defined as follows:

$$E^u_{\max}(\rho_{AB}) := \frac{1}{2} \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} D_{\max}(\rho_{AB}\|\sigma_{AB})\,. \tag{4.5.35}$$

Besides monotonicity under two-extendible channels, the α-sandwiched unextendible entanglement has several other properties desirable in a resource monotone. We state some of the relevant properties below.

- **Subadditivity:** The α-sandwiched unextendible entanglement obeys the following subadditivity inequality [WWW24, Proposition 13]

$$\widetilde{E}^u_\alpha(\rho_{A_1B_1}\otimes\sigma_{A_2B_2}) \le \widetilde{E}^u_\alpha(\rho_{A_1B_1}) + \widetilde{E}^u_\alpha(\sigma_{A_2B_2}) \qquad \forall \alpha \in \left[\frac{1}{2}, 1\right) \cup (1, \infty)\,. \tag{4.5.36}$$

- **Additivity of max-unextendible entanglement:** The max-unextendible entanglement is additive under tensor product of states [WWW24, Proposition 14]; that is,

$$E^u_{\max}(\rho_{A_1B_1}\otimes\sigma_{A_2B_2}) = E^u_{\max}(\rho_{A_1B_1}) + E^u_{\max}(\sigma_{A_2B_2})\,. \tag{4.5.37}$$

- **Monotonicity in α:** The α-sandwiched unextendible entanglement of a state increases monotonically with increasing α, which follows from the fact that the α-sandwiched Rényi relative entropy between two states increases monotonically with α [MLDS+13, Theorem 7].

- **Semidefinite representation:** The max-unextendible entanglement can be computed using a semidefinite program [WWW24] (see Appendix 4.H for a review).

The max-unextendible entanglement of a state can be written as a limiting case of the α-sandwiched unextendible entanglement as follows:

$$\lim_{\alpha\to\infty} \widetilde{E}^{u}_{\alpha}(\rho_{AB}) = \sup_{\alpha\in(1,\infty)} \frac{1}{2} \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \widetilde{D}_{\alpha}(\rho_{AB}\|\sigma_{AB}) \tag{4.5.38}$$

$$= \frac{1}{2} \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \sup_{\alpha\in(1,\infty)} \widetilde{D}_{\alpha}(\rho_{AB}\|\sigma_{AB}) \tag{4.5.39}$$

$$= \frac{1}{2} \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} D_{\max}(\rho_{AB}\|\sigma_{AB}) \tag{4.5.40}$$

$$= E^{u}_{\max}(\rho_{AB}), \tag{4.5.41}$$

where the first equality follows from the monotonicity of the α-sandwiched unextendible entanglement in α. The α-sandwiched Rényi relative entropy $\widetilde{D}_{\alpha}(\rho\|\sigma)$ is lower-semicontinuous with respect to σ [MO21, Lemma IV.8] (see also [DKQ+23, Remark 38]), and it increases monotonically with $\alpha \in (1,\infty)$. Therefore, we can use the Mosonyi–Hiai minimax theorem from [MH11, Corollary A.2] to arrive at the second equality above. The last two equalities follow from the equality in (4.5.34) and the definition of the max-unextendible entanglement, respectively.

The subadditivity of α-sandwiched unextendible entanglement is useful in the analysis of one-shot, one-way secret-key distillation from independent and identically distributed (i.i.d.) copies of a bipartite state, as we shall see in Section 4.6.2.

4.6 Limits on secret-key distillation from bipartite states

In this section we use the framework of unextendible entanglement discussed in Section 4.5 to obtain upper bounds on the one-shot, one-way distillable key of a state defined in (4.4.8).

Consider a quantum state $\psi^{\gamma}_{ABA'B'E}$, which is an extension of a private state $\gamma^{k}_{ABA'B'}$ with system E held by an eavesdropper. The reduced state of $\psi^{\gamma}_{ABA'B'E}$ on systems AE is a product state, with the reduced state on system A being the maximally mixed state. This is evident from the equivalence between a bipartite private state and a tripartite secret-key state. It was further shown in [WWW24, Appendix K] that applying a twisting unitary on the joint systems of Alice and the eavesdropper is also insufficient to establish any correlations between Alice's key system, A, and the eavesdropper's system, E. We state this formally in Lemma 4.1, which we later use to establish the main results of this work.

Lemma 4.1 ([WWW24]) *Let $\psi^{\gamma}_{ABA'B'EE'R}$ be a purification of a bipartite private state $\gamma^{k}_{ABA'B'}$. For every purification for which system E is isomorphic to B and system E' is isomorphic to B', the following equality holds:*

$$\mathrm{Tr}_{A'BB'E'R}\left[W^{\dagger}_{AEA'E'}\psi^{\gamma}W_{AEA'E'}\right] = \pi_A \otimes \sigma_E, \tag{4.6.1}$$

where τ_E is a quantum state, π_A is the maximally mixed state, and $W_{AEA'E'}$ is a twisting unitary of the form given in (4.4.3).

Proof: See [WWW24, Appendix K]. □

The fact that Alice's system is in a product state with the eavesdropper ensures that the state shared by Alice and the eavesdropper does not pass the privacy test with a

probability greater than $\frac{1}{k}$. We generalize this statement to approximate private states in Lemma 4.2 below.

Lemma 4.2 *Fix $k \in \mathbb{N}$ and $\varepsilon \in \left[0, 1 - \frac{1}{k^2}\right]$. Let $\sigma_{ABA'B'}$ be a quantum state such that*

$$F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1 - \varepsilon, \tag{4.6.2}$$

where $\gamma^k_{ABA'B'}$ is a bipartite private state holding $\log_2 k$ secret key bits. Let $V_{ABA'B'}$ be the twisting unitary corresponding to the private state; that is, there exists a state $\tau_{A'B'}$ such that

$$\gamma^k_{ABA'B'} = V_{ABA'B'}\left(\Phi^k_{AB} \otimes \tau_{A'B'}\right) V^\dagger_{ABA'B'}. \tag{4.6.3}$$

The probability of an arbitrary state $\omega_{AEA'E'} \in \mathcal{F}(\sigma_{ABA'B'})$ passing the γ^k-privacy test is bounded from above by the following quantity:

$$\operatorname{Tr}\left[\Pi^\gamma_{AEA'E'} \omega_{AEA'E'}\right] \leq \varsigma(\varepsilon, k), \tag{4.6.4}$$

where

$$\varsigma(\varepsilon, k) := \varepsilon + \frac{1 - 2\varepsilon}{k^2} + \frac{2\sqrt{(k^2 - 1)\varepsilon(1 - \varepsilon)}}{k^2}, \tag{4.6.5}$$

$\Pi^\gamma_{ABA'B'}$ is the privacy test, system B is isomorphic to E, and system B' is isomorphic to E'. The set $\mathcal{F}(\sigma_{ABA'B'})$ was defined in (4.5.19).

Proof: Let $\phi^\sigma_{ABA'B'EE'R}$ be an arbitrary purification of $\sigma_{ABA'B'}$, such that system E is isomorphic to B and system E' is isomorphic to B'. Then the quantum state $\operatorname{Tr}_{BB'R}[\phi^\sigma]$ is in the set $\mathcal{F}(\sigma_{ABA'B'})$. Let $\psi^\gamma_{ABA'B'EE'R}$ be a purification of $\gamma^k_{ABA'B'}$. An arbitrary purification of the private state $\gamma^k_{ABA'B'}$ is of the following form:

$$\psi^\gamma_{ABA'B'X} = V_{ABA'B'}\left(\Phi^k_{AB} \otimes \psi^\tau_{A'B'X}\right) V^\dagger_{ABA'B'}, \tag{4.6.6}$$

where $\psi^\tau_{A'B'X}$ is a pure state and X is a purifying system.

As a consequence of Uhlmann's theorem, consider that

$$F\left(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}\right) = \max_{\psi^\gamma} |\langle \psi^\gamma | \phi^\sigma \rangle|^2 \tag{4.6.7}$$

$$= \max_{\psi^\gamma} F\left(\psi^\gamma_{ABA'B'EE'R}, \phi^\sigma_{ABA'B'EE'R}\right) \tag{4.6.8}$$

$$= \max_{\psi^\tau_{A'B'EE'R}} F\left(V_{ABA'B'}\left(\Phi^k_{AB} \otimes \psi^\tau_{A'B'EE'R}\right) V^\dagger_{ABA'B'}, \phi^\sigma_{ABA'B'EE'R}\right). \tag{4.6.9}$$

The maximizations in the first and second equalities are over every purification ψ^γ of $\gamma^k_{ABA'B'}$ on the systems $ABA'B'EE'R$. Since every purification of the state $\gamma^k_{ABA'B'}$ can be written in the form mentioned in (4.6.6), the maximization over every purification $\psi^\gamma_{ABA'B'EE'R}$ is equivalent to a maximization over every purification $\psi^\tau_{A'B'EE'R}$ of the state $\tau_{A'B'}$. Therefore, there exists a pure state $\psi^\tau_{A'B'EE'R}$ and a corresponding purification $\psi^\gamma_{ABA'B'EE'R}$ such that the following equality holds:

$$F\left(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}\right) = |\langle \psi^\gamma | \phi^\sigma \rangle|^2 = F(\psi^\gamma, \phi^\sigma). \tag{4.6.10}$$

Using the data-processing inequality for fidelity of states, consider that

$$F(\psi^\gamma, \phi^\sigma) \leq F\left(\mathrm{Tr}_{A'BB'E'R}\left[V^\dagger_{AEA'E'} \psi^\gamma V_{AEA'E'}\right], \mathrm{Tr}_{A'BB'E'R}\left[V^\dagger_{AEA'E'} \phi^\sigma V_{AEA'E'}\right]\right) \tag{4.6.11}$$

$$= F\left(\pi_A \otimes \tau_E, \mathrm{Tr}_{A'E'}\left[V^\dagger_{AEA'E'} \omega_{AEA'E'} V_{AEA'E'}\right]\right), \tag{4.6.12}$$

where we have used Lemma 4.1 to arrive at the final equality and $\omega_{AEA'E'}$ is defined in the statement of the lemma.

Now consider the twirling channel, defined as follows:

$$\mathcal{T}_{AB}(\cdot) = \int dU \left(U_A \otimes \overline{U}_B\right)(\cdot)\left(U_A \otimes \overline{U}_B\right)^\dagger, \tag{4.6.13}$$

where the integral is with respect to the Haar measure. The action of this channel on an arbitrary quantum state ρ_{AB}, with $\dim(A) = \dim(B) = d$, results in the following isotropic

state [HH99, Wat18]:

$$\mathcal{T}_{AB}(\rho_{AB}) = \operatorname{Tr}\left[\Phi^d_{AB}\rho_{AB}\right]\Phi^d_{AB} + \left(1 - \operatorname{Tr}\left[\Phi^d_{AB}\rho_{AB}\right]\right)\frac{I_{AB} - \Phi^d_{AB}}{d^2 - 1}. \tag{4.6.14}$$

Consider that

$$\begin{aligned}\operatorname{Tr}\left[\Phi^k_{AE}\left(\pi_A \otimes \tau_E\right)\right] &= \frac{1}{k}\operatorname{Tr}\left[\Phi^k_{AE}(I_A \otimes \tau_E)\right] &(4.6.15)\\ &= \frac{1}{k^2}\operatorname{Tr}[\tau_E] &(4.6.16)\\ &= \frac{1}{k^2}. &(4.6.17)\end{aligned}$$

Therefore,

$$\mathcal{T}_{AE}(\pi_A \otimes \tau_E) = \frac{1}{k^2}\Phi^k_{AE} + \left(1 - \frac{1}{k^2}\right)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1} = \frac{I_{AE}}{k^2}. \tag{4.6.18}$$

The action of the twirling channel $\mathcal{T}_{AE}$ on the state $\operatorname{Tr}_{A'E'}\left[V^\dagger \omega_{AEA'E'} V\right]$ is given by the following expression:

$$\mathcal{T}_{AE}\left(\operatorname{Tr}_{A'E'}\left[V^\dagger \omega_{AEA'E'} V\right]\right) = q\,\Phi^k_{AE} + (1-q)\,\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}, \tag{4.6.19}$$

where

$$q := \operatorname{Tr}\left[\Phi^k_{AE}\left(\operatorname{Tr}_{A'E'}\left[V^\dagger \omega_{AEA'E'} V\right]\right)\right]. \tag{4.6.20}$$

The above expression can be rewritten as follows:

$$q = \operatorname{Tr}\left[V_{AEA'E'}\left(\Phi^k_{AE} \otimes I_{A'E'}\right)V^\dagger_{AEA'E'}\omega_{AEA'E'}\right] = \operatorname{Tr}\left[\Pi^\gamma_{AEA'E'}\omega_{AEA'E'}\right], \tag{4.6.21}$$

where $\Pi^\gamma_{AEA'E'}$ is the γ-privacy test defined in (4.4.7). Therefore, q can be interpreted as the probability of the state $\omega_{AEA'E'}$ passing the γ-privacy test.

Going back to (4.6.12) and using the data-processing inequality for fidelity, we arrive at the following inequality:

$$F(\psi^\gamma, \phi^\sigma) \leq F\left(\mathcal{T}_{AE}(\pi_A \otimes \tau_E), \mathcal{T}_{AE}\left(\operatorname{Tr}_{A'E'}\left[V^\dagger \omega V\right]\right)\right) \tag{4.6.22}$$

$$= F\Big(\pi_{AE}, \mathcal{T}_{AE}\Big(\mathrm{Tr}_{A'E'}\Big[V^\dagger \omega V\Big]\Big)\Big). \tag{4.6.23}$$

Since the above inequality holds for all $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1-\varepsilon$ for some private state $\gamma^k_{ABA'B'}$ and every $\omega_{AEA'E'}$ that is in the set $\mathcal{F}(\sigma_{ABA'B'})$, we can combine (4.6.10), (4.6.12), and (4.6.23) to arrive at the following inequality:

$$1-\varepsilon \leq F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \tag{4.6.24}$$

$$\leq F\Big(\pi_{AE}, \mathcal{T}_{AE}\Big(\mathrm{Tr}_{A'E'}\Big[V^\dagger \omega V\Big]\Big)\Big) \tag{4.6.25}$$

$$= F\left(\pi_{AE}, q\, \Phi^k_{AE} + (1-q)\frac{I_{AE} - \Phi^k_{AE}}{k^2-1}\right) \tag{4.6.26}$$

$$= \left(\sqrt{\frac{q}{k^2}} + \sqrt{(1-q)\left(1-\frac{1}{k^2}\right)}\right)^2, \tag{4.6.27}$$

where the first equality follows from (4.6.19) and the last equality follows by evaluating the fidelity between the two isotropic states.

The inequality in (4.6.27) is satisfied for all $q \in [0,1]$ if $\varepsilon \geq 1 - \frac{1}{k^2}$. If $\varepsilon \in \left[0, 1-\frac{1}{k^2}\right]$ then q must lie in the following range for (4.6.27) to hold:

$$0 \leq q \leq \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2}. \tag{4.6.28}$$

See Appendix 4.C for a detailed proof of the aforementioned statement. Since we have identified q to be the probability of the state $\omega_{AEA'E'}$ passing the γ-privacy test, we conclude the statement of the lemma. □

Lemma 4.2 plays a central role in obtaining lower bounds on the unextendible entanglement of an approximate private state $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1-\varepsilon$ for some private state $\gamma^k_{ABA'B'}$.

Remark 4.2 *Note that $F\left(\pi_{AB}, \Phi^k_{AB}\right) = \frac{1}{k^2}$, where π_{AB} is the maximally mixed state. Therefore, if $\varepsilon \geq 1 - \frac{1}{k^2}$ for some $k \in \mathbb{N}$, then the following inequality holds for the one-shot, one-way distillable*

key of an arbitrary bipartite state ρ_{AB}:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \geq \log_2 k. \tag{4.6.29}$$

As such, choosing $\varepsilon \geq 1 - \frac{1}{k^2}$ allows the one-shot, one-way distillable key of a separable state to be non-zero, which makes this regime uninteresting from a practical perspective.

4.6.1 Smooth-min unextendible entanglement upper bound on one-shot distillable secret key of bipartite states

The γ-privacy test is a special POVM that can be used to distinguish a bipartite state $\sigma_{ABA'B'}$ from any state $\omega_{AEA'E'} \in \mathcal{F}(\sigma_{ABA'B'})$. Recall that the smooth-min unextendible entanglement quantifies the ability to distinguish between a state ρ_{AB} from an arbitrary state $\sigma_{AB} \in \mathcal{F}(\rho_{AB})$. Therefore, Lemma 4.2 allows us to obtain a bound on the unextendible entanglement of a state $\sigma_{ABA'B'}$ satisfying $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1 - \varepsilon$. This is stated as Proposition 4.3 below.

Proposition 4.3 *Fix $k \in \mathbb{N}$ and $\varepsilon \in \left[0, 1 - \frac{1}{k^2}\right]$. Consider a quantum state $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1 - \varepsilon$, where $\gamma^k_{ABA'B}$ is a bipartite private state. The smooth-min unextendible entanglement of the state $\sigma_{ABA'B'}$ is bounded from below by the following quantity:*

$$E_{\min}^{u,\varepsilon}(\sigma_{ABA'B'}) \geq -\frac{1}{2}\log_2(\varsigma(\varepsilon, k)), \tag{4.6.30}$$

where $\varsigma(\varepsilon, k)$ is defined in (4.6.5).

Proof: Let $\sigma_{ABA'B'}$ be a quantum state such that $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1-\varepsilon$ for some bipartite private state $\gamma^k_{ABA'B'}$ and some $\varepsilon \in \left[0, 1 - \frac{1}{k^2}\right]$. The following inequality holds for every such

state $\sigma_{ABA'B'}$ [WTB17, Lemma 9]:

$$\operatorname{Tr}\left[\Pi^{\gamma}_{ABA'B'}\sigma_{ABA'B'}\right] \geq 1-\varepsilon, \tag{4.6.31}$$

where the projector $\Pi^{\gamma}_{ABA'B'}$ is the γ^k-privacy test defined in (4.4.7).

Now consider the hypothesis testing relative entropy between the state $\sigma_{ABA'B'}$, for which $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1-\varepsilon$ for some private state $\gamma^k_{ABA'B'}$, and an arbitrary state $\omega_{AEA'E'}$ which lies in the set $\mathcal{F}(\sigma_{ABA'B'})$:

$$D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) = \sup_{0\leq\Lambda\leq I} -\log_2\left\{\operatorname{Tr}[\Lambda\omega] : \operatorname{Tr}[\Lambda\sigma] \geq 1-\varepsilon\right\}. \tag{4.6.32}$$

It is understood here that system E is isomorphic to B and system E' is isomorphic to B'.

Since $\Pi^{\gamma}_{ABA'B'}$ is a specific measurement operator that satisfies the constraints in (4.6.32), the following inequality holds:

$$D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) \geq -\log_2 \operatorname{Tr}\left[\Pi^{\gamma}_{AEA'E'}\omega_{AEA'E'}\right], \tag{4.6.33}$$

which leads to the following inequality after applying Lemma 4.2:

$$D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) \geq -\log_2(\varsigma(\varepsilon,k)). \tag{4.6.34}$$

Since (4.6.34) holds for all $\omega_{AEA'E'}$ in the set $\mathcal{F}(\sigma_{ABA'B'})$, we conclude that the smooth-min unextendible entanglement of the state $\sigma_{ABA'B'}$ is bounded from below by the following quantity:

$$E^{u,\varepsilon}_{\min}(\sigma_{ABA'B'}) = \frac{1}{2}\inf_{\omega\in\mathcal{F}(\sigma)} D^{\varepsilon}_{\min}(\sigma_{ABA'B'}\|\omega_{AEA'E'}) \tag{4.6.35}$$

$$\geq -\frac{1}{2}\log_2(\varsigma(\varepsilon,k)), \tag{4.6.36}$$

thus completing the proof. □

Remark 4.3 *For a fixed* $\varepsilon \in \left[0, \frac{3}{4}\right]$, *if* $E_{\min}^{u,\varepsilon}(\sigma_{ABA'B'}) < -\frac{1}{2}\log_2(\varsigma(\varepsilon, 2))$, *then there does not exist a private state* $\gamma_{ABA'B'}^k$ *such that* $F\left(\sigma_{ABA'B'}, \gamma_{ABA'B'}^k\right) \geq 1 - \varepsilon$.

The unextendible entanglement of a state does not increase under the action of a one-way LOCC channel. Therefore, for any one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ that is used to distill an ε-approximate private state $\sigma_{A'B'A''B''}$ from a bipartite resource state ρ_{AB}, the unextendible entanglement of ρ_{AB} must be larger than the unextendible entanglement of $\sigma_{A'B'A''B''}$, which in turn is bounded from below by $-\frac{1}{2}\log_2(\varsigma(\varepsilon, k))$ as stated in Proposition 4.3. That is,

$$E_{\min}^{u,\varepsilon}(\rho_{AB}) \geq E_{\min}^{u,\varepsilon}(\sigma_{A'B'A''B''}) \geq -\frac{1}{2}\log_2(\varsigma(\varepsilon, k)). \tag{4.6.37}$$

Rewriting the above inequality as an upper bound on $\log_2 k$, which is the maximum number of secret bits that can be distilled from ρ_{AB} using a two-extendible channel, yields an upper bound on the one-shot, one-way distillable key of the state ρ_{AB}.

Theorem 4.2 (Unextendibility bound on one-shot distillable key) *Fix* $\varepsilon \in (0, 1)$. *Let* ρ_{AB} *be a quantum state such that the following inequality holds:*

$$\varepsilon < J_{\min}^{\varepsilon}(\rho_{AB}) \leq \frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}, \tag{4.6.38}$$

where $J_{\min}^{\varepsilon}(\rho_{AB})$ *is defined in* (4.5.26). *Then the one-shot, one-way distillable key of a bipartite state* ρ_{AB} *is bounded from above by the following quantity:*

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J_{\min}^{\varepsilon}(\rho_{AB})\left(1 - J_{\min}^{\varepsilon}(\rho_{AB})\right)} + \sqrt{\varepsilon(1-\varepsilon)}}{J_{\min}^{\varepsilon}(\rho_{AB}) - \varepsilon}\right)^2 + 1\right]. \tag{4.6.39}$$

If $J_{\min}^{\varepsilon}(\rho_{AB}) > \frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}$, *then the one-shot, one-way distillable key of the state is equal to zero.*

Proof: See Appendix 4.D. □

When $\varepsilon = 0$, the upper bound from Theorem 4.2 simplifies to the min-unextendible entanglement bound on the exact one-way distillable key of a state obtained in [WWW24, Theorem 24].

The one-shot, one-way distillable key of a state does not increase under the action of one-way LOCC channels, and we expect the same from any reasonable bound on the quantity. Similarly, we expect that the bound does not increase with decreasing ε because demanding a higher fidelity between the distilled state and the target state should only lead to a lower yield from the distillation process. To examine if the upper bound on the one-shot, one-way distillable key of a state given in Theorem 4.2 satisfies the aforementioned criteria, we invoke Lemma 4.3 stated below.

Lemma 4.3 *For all $J \in (\varepsilon, 1-\varepsilon]$ and $\varepsilon \in [0,1]$, the following function*

$$f(J,\varepsilon) := \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right)^2 + 1\right] \tag{4.6.40}$$

decreases monotonically with J and increases monotonically with ε.

Proof: See Appendix 4.E. □

Recall that the quantity $J^{\varepsilon}_{\min}(\rho_{AB})$ increases under the action of one-way LOCC channels. Therefore, Lemma 4.3 implies that the upper bound on the one-shot, one-way distillable key of a state given in Theorem 4.2 decreases monotonically under the action of one-way LOCC channels, and it increases monotonically with ε.

The smooth-min unextendible entanglement of a state can be written as a semidefinite program (see Appendix 4.H), which allows us to compute the upper bound on the one-shot, one-way distillable key given in Theorem 4.2 using a semidefinite pro-

gram. In Figure 4.3 we demonstrate some numerical results for the smooth-min unextendible entanglement upper bound on the one-shot, one-way distillable key of an isotropic state [HH99], which is parameterized as follows:

$$\zeta_{AB}^{F,d} = F\Phi_{AB}^{d} + (1-F)\frac{I_{AB} - \Phi_{AB}^{d}}{d^2 - 1}, \tag{4.6.41}$$

where F is a parameter in the interval $[0, 1]$ and $d = d_A = d_B$.

In Figure 3c, we compare the upper bounds on $K_D^{\varepsilon,\rightarrow}\left(\zeta_{AB}^{F,d}\right)$ and $K_D^{\varepsilon,\rightarrow}\left(\left(\zeta_{AB}^{F,d}\right)^{\otimes 2}\right)$ for $\varepsilon = 0.01$ obtained using Theorem 2. The time complexity of computing the upper bound on the one-shot, one-way distillable key of n copies of a state using the SDP bound in Theorem 2 is exponential in n. We address this problem later in Section 5.2 by obtaining an efficiently computable upper bound on the n-shot, one-way distillable key of a state.

Comparison with smooth-min relative entropy of entanglement bound

The one-shot distillable key of a state, roughly defined as the number of approximate secret bits that can be distilled from the state using an LOCC channel, is known to be bounded from above by the smooth-min relative entropy of entanglement of the state [WTB17], which is defined as follows:

$$E_R^{\varepsilon}(\rho_{AB}) \coloneqq \inf_{\sigma_{AB} \in \mathrm{SEP}(A:B)} D_{\min}^{\varepsilon}(\rho_{AB} \| \sigma_{AB}), \tag{4.6.42}$$

where $\mathrm{SEP}(A:B)$ denotes the set of all separable states in $\mathcal{S}(AB)$. Naturally, the smooth-min relative entropy of entanglement is also an upper bound on the one-shot, one-way distillable key of a state since every one-way LOCC channel lies in the set of LOCC channels. As such,

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leq E_R^{\varepsilon}(\rho_{AB}). \tag{4.6.43}$$

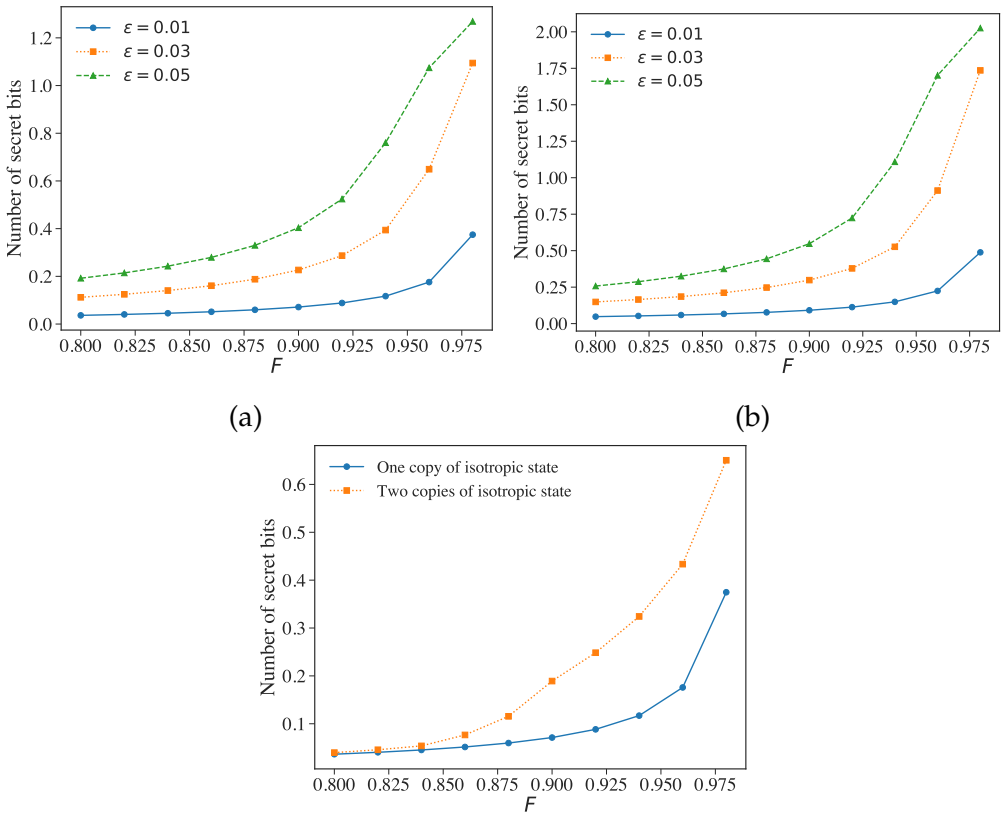


Figure 4.3: Upper bounds on the one-shot one-way distillable key of an isotropic state, described in (4.6.41), using (4.6.39). (a) Upper bounds for a two-dimensional isotropic state for different values of ε plotted against the parameter F. (b) Upper bounds for a three-dimensional isotropic state for different values of ε plotted against the parameter F. (c) For $\varepsilon = 0.01$, comparison between the upper bounds obtained for a single copy of a two-dimensional isotropic state with the upper bound obtained for two copies of a two-dimensional isotropic state, plotted against the parameter F.

In general, it is not practical to compute the smooth-min relative entropy of entanglement as it involves an optimization over the set of separable states, which is known to be an NP-hard problem [Gur03, Gha10]. However, one can evaluate this quantity for some highly symmetric states, such as the isotropic state defined in (4.6.41). It is known from [HH99] that a d-dimensional isotropic state $\zeta_{AB}^{F,d}$ is separable if and only if $F \leq \frac{1}{d}$. As

such,

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F,d}\right) = 0 \qquad \forall F \in \left[0, \frac{1}{d}\right]. \tag{4.6.44}$$

In Proposition 4.4, we state the smooth-min relative entropy of entanglement of a d-dimensional entangled isotropic state.

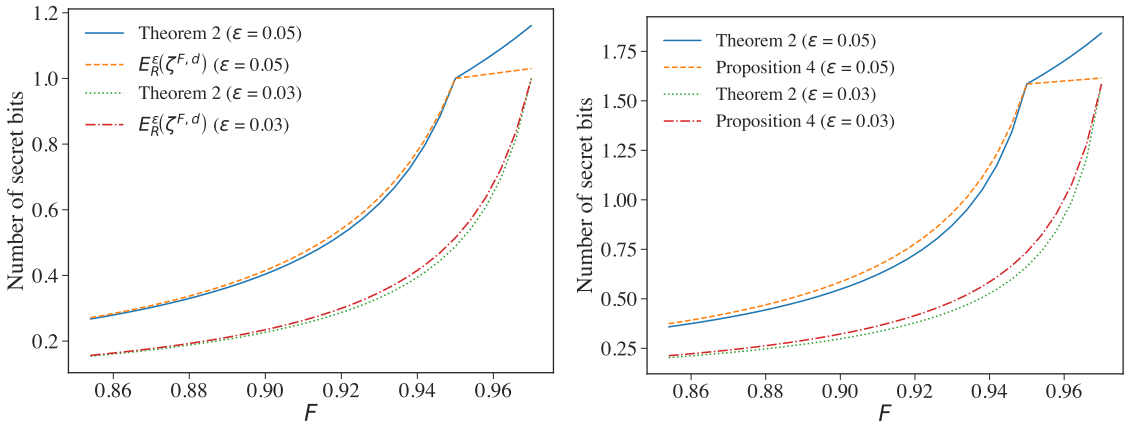
Proposition 4.4 *The smooth-min relative entropy of entanglement of an isotropic state $\zeta_{AB}^{F,d}$, with $F > \frac{1}{d}$, is equal to the following:*

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F}\right) = \begin{cases} -\log_2\left(1 - \frac{\varepsilon}{1-F}\left(1 - \frac{1}{d}\right)\right) & \text{if} \quad 1 - \varepsilon \geq F \\ \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) & \text{otherwise} \end{cases}. \tag{4.6.45}$$

Proof: See Appendix 4.I. □

The analytical expression for the smooth-min relative entropy of entanglement of isotropic states allows us to compare our bound from Theorem 4.2 with the bound from [WTB17] for isotropic states. We must note that this is not a direct comparison of results since the smooth-min relative entropy of entanglement is an upper bound on the one-shot distillable key of a state, which is expected to be strictly larger than the one-shot, one-way distillable key of the state in general.

In Figure 4.4, we plot the upper bound on the one-shot, one-way distillable key of an isotropic state given in Theorem 4.2 and the smooth-min relative entropy of entanglement of the isotropic state against the parameter F for different values of ε and dimension d. For a range of parameters F, the bound in Theorem 4.2 performs better than the smooth-min relative entropy of entanglement bound, demonstrating the advantage of the bound in Theorem 4.2 over previously known bounds numerically. Moreover, the smooth-min



(a) Two-dimensional isotropic state (b) Three-dimensional isotropic state

Figure 4.4: Comparison between the upper bounds on the one-shot, one-way distillable key of two-dimensional and three-dimensional isotropic states, parameterized as given in (4.6.41), obtained using Theorem 4.2 and Proposition 4.4.

relative entropy of entanglement is not efficiently computable for arbitrary states while the bound in Theorem 4.2 is efficiently computable for arbitrary quantum states.

Simplified upper bounds

The upper bound on the one-shot, one-way distillable key of a bipartite state obtained in Theorem 4.2 is difficult to analyze, due to its complicated form. Weaker but simpler bounds can be obtained by using the smooth-min unextendible entanglement of states.

Relaxation 1: We first consider a relaxation of the upper bound in (4.6.39) by finding an algebraic inequality for the function $\varsigma(\varepsilon, k)$ defined in (4.6.5):

$$\varsigma(\varepsilon, k) = \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2} \tag{4.6.46}$$

$$\leq \frac{1}{k^2} + \varepsilon\left(1 - \frac{2}{k^2}\right) + 2\frac{\sqrt{k^2\varepsilon}}{k^2} \tag{4.6.47}$$

$$\leq \frac{1}{k^2} + \varepsilon + 2\frac{\sqrt{\varepsilon}}{k} \tag{4.6.48}$$

$$= \left(\frac{1}{k} + \sqrt{\varepsilon}\right)^2, \tag{4.6.49}$$

where the first inequality follows from the fact that $(k^2 - 1)(1 - \varepsilon) \leq k^2$ for all $k \in \mathbb{N}$ and $\varepsilon \in [0, 1]$ and the second inequality follows from the fact that $1 - \frac{2}{k^2} < 1$ for all $k \in \mathbb{N}$.

We can now use this upper bound on $\varsigma(\varepsilon, k)$ along with the statement of Proposition 4.3 to obtain a lower bound on the smooth-min unextendible entanglement of a state $\sigma_{ABA'B'}$ such that $F(\sigma_{ABA'B'}, \gamma^k_{ABA'B'}) \geq 1 - \varepsilon$ for some private state $\gamma^k_{ABA'B'}$. In particular,

$$E^{u,\varepsilon}_{\min}(\sigma_{ABA'B'}) \geq -\frac{1}{2}\log_2\left(\frac{1}{k} + \sqrt{\varepsilon}\right)^2 = -\log_2\left(\frac{1}{k} + \sqrt{\varepsilon}\right). \tag{4.6.50}$$

This leads to the following simplified but weaker upper bound on the one-shot, one-way distillable key of a bipartite state:

Corollary 4.1 *Fix $\varepsilon \in (0, 1)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2} \geq J^{\varepsilon}_{\min}(\rho_{AB}) > \varepsilon, \tag{4.6.51}$$

where $J^{\varepsilon}_{\min}$ is defined in (4.5.26). Then the one-shot, one-way distillable key of a bipartite state ρ_{AB} is bounded from above as follows:

$$K^{\varepsilon,\rightarrow}_{D}(\rho_{AB}) \leq -\log_2\left(\sqrt{J^{\varepsilon}_{\min}(\rho_{AB})} - \sqrt{\varepsilon}\right). \tag{4.6.52}$$

Proof: The proof is similar to the proof of Theorem 4.2 and follows directly from (4.6.50). □

Relaxation 2: Another way to obtain a simpler bound on the one-shot, one-way distillable key of a state is by considering the trace norm. First we will find a simpler but weaker statement of Lemma 4.2. Consider a state $\sigma_{ABA'B'}$ such that $F(\gamma^k_{ABA'B'}, \sigma_{ABA'B'}) \geq 1 - \varepsilon$

for some private state $\gamma^k_{ABA'B'}$. Combining (4.6.19) and (4.6.25), we find that the following inequality holds for any state $\omega_{AEA'E'} \in \mathcal{F}(\sigma_{ABA'B'})$:

$$1 - \varepsilon \leq F\left(\pi_{AE}, q\ \Phi^k_{AE} + (1-q)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right), \tag{4.6.53}$$

where $q = \mathrm{Tr}\left[\Pi^{\gamma}_{AEA'E'}\omega_{AEA'E'}\right]$ as stated in (4.6.21). Using the Fuchs-van de Graaf inequality [FvdG99] (specifically, $F(\rho,\sigma) \leq 1 - \frac{1}{4}\left\|\rho - \sigma\right\|_1^2$), we arrive at the following inequality:

$$1 - \varepsilon \leq F\left(\pi_{AE}, q\ \Phi^k_{AE} + (1-q)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right) \leq 1 - \frac{1}{4}\left\|\pi_{AE} - q\ \Phi^k_{AE} + (1-q)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right\|_1^2. \tag{4.6.54}$$

The above inequality can be rewritten as follows:

$$\begin{aligned}
\sqrt{\varepsilon} &\geq \frac{1}{2}\left\|\pi_{AE} - q\ \Phi^k_{AE} + (1-q)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right\|_1 && (4.6.55)\\
&= \frac{1}{2}\left\|\frac{1}{k^2}\Phi^k_{AE} - \left(1 - \frac{1}{k^2}\right)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1} - q\ \Phi^k_{AE} + (1-q)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right\|_1 && (4.6.56)\\
&= \frac{1}{2}\left\|\left(\frac{1}{k^2} - q\right)\Phi^k_{AE} + \left(\frac{1}{k^2} - q\right)\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right\|_1 && (4.6.57)\\
&= \left|\frac{1}{k^2} - q\right|\left\|\frac{1}{2}\Phi^k_{AE} + \frac{1}{2}\frac{I_{AE} - \Phi^k_{AE}}{k^2 - 1}\right\|_1 && (4.6.58)\\
&= \left|\frac{1}{k^2} - q\right|, && (4.6.59)
\end{aligned}$$

where the first equality follows by writing the maximally mixed state as an isotropic state and the last equality follows by realizing that $\frac{1}{2}\Phi^k_{AE} + \frac{1}{2}\frac{I_{AE} - \Phi^k_{AE}}{k^2-1}$ is a quantum state for which the trace norm is equal to 1. The inequality in (4.6.59) is satisfied if and only if q lies in the following range:

$$\frac{1}{k^2} - \sqrt{\varepsilon} \leq q \leq \frac{1}{k^2} + \sqrt{\varepsilon}. \tag{4.6.60}$$

Since $q = \mathrm{Tr}\left[\Pi^{\gamma}_{ABA'B'}\omega_{ABA'B'}\right]$, we have the following inequality:

$$\mathrm{Tr}\left[\Pi^{\gamma}_{ABA'B'}\omega_{ABA'B'}\right] \leq \frac{1}{k^2} + \sqrt{\varepsilon}. \tag{4.6.61}$$

Using the inequality in (4.6.61) and the arguments used in the proof of Proposition 4.3, we can bound the smooth-min unextendible entanglement of the state $\sigma_{ABA'B'}$ as follows:

$$E_{\min}^{u,\varepsilon}(\sigma_{ABA'B'}) \geq -\frac{1}{2}\log_2\left(\frac{1}{k^2} + \sqrt{\varepsilon}\right). \tag{4.6.62}$$

A relaxed upper bound on the one-shot, one-way distillable key of a bipartite state can be found by using the inequality mentioned above, which we state as Corollary 4.2.

Corollary 4.2 *Fix $\varepsilon \in (0,1)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2} \geq J_{\min}^{\varepsilon}(\rho_{AB}) > \sqrt{\varepsilon}, \tag{4.6.63}$$

where $J_{\min}^{\varepsilon}$ is defined in (4.5.26). Then the one-shot, one-way distillable key of a bipartite state ρ_{AB} is bounded from above by the following quantity:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leq -\frac{1}{2}\log_2\left(J_{\min}^{\varepsilon}(\rho_{AB}) - \sqrt{\varepsilon}\right). \tag{4.6.64}$$

Proof: The proof is similar to the proof of Theorem 4.2 and follows directly from (4.6.62). □

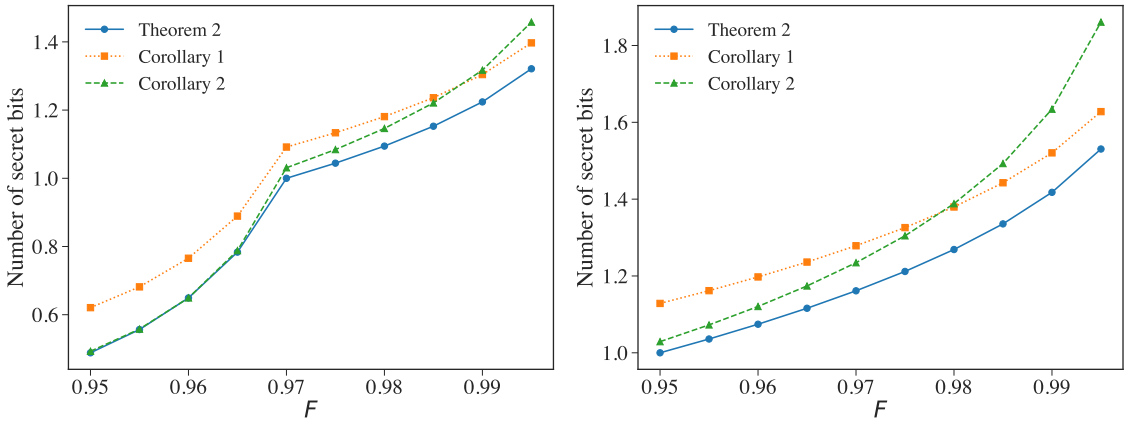
Remark 4.4 *The upper bound on the one-shot, one-way distillable key given in Corollary 4.1 is tighter than the upper bound given in Corollary 4.2 for highly entangled states, but the order is reversed for weakly entangled states. To be precise,*

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leq -\log_2\left(\sqrt{J_{\min}^{\varepsilon}} - \sqrt{\varepsilon}\right) \leq -\frac{1}{2}\log_2\left(J_{\min}^{\varepsilon} - \sqrt{\varepsilon}\right), \tag{4.6.65}$$

for all $J_{\min}^{\varepsilon} \in \left[\sqrt{\varepsilon}, \frac{1}{4}\left(1+\varepsilon+2\sqrt{\varepsilon}\right)\right]$, and

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leq -\frac{1}{2}\log_2\left(J_{\min}^{\varepsilon} - \sqrt{\varepsilon}\right) \leq -\log_2\left(\sqrt{J_{\min}^{\varepsilon}} - \sqrt{\varepsilon}\right), \tag{4.6.66}$$

for all $J_{\min}^{\varepsilon} \in \left[\frac{1}{4}\left(1+\varepsilon+2\sqrt{\varepsilon}\right), 1-\varepsilon\right]$.



(a) $\varepsilon = 0.03$ (b) $\varepsilon = 0.05$

Figure 4.5: Comparison between the upper bounds on the one-shot, one-way distillable key of two-dimensional isotropic states, parameterized as given in (4.6.41), obtained using Theorem 4.2, Corollary 4.1, and Corollary 4.2.

The bounds obtained in Corollary 4.1 and Corollary 4.2 can be computed using a semidefinite program. In Figure 4.5 we plot the three different upper bounds on the one-shot, one-way distillable key of isotropic states, defined in (4.6.41), obtained from Theorem 4.2, Corollary 4.1, and Corollary 4.2. Notice that the bound from Corollary 4.1 is tighter than the bound from Corollary 4.2 when the resource state is highly entangled.

4.6.2 One-way secret-key distillation from i.i.d. copies of a state

Resource distillation from independent and identically distributed (i.i.d.) copies of a state is often considered a physically relevant setting. As such, the rate at which secret bits can be distilled from n i.i.d. copies of a state, which is equal to $\frac{1}{n} K_D^{\varepsilon,\rightarrow}\left(\rho_{AB}^{\otimes n}\right)$, is an important quantity from both information-theoretic and practical perspectives.

In principle, the bounds obtained for the one-shot, one-way distillable key of a state can be used to obtain an upper bound on the one-way distillable key rate from n copies

of ρ_{AB}, with ε error tolerance, by simply calculating the upper bounds for the state $\rho_{AB}^{\otimes n}$. However, the complexity of computing these bounds scales exponentially with the number of copies n, rendering the computation of these bounds intractable for large enough n. The smooth-min relative entropy is not subadditive; that is, there exists a choice of states ρ^1, ρ^2, σ^2, and σ^2, such that the following inequality does not hold:

$$D_{\min}^{\varepsilon}\left(\rho^2 \otimes \rho^2 \middle\| \sigma^1 \otimes \sigma^2\right) \leq D_{\min}^{\varepsilon}\left(\rho^1 \middle\| \sigma^1\right) + D_{\min}^{\varepsilon}\left(\rho^2 \middle\| \sigma^2\right), \tag{4.6.67}$$

which makes it difficult to obtain a single-letter bound on the one-way distillable key rate with our approach. We turn to the α-sandwiched unextendible entanglement of bipartite states to address this problem.

The smooth-min relative entropy is related to the α-sandwiched Rényi relative entropy by the following inequality [CMW16, Lemma 5]:

$$D_{\min}^{\varepsilon}(\rho\|\sigma) \leq \widetilde{D}_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha - 1} \log_2\left(\frac{1}{1-\varepsilon}\right) \tag{4.6.68}$$

for all $\varepsilon \in [0, 1)$ and $\alpha \in (1, \infty)$. By taking an infimum over all states $\sigma \in \mathcal{F}(\rho)$, we arrive at an inequality relating the smooth-min unextendible entanglement of a state and the α-sandwiched unextendible entanglement of the state, which we state in Proposition 4.5 below.

Proposition 4.5 *Let $\alpha \in (1, \infty)$ and $\varepsilon \in [0, 1)$. Then the following inequality holds between the smooth-min unextendible entanglement of a state and the α-sandwiched unextendible entanglement of the state:*

$$E_{\min}^{u,\varepsilon}(\rho) \leq \widetilde{E}_{\alpha}^{u}(\rho) + \frac{1}{2} \cdot \frac{\alpha}{\alpha - 1} \log_2\left(\frac{1}{1-\varepsilon}\right). \tag{4.6.69}$$

As a counterpart of $J_{\min}^{\varepsilon}(\rho_{AB})$, we define the following quantity for mathematical simplicity:

$$\widetilde{J}_{\alpha}^{\varepsilon}(\rho_{AB}) := 2^{-2\widetilde{E}_{\alpha}^{u}(\rho_{AB})} (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} \qquad \forall \alpha \in (1, \infty). \tag{4.6.70}$$

It is straightforward to verify from Proposition 4.5 that

$$J^{\varepsilon}_{\min}(\rho_{AB}) \geq \widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB}) \qquad \forall \alpha \in (1,\infty). \tag{4.6.71}$$

One can simply use Theorem 4.2 and Lemma 4.3 to obtain an upper bound on the one-shot, one-way distillable key of a state in terms of the α-sandwiched unextendible entanglement, as follows:

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}) \leq f(J^{\varepsilon}_{\min}(\rho_{AB}),\varepsilon) \leq f\left(\widetilde{J}^{\varepsilon}_{\alpha}(\rho_{AB}),\varepsilon\right) \qquad \forall \alpha \in (1,\infty), \tag{4.6.72}$$

where the function f is defined in Lemma 4.3. The first inequality follows from Theorem 4.2, and the second inequality follows from (4.6.71) and Lemma 4.3.

While the α-sandwiched unextendible entanglement bound is clearly worse than the smooth-min unextendible entanglement bound, it gives a single-letter upper bound on the one-shot, one-way distillable key from n i.i.d. copies of a state ρ_{AB}. The subadditivity of the α-sandwiched unextendible entanglement implies the following for all $\alpha \in (1,\infty)$:

$$\widetilde{J}^{\varepsilon}_{\alpha}(\rho^{\otimes n}_{AB}) = 2^{-2\widetilde{E}^{u}_{\alpha}(\rho^{\otimes n}_{AB})}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}} \geq 2^{-2n\widetilde{E}^{u}_{\alpha}(\rho_{AB})}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}}. \tag{4.6.73}$$

Let us define the following quantity:

$$\widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB}) := 2^{-2n\widetilde{E}^{u}_{\alpha}(\rho_{AB})}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}}. \tag{4.6.74}$$

Then the fact that $\widetilde{J}^{\varepsilon}_{\alpha}\left(\rho^{\otimes n}_{AB}\right) \geq \widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB})$, combined with Lemma 4.3 and (4.6.72), leads to a single-letter upper bound on the one-shot, one-way distillable key of n i.i.d. copies of a state, which we state formally in Corollary 4.3.

Corollary 4.3 *Fix $\varepsilon \in (0,1)$ and $\alpha \in (1,\infty)$. Let ρ_{AB} be a quantum state such that the following inequality holds:*

$$\varepsilon < \widetilde{J}^{\varepsilon,n}_{\alpha}(\rho_{AB}) \leq \frac{1}{4} + \frac{\varepsilon}{2} + \frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}, \tag{4.6.75}$$

where $\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB})$ *is defined in* (4.6.74). *Then the n-shot, one-way distillable key of a state* ρ_{AB} *is bounded from above by the following quantity:*

$$K_D^{\varepsilon,\rightarrow}(\rho_{AB}^{\otimes n}) \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB})\left(1-\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB})\right)}+\sqrt{\varepsilon(1-\varepsilon)}}{\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB})-\varepsilon}\right)^2+1\right], \tag{4.6.76}$$

If $\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) > \frac{1}{4}+\frac{\varepsilon}{2}+\frac{\sqrt{3\varepsilon(1-\varepsilon)}}{2}$, *then the n-shot, one-way distillable key of the state is equal to zero.*

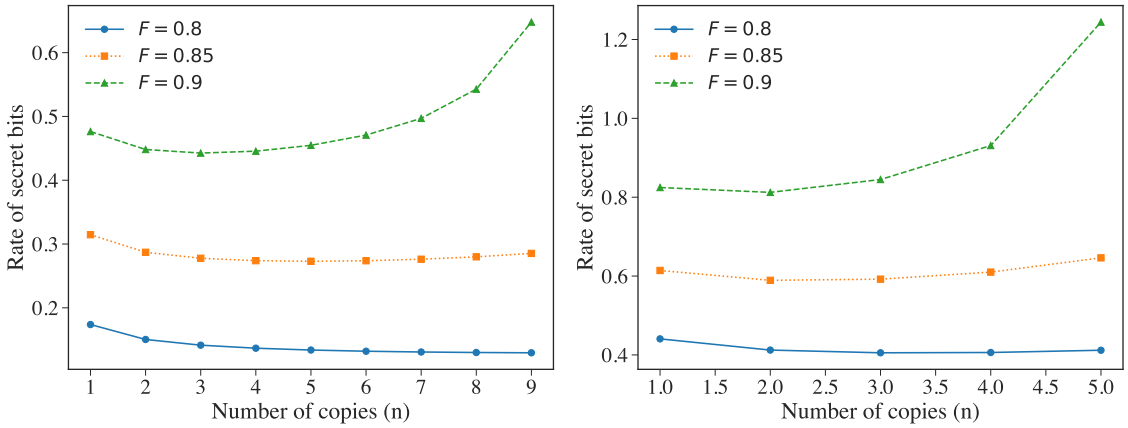
A special case of the bound stated above arises when $\alpha \to \infty$. Let us define the following quantity:

$$\begin{aligned} J_{\max}^{\varepsilon}(\rho_{AB}) &:= \lim_{\alpha\to\infty} \widetilde{J}_\alpha^{\varepsilon}(\rho_{AB}) && (4.6.77)\\ &= \left(\lim_{\alpha\to\infty} 2^{-2\widetilde{E}_\alpha^{u}(\rho_{AB})}\right)\left(\lim_{\alpha\to\infty}(1-\varepsilon)^{\frac{\alpha}{\alpha-1}}\right) && (4.6.78)\\ &= 2^{-2E_{\max}^{u}(\rho_{AB})}(1-\varepsilon), && (4.6.79) \end{aligned}$$

where the second equality follows from the definition of $\widetilde{J}_\alpha^{\varepsilon}(\rho_{AB})$ and the last equality follows from (4.5.41). The max-unextendible entanglement of a state can be computed using an SDP, which implies that $J_{\max}^{\varepsilon}(\rho_{AB})$ can be computed using an SDP. Thus, setting $\alpha \to \infty$ in Corollary 4.3 leads to a single-letter, computable bound on the *n*-shot, one-way distillable key of a state.

In Figure 4.6 we plot the upper bounds on the *n*-shot, one-way distillable key of isotropic states calculated using Corollary 4.3 with $\alpha \to \infty$. In Figure 4.6a we plot the upper bounds for two-dimensional isotropic states, and in Figure 4.6b we plot the upper bounds for three-dimensional isotropic states, with $\varepsilon = 0.01$ in all the cases.

Remark 4.5 *The techniques used to arrive at Corollaries 4.1 and 4.2 can be used to find simpler bounds on the one-shot, one-way distillable key of n i.i.d. copies of a state* ρ_{AB} *by using the* α*-sandwiched unextendible entanglement. As such, for all* $\varepsilon \in (0,1)$, $\alpha \in (1,\infty)$, $n \in \mathbb{N}$, *and a state*



(a) Two-dimensional isotropic state (b) Three-dimensional isotropic state

Figure 4.6: Upper bounds on the n-shot, one-way distillable-key rate of isotropic states using Corollary 4.3 and setting $\alpha \to \infty$. The upper bounds are plotted for different values of the parameter F of the isotropic state, with respect to the parameterization given in (4.6.41), against the number of copies of the isotropic state, and ε is set equal to 0.01.

ρ_{AB}, if $\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) > \varepsilon$, then

$$K_D^{\varepsilon,\to}(\rho_{AB}^{\otimes n}) \leq -\log_2\left(\sqrt{\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB})} - \sqrt{\varepsilon}\right), \tag{4.6.80}$$

and if $\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) > \sqrt{\varepsilon}$, then

$$K_D^{\varepsilon,\to}(\rho_{AB}^{\otimes n}) \leq -\frac{1}{2}\log_2\left(\widetilde{J}_\alpha^{\varepsilon,n}(\rho_{AB}) - \sqrt{\varepsilon}\right). \tag{4.6.81}$$

4.6.3 One-way secret-key distillation in the asymptotic setting

Now let us study the asymptotic setting of one-way secret-key distillation by using the framework of unextendibility.

In the asymptotic setting, we are interested in the maximum rate at which an arbitrarily large number of i.i.d. copies of a state ρ_{AB} can be transformed into a state that is arbitrarily close to an ideal secret key. In this setting, a one-way secret-key distillation

protocol is given by a sequence of one-way LOCC channels $\left\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\rightarrow A'B'A''B''}\right\}_{n\in\mathbb{N}}$, a sequence of bipartite private states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$, and a sequence of real numbers $\{\varepsilon_n\}_{n\in\mathbb{N}}$ corresponding to the error in distillation. The joint system A^n refers to n systems, each of which are identical to the system A. The n^{th} element of this sequence acts on n copies of the resource state ρ_{AB} such that the infidelity between the output state and $\gamma^{k_n}_{A'B'A''B''}$ is less than or equal to ε_n. That is,

$$F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{n,\rightarrow}_{A^nB^n\rightarrow A'B'A''B''}(\rho^{\otimes n}_{AB})\right) \geq 1-\varepsilon_n \qquad \forall n\in\mathbb{N}. \tag{4.6.82}$$

To achieve arbitrary precision in distilling secret keys, we demand that $\varepsilon_n \to 0$ as $n \to \infty$. The maximum achievable rate of distilling secret keys is then given by the one-way distillable key of the state, which can be mathematically defined in terms of the one-shot, one-way distillable key as follows [KW24, Chapter 15]:

$$K^{\rightarrow}_D(\rho_{AB}) \coloneqq \inf_{\varepsilon\in(0,1]} \liminf_{n\to\infty} \frac{1}{n} K^{\varepsilon,\rightarrow}_D(\rho^{\otimes n}_{AB}). \tag{4.6.83}$$

The upper bounds on the one-shot, one-way distillable key, obtained in Sections 4.6.1 and 4.6.2, do not provide any new insight into the one-way distillable key of the state. This is because, for most states of interest, there exists an $n\in\mathbb{N}$ such that $J^{\varepsilon}_{\min}\left(\rho^{\otimes n}_{AB}\right) \leq \varepsilon$ for any $\varepsilon\in(0,1]$, rendering the bound useless.

However, consider a further restricted setting where the sequence $\{\varepsilon_n\}_{n\in\mathbb{N}}$ is required to decrease exponentially fast. The maximum rate of key distillation from an arbitrarily large number of copies of a resource state, for a fixed error exponent a, which we call the a-exponential one-way distillable key of a state, can be mathematically defined in the following manner.

Definition 4.6 *Fix $a > 0$. We define the a-exponential one-way distillable key of a state ρ_{AB} as*

follows:

$$K^{\rightarrow}_{D,a}(\rho_{AB}) := \sup_{\substack{\{k_n\}_{n\in\mathbb{N}},\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\right\}_{n\in\mathbb{N}}}} \liminf_{n\to\infty} \left\{ \frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{\rightarrow}(\rho^{\otimes n}_{AB})\right) \geq 1 - 2^{-an} \right\}, \tag{4.6.84}$$

where the supremum is over all sequences of bipartite states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ *and all sequences of one-way LOCC channels* $\left\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\right\}_{n\in\mathbb{N}}$*. The bipartite state* $\gamma^{k_n}_{A'B'A''B''}$ *holds* $\log_2 k_n$ *secret bits.*

We define the converse of a-exponential one-way distillable key of ρ_{AB} *as follows:*

$$\widetilde{K}^{\rightarrow}_{D,a}(\rho_{AB}) := \sup_{\substack{\{k_n\}_{n\in\mathbb{N}},\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\right\}_{n\in\mathbb{N}}}} \limsup_{n\to\infty} \left\{ \frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{\rightarrow}(\rho^{\otimes n}_{AB})\right) \geq 1 - 2^{-an} \right\}. \tag{4.6.85}$$

Theorem 4.3 *Consider an arbitrary bipartite state* ρ_{AB}*. Let* $d := \min\{\dim(A), \dim(B)\}$ *with* $\dim(A)$ *and* $\dim(B)$ *being the dimensions of systems A and B, respectively. Fix* $a \in (2\log_2 d, \infty)$*. Then the following bound holds:*

$$\widetilde{K}^{\rightarrow}_{D,a}(\rho_{AB}) \leq E^u(\rho_{AB}), \tag{4.6.86}$$

where $E^u(\rho_{AB})$ *is the relative-entropy-induced unextendible entanglement of the state* ρ_{AB} *(i.e., defined as in* (4.5.15) *with* $\boldsymbol{D}$ *replaced by the quantum relative entropy D).*

Proof: Let ρ_{AB} be an arbitrary bipartite state from which we wish to distill secret keys, and let $\dim(A)$ and $\dim(B)$ be the dimensions of systems A and B, respectively. Let $\left\{\mathcal{L}^{n,\rightarrow}_{A^nB^n\to A'B'A''B''}\right\}_{n\in\mathbb{N}}$ be a sequence of one-way LOCC channels, and let $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ be a sequence of bipartite private states such that the following condition holds for all $a > 2\log_2 d$ and $n \in \mathbb{N}$:

$$F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{n,\rightarrow}(\rho^{\otimes n}_{AB})\right) \geq 1 - 2^{-an}, \tag{4.6.87}$$

where $d := \min\{\dim(A), \dim(B)\}$.

Let us define $\varepsilon_n := 2^{-an}$ for convenience. Let us also define $J^{\varepsilon_n,n}(\rho_{AB}) := 2^{-E_{\min}^{u,\varepsilon_n}(\rho_{AB}^{\otimes n})}$. From Proposition 4.2 we know that $J^{\varepsilon,n}$ is bounded from below as follows:

$$J^{\varepsilon_n,n}(\rho) \geq \frac{1-\varepsilon_n}{d^{2n}}. \tag{4.6.88}$$

Corollary 4.1 implies that the following inequality holds for all one-way LOCC channels $\mathcal{L}^{n,\rightarrow}_{A^nB^n\rightarrow A'B'A''B''}$ and all private states $\gamma^{k_n}_{A'B'A''B''}$:

$$\begin{aligned}
\log_2 k_n &\leq -\log_2\left(\sqrt{J^{\varepsilon_n,n}(\rho)} - \sqrt{\varepsilon_n}\right) && (4.6.89)\\
&= -\log_2\left(\sqrt{J^{\varepsilon_n,n}(\rho)}\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right)\right) && (4.6.90)\\
&= -\frac{1}{2}\log_2(J^{\varepsilon_n,n}(\rho)) - \log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right). && (4.6.91)
\end{aligned}$$

Dividing both sides by n and taking the limit superior as $n \to \infty$ leads to the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leq \limsup_{n\to\infty} \left\{-\frac{1}{2n}\log_2 J^{\varepsilon_n,n}(\rho) - \frac{1}{n}\log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right)\right\} \tag{4.6.92}$$

Using the lower bound on $J^{\varepsilon_n,n}(\rho)$ from (4.6.88), we arrive at the following inequality:

$$\begin{aligned}
\frac{\varepsilon_n}{J^{\varepsilon,n}} &\leq \varepsilon_n \cdot \frac{d^{2n}}{1-\varepsilon_n} && (4.6.93)\\
&\leq \frac{2^{-an}d^{2n}}{1-2^{-an}} && (4.6.94)\\
&= \frac{d^{2n}}{2^{an}-1} && (4.6.95)\\
&= \frac{2^{2n\log_2 d}}{2^{an}-1} && (4.6.96)\\
&= \frac{2^{-n(a-2\log_2 d)}}{1-2^{-an}}, && (4.6.97)
\end{aligned}$$

where the second inequality follows from the fact that the function $\varepsilon_n/(1-\varepsilon_n)$ increases monotonically with $\varepsilon_n \in [0,1)$ and the fact that $\varepsilon_n \leq 2^{-an}$. Thus, for sufficiently large n, since $a > 2\log_2 d$ by assumption, it follows that $\frac{2^{-n(a-2\log_2 d)}}{1-2^{-an}} \leq 1$ and thus that $\frac{\varepsilon_n}{J^{\varepsilon,n}} \leq 1$.

Then we find that

$$\limsup_{n\to\infty} -\log_2\left(1-\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right) = -\log_2\left(1-\limsup_{n\to\infty}\sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n,n}(\rho)}}\right) \tag{4.6.98}$$

$$\leq -\log_2\left(1-\limsup_{n\to\infty}\sqrt{\frac{2^{-n(a-2\log_2 d)}}{1-2^{-an}}}\right) \tag{4.6.99}$$

$$= -\log_2(1-0) = 0. \tag{4.6.100}$$

Now let us go back to (4.6.92). Substituting (4.6.100) in (4.6.92) leads to the following inequality:

$$\limsup_{n\to\infty}\frac{\log_2 k_n}{n} \leq \limsup_{n\to\infty} -\frac{1}{2n}\log_2 J^{\varepsilon_n,n}(\rho) \tag{4.6.101}$$

$$= \limsup_{n\to\infty}\frac{1}{n}E_{\min}^{u,\varepsilon_n}(\rho_{AB}^{\otimes n}) \tag{4.6.102}$$

$$= \limsup_{n\to\infty}\frac{1}{2n}\inf_{\sigma_{A^nB^n}\in\mathcal{F}(\rho_{AB}^{\otimes n})} D_{\min}^{\varepsilon_n}(\rho_{AB}^{\otimes n}\|\sigma_{A^nB^n}) \tag{4.6.103}$$

where we have used the definition of $J^{\varepsilon_n,n}(\rho)$ to arrive at the first equality and the definition of $E_{\min}^{u,\varepsilon}$ to arrive at the second equality. Note that if $\sigma_{AB}\in\mathcal{F}(\rho_{AB})$ then $\sigma_{AB}^{\otimes n}\in\mathcal{F}\left(\rho_{AB}^{\otimes n}\right)$. Therefore,

$$\inf_{\sigma_{A^nB^n}\in\mathcal{F}(\rho_{AB}^{\otimes n})} D_{\min}^{\varepsilon_n}(\rho_{AB}^{\otimes n}\|\sigma_{A^nB^n}) \leq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} D_{\min}^{\varepsilon_n}(\rho_{AB}^{\otimes n}\|\sigma_{AB}^{\otimes n})\,. \tag{4.6.104}$$

Substituting the above inequality in (4.6.103), we arrive at the following inequality:

$$\limsup_{n\to\infty}\frac{\log_2 k_n}{n} \leq \limsup_{n\to\infty}\frac{1}{2n}\inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} D_{\min}^{\varepsilon_n}(\rho_{AB}^{\otimes n}\|\sigma_{AB}^{\otimes n}) \tag{4.6.105}$$

$$\leq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})}\limsup_{n\to\infty}\frac{1}{2n}D_{\min}^{\varepsilon_n}(\rho_{AB}^{\otimes n}\|\sigma_{AB}^{\otimes n})\,, \tag{4.6.106}$$

where the second inequality from an asymptotic version of the max-min inequality.

Note that $D_{\min}^{\varepsilon}(\rho\|\sigma)$ increases monotonically with increasing ε. Since $\varepsilon_n \leq 2^{-an}$, for every $\varepsilon^*\in(0,1)$, there exists an $N\in\mathbb{N}$ such that $\varepsilon_n\leq\varepsilon^*$ for all $n\geq N$. Consequently,

$$\frac{1}{n}D_{\min}^{\varepsilon_n}(\rho_{AB}^{\otimes n}\|\sigma_{AB}^{\otimes n}) \leq \frac{1}{n}D_{\min}^{\varepsilon^*}(\rho_{AB}^{\otimes n}\|\sigma_{AB}^{\otimes n}) \qquad \forall n\geq N. \tag{4.6.107}$$

Substituting the above inequality in (4.6.106), we arrive at the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2} \limsup_{n\to\infty} \frac{1}{n} D^{\varepsilon^*}_{\min}(\rho^{\otimes n}_{AB} \| \sigma^{\otimes n}_{AB}) \,. \tag{4.6.108}$$

For all $\varepsilon \in (0,1)$, the following inequality holds [NO00]:

$$\limsup_{n\to\infty} \frac{1}{n} D^{\varepsilon}_{\min}(\rho^{\otimes n} \| \sigma^{\otimes n}) \leq D(\rho\|\sigma) \,, \tag{4.6.109}$$

where $D(\cdot\|\cdot)$ is the Umegaki relative entropy [Ume62]. Therefore, we conclude the following:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leq \inf_{\sigma_{AB}\in\mathcal{F}(\rho_{AB})} \frac{1}{2} D(\rho_{AB}\|\sigma_{AB}) = E^u(\rho_{AB}) \,. \tag{4.6.110}$$

Since the above inequality holds for all sequences of one-way LOCC channels $\left\{\mathcal{L}^{n,\to}_{A^nB^n\to A'B'A''B''}\right\}_{n\in\mathbb{N}}$ and all sequences of private states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ such that $F\left(\gamma^{k_n}_{A'B'A''B''}, \mathcal{L}^{\to}(\rho^{\otimes n}_{AB})\right) \geq 1 - 2^{-an}$ for all $a > 2\log_2 d$, we conclude the statement of theorem. □

Remark 4.6 *The relative-entropy-induced unextendible entanglement of a state can be computed using a semidefinite program. See [KS24] for a semidefinite representation of the relative entropy between two states that can be used directly to estimate the relative-entropy-induced unextendible entanglement of a state to arbitrary precision.*

4.7 Forward-assisted private communication from channels

In this section we extend the results obtained in Section 4.6 to understand the limitations of private communication over channels. We begin with a brief discussion on secret-key distillation from a channel with local operations and forward classical communication in the one-shot setting. In this setting, where forward classical communication can be

performed with no cost, the task of secret-key distillation from a channel is equivalent to the task of private communication from the channel.

4.7.1 One-shot, one-way distillable key of a channel

To distill a secret key from a channel using one-way LOCC, Alice locally prepares a state $\psi_{A'A''\hat{A}}$, and encodes one share of this state using a quantum instrument $\left\{\mathcal{E}^x_{\hat{A}\to A}\right\}_{x\in\mathcal{X}}$. She then sends the system A to Bob through the quantum channel $\mathcal{N}_{A\to B}$ along with the classical label x. Bob then decodes the received state by applying a quantum channel $\mathcal{D}^x_{B\to B'B''}$, which he can choose based on the classical label x that he received from Alice. The state established at the end of the protocol can be mathematically described as follows:

$$\sigma_{A'B'A''B''} \coloneqq \sum_{x\in\mathcal{X}} \left(\mathcal{D}^x_{B\to B'B''} \circ \mathcal{N}_{A\to B} \circ \mathcal{E}^x_{\hat{A}\to A}\right)(\psi_{A'A''\hat{A}}). \tag{4.7.1}$$

For the secret-key distillation task to be successful in distilling $\log_2 k$ secret bits with an error tolerance ε, we require the following inequality to hold:

$$F\left(\sigma_{A'B'A''B''}, \gamma^k_{A'B'A''B''}\right) \geq 1-\varepsilon \tag{4.7.2}$$

for some private state $\gamma^k_{A'B'A''B''}$ holding $\log_2 k$ secret bits. Figure 4.7 depicts a schematic diagram of the task of one-way secret-key distillation from a channel.

The task of secret-key distillation from a quantum channel can be expressed more concisely using the language of superchannels [CDP08, Gou19]. To distill $\log_2 k$ secret bits from a channel $\mathcal{N}_{A\to B}$ with an error tolerance ε and only using one-way LOCC, Alice and Bob apply a one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{A}\to B'B'')}$ on the channel $\mathcal{N}_{A\to B}$ such that the following inequality holds:

$$F\left((\Theta(\mathcal{N}))(\psi_{A'A''\hat{A}}), \gamma^k_{A'B'A''B''}\right) \geq 1-\varepsilon, \tag{4.7.3}$$

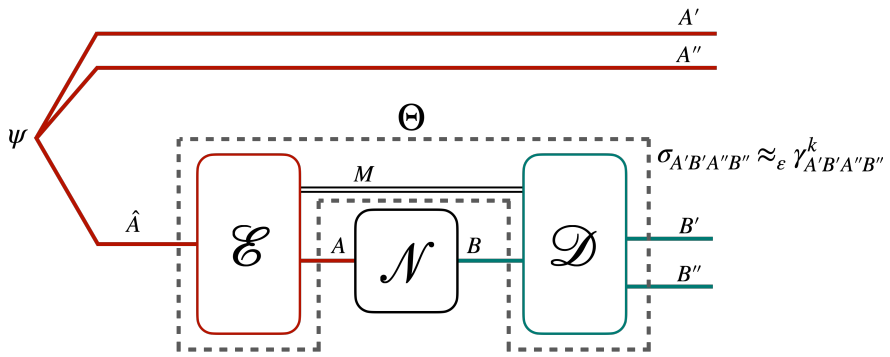


Figure 4.7: Schematic diagram of secret-key distillation from a channel $\mathcal{N}_{A\to B}$ using a one-way LOCC superchannel Θ. The error in the distillation process, denoted by ε, is given by the infidelity between the state $\sigma_{A'B'A''B''}$ established at the end of the protocol and a private state $\gamma^k_{A'B'A''B''}$ that holds $\log_2 k$ secret bits.

for some locally prepared state $\psi_{A'A''\hat{A}}$ and some private state $\gamma^k_{A'B'A''B''}$ holding $\log_2 k$ secret bits. The ability to distill secret keys from a channel in the one-shot setting can then be quantified by the one-shot, one-way distillable key of the channel, which we define below.

Definition 4.7 *The one-shot, one-way distillable key of a channel $\mathcal{N}_{A\to B}$ is defined as follows:*

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) := \sup_{\substack{k\in\mathbb{N},\gamma^k_{A'B'A''B''},\\ \psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A}),\\ \Theta\in 1\text{WL}}} \left\{\log_2 k : F\left((\Theta(\mathcal{N}))(\psi_{A'A''\hat{A}}), \gamma^k_{A'B'A''B''}\right) \geq 1-\varepsilon\right\}, \tag{4.7.4}$$

where the supremum is over every natural number k, every quantum state $\psi_{A'A''\hat{A}}$, every private state $\gamma^k_{A'B'A''B''}$, and every one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{A}\to B'B'')}$.

The one-shot, one-way distillable key of a channel can be written in terms of the one-shot, one-way distillable key of a state as follows:

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) = \sup_{\substack{\psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A}),\\ \Theta\in 1\text{WL}}} K_D^{\varepsilon,\to}\left(\left(\Theta_{(A\to B)\to(\hat{A}\to B'B'')}(\mathcal{N}_{A\to B})\right)(\psi_{A'A''\hat{A}})\right). \tag{4.7.5}$$

Establishing a secret key and using the one-time-pad scheme for private communication is not the only way to transmit private bits over a channel, and there may exist

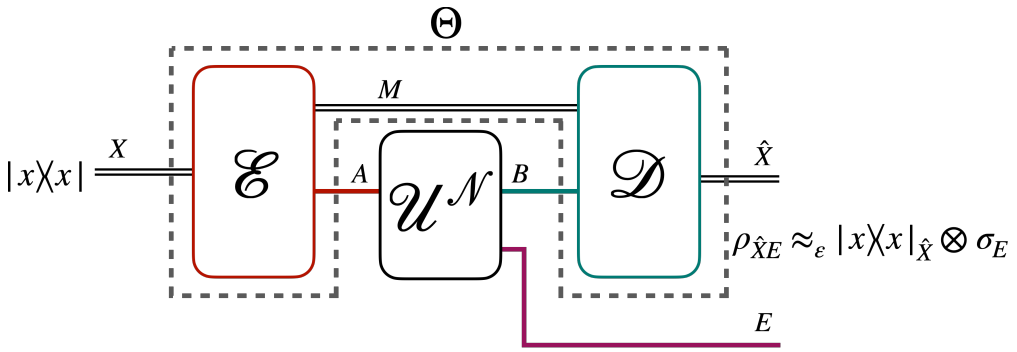


Figure 4.8: Schematic diagram of private communication over a channel $\mathcal{N}_{A\to B}$, with an isometric extension $\mathcal{U}^{\mathcal{N}}_{A\to BE}$, using a one-way LOCC superchannel Θ. The objective of this protocol is to send an arbitrary classical label x from Alice to Bob such that the state of an eavesdropper, who holds the system E, is independent of the state Bob receives. The error in private communication, denoted by ε, is defined in (4.7.6).

alternate protocols to realize private communication over a quantum channel [DLL03]. The notion of one-shot private capacity of channels is used to quantify the ability of a quantum channel to communicate data privately using local operations without making assumptions on the protocol.

Suppose that Alice wants to send private data to Bob by using a channel $\mathcal{N}_{A\to B}$. To do this, Alice and Bob apply a superchannel $\Theta_{(A\to B)\to(X\to\hat{X})}$ on the channel $\mathcal{N}_{A\to B}$, where X and $\hat{X}$ are classical systems. Let $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ be an isometric extension of the channel $\mathcal{N}_{A\to B}$, where the eavesdropper has access to the system E. The error in private communication through this protocol is defined as follows:

$$p_{\text{err}}(\Theta,\mathcal{N}) := \inf_{\sigma_E}\max_{x\in\mathcal{X}}\left(1-F\left(|x\rangle\langle x|_{\hat{X}}\otimes\sigma_E,\left(\Theta\left(\mathcal{U}^{\mathcal{N}}_{A\to BE}\right)\right)(|x\rangle\langle x|_X)\right)\right), \tag{4.7.6}$$

where the infimum is over all quantum states σ_E and the maximum is over all messages x in the set $\mathcal{X}$. In Figure 4.8, we show a schematic diagram of a protocol for private communication over a channel $\mathcal{N}_{A\to B}$. The one-shot private capacity of a channel $\mathcal{N}_{A\to B}$ is then defined as follows:

$$P^{\varepsilon}(\mathcal{N}_{A\to B}) := \sup_{\mathcal{X},\Theta\in\text{LO}}\left\{\log_2|\mathcal{X}| : p_{\text{err}}(\Theta,\mathcal{N})\leq\varepsilon\right\}, \tag{4.7.7}$$

where LO refers to the set of all superchannels that can be realized by local operations only and $|\mathcal{X}|$ refers to the number of elements in the set $\mathcal{X}$. As such, the supremum is over all sets of messages $\mathcal{X}$ and all superchannels $\Theta_{(A\to B)\to(X\to\hat{X})}$ that can be realized by only local operations.

In the one-way LOCC setting considered throughout this work, Alice is allowed to send arbitrary amounts of classical data to Bob, which is publicly available to any eavesdropper as well. In this setting, the quantity of interest is the one-shot forward-assisted private capacity of a channel, which is defined as follows:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\mathcal{X},\Theta\in 1\text{WL}} \left\{\log_2 |\mathcal{X}| : p_{\text{err}}(\Theta,\mathcal{N}) \leq \varepsilon\right\}, \tag{4.7.8}$$

where 1WL refers to the set of all one-way LOCC superchannels. Since LO $\subseteq$ 1WL, the following inequality holds for all quantum channels $\mathcal{N}_{A\to B}$:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \geq P^{\varepsilon}(\mathcal{N}_{A\to B}). \tag{4.7.9}$$

In the remainder of this paper, we will derive several upper bounds on the one-shot forward-assisted private capacity of channels, which, as a consequence of (4.7.9), also serve as upper bounds on the one-shot private capacity of the channel due to the inequality mentioned above.

In the presence of forward-classical assistance, the task of secret-key distillation is equivalent to the task of private communication. Suppose that a forward-assisted protocol allows Alice to send n private bits to Bob through a channel $\mathcal{N}_{A\to B}$ with some error ε. Alice can send a secret key itself through this channel, hence, transforming the one-shot private communication protocol to a one-shot secret-key distillation protocol. Moreover, in the forward-classical assistance setting, a secret-key distillation protocol can be transformed into a private communication protocol by using the one-time-pad scheme, thus demonstrating the equivalence between the two tasks.

Due to the equivalence between the tasks of private communication and secret-key distillation in the presence of forward-classical assistance, the one-shot forward-assisted private capacity of a channel $P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B})$ is equal to the one-shot, one-way distillable key of the channel. That is,

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) = K_D^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B})\,. \tag{4.7.10}$$

The techniques used in Section 4.6 for obtaining upper bounds on the one-shot, one-way distillable key of a state can be extended to obtain upper bounds on the one-shot, one-way distillable key of a channel, using the unextendible entanglement of channels. Furthermore, the equality in (4.7.10) allows us to obtain upper bounds on the one-shot forward-assisted private capacity, which are also upper bounds on the one-shot private capacity by definition.

4.7.2 Unextendible entanglement of channels

The generalized unextendible entanglement of channels was defined in [SW24b]. We briefly present the relevant properties of the quantity here.

Let us define the following set of channels with respect to a given channel $\mathcal{N}_{A\to B}$:

$$\mathcal{F}(\mathcal{N}_{A\to B}) := \{\mathrm{Tr}_B \circ \mathcal{P}_{A\to BE} : \mathrm{Tr}_E \circ \mathcal{P}_{A\to BE} = \mathcal{N}_{A\to B}\}\,, \tag{4.7.11}$$

where systems B and E are isomorphic. The generalized unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ is defined with respect to a generalized channel divergence $\mathbf{D}$ [CMW16, LKDW18] as follows:

$$\mathbf{E}^u(\mathcal{N}_{A\to B}) := \frac{1}{2}\inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \mathbf{D}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to E})\,, \tag{4.7.12}$$

where the generalized divergence between channels is defined as

$$\mathbf{D}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) = \sup_{\rho_{RA}\in\mathcal{S}(RA)} \mathbf{D}(\mathcal{N}_{A\to B}(\rho_{RA})\,\|\mathcal{M}_{A\to B}(\rho_{RA}))\,. \tag{4.7.13}$$

The generalized unextendible entanglement of a channel does not increase under the action of one-way LOCC superchannels, the latter defined in Section 4.3.2.

Lemma 4.4 ([SW24b]) *The generalized unextendible entanglement of a channel does not increase under the action of one-way LOCC superchannels. That is,*

$$\mathbf{E}^{u}(\Theta(\mathcal{N}_{A\to B})) \leq \mathbf{E}^{u}(\mathcal{N}_{A\to B}) \qquad \forall \Theta \in \mathrm{1WL}, \tag{4.7.14}$$

where 1WL *represents the set of all one-way LOCC superchannels.*

A more general statement of Lemma 4.4 was presented in [SW24b], where it was shown that the generalized unextendible entanglement of a channel does not increase under the action of two-extendible superchannels, which is a semidefinite relaxation of the set of one-way LOCC superchannels, and hence, contains the set of one-way LOCC superchannels. In this work we will only consider one-way LOCC superchannels and not two-extendible superchannels. We point the interested reader to [SW24b] for a more detailed discussion.

A direct consequence of Lemma 4.4 is that the maximum value of the generalized unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ is not larger than the generalized unextendible entanglement of the identity channel $\mathrm{id}_{A'\to B'}$, where $\dim(A') = \dim(B') = \min\{\dim(A), \dim(B)\}$. This can be seen from the following argument: Consider an arbitrary channel $\mathcal{N}_{A\to B}$. If $\dim(A) \geq \dim(B)$, then construct a superchannel $\Theta_{(B\to C)\to(A\to D)}$ that acts on an arbitrary channel $\mathcal{M}_{B\to C}$ as follows:

$$\Theta_{(B\to C)\to(A\to D)}(\mathcal{M}_{B\to C}) = \mathrm{id}_{C\to D} \circ \mathcal{M}_{B\to C} \circ \mathcal{N}_{A\to B}. \tag{4.7.15}$$

Lemma 4.4 implies the following inequality:

$$\mathbf{E}^u(\mathrm{id}_{B\to C}) \geq \mathbf{E}^u(\Theta(\mathrm{id}_{B\to C})) \tag{4.7.16}$$

$$= \mathbf{E}^u(\mathrm{id}_{C\to D} \circ \mathrm{id}_{B\to C} \circ \mathcal{N}_{A\to B}) \tag{4.7.17}$$

$$= \mathbf{E}^u(\mathcal{N}_{A\to B})\,. \tag{4.7.18}$$

Similarly, if $\dim(B) \geq \dim(A)$, then we can construct a superchannel $\Upsilon_{(D\to A)\to(C\to B)}$ that acts on an arbitrary channel $\mathcal{M}_{D\to A}$ as follows:

$$\Upsilon_{(D\to A)\to(C\to B)}(\mathcal{M}_{D\to A}) = \mathcal{N}_{A\to B} \circ \mathcal{M}_{D\to A} \circ \mathrm{id}_{C\to D}\,. \tag{4.7.19}$$

Once again, applying Lemma 4.4 leads to the following inequality:

$$\mathbf{E}^u(\mathrm{id}_{D\to A}) \geq \mathbf{E}^u(\Upsilon(\mathrm{id}_{D\to A})) = \mathbf{E}^u(\mathcal{N}_{A\to B})\,. \tag{4.7.20}$$

The inequalities in (4.7.18) and (4.7.20) can be written together as the following inequality:

$$\mathbf{E}^u(\mathcal{N}_{A\to B}) \leq \min\{\mathbf{E}^u(\mathrm{id}_{A\to C})\,, \mathbf{E}^u(\mathrm{id}_{B\to D})\}\,, \tag{4.7.21}$$

where $\dim(A) = \dim(C)$ and $\dim(B) = \dim(D)$.

Another important property of generalized unextendible entanglement of channels, which is relevant to our discussion, is its relation with the generalized unextendible entanglement of states. In particular, the generalized unextendible entanglement of a bipartite state that can be established between two distant parties using a quantum channel $\mathcal{N}_{A\to B}$ and one-way LOCC superchannels cannot be larger than the generalized unextendible entanglement of the channel $\mathcal{N}_{A\to B}$. We state this formally in Lemma 4.5 below.

Lemma 4.5 ([SW24b]) *The unextendible entanglement of a quantum state $\sigma_{RC'D}$, with respect to the partition $RC' : D$, that can be established between two parties using a point-to-point quantum*

channel $\mathcal{N}_{A\to B}$ and a one-way LOCC superchannel $\Theta_{(A\to B)\to(C\to C'D)}$ is no greater than the unextendible entanglement of the quantum channel $\mathcal{N}_{A\to B}$; i.e.,

$$\sup_{\rho_{RC}} \mathbf{E}^u(\sigma_{RC':D}) \leq \mathbf{E}^u(\mathcal{N}_{A\to B}), \tag{4.7.22}$$

where

$$\sigma_{RC'D} \coloneqq (\Theta_{(A\to B)\to(C\to C'D)}(\mathcal{N}_{A\to B}))(\rho_{RC}), \tag{4.7.23}$$

and ρ_{RC} is a quantum state. The symbol $\mathbf{E}^u(\sigma_{RC':D})$ denotes that the unextendible entanglement of the state $\sigma_{RC'D}$ is calculated with respect to the bipartition $RC' : D$.

Lemma 4.5, Lemma 4.3, and (4.7.5) provide us with all the necessary tools to obtain an upper bound on the one-shot, one-way distillable key of a channel using unextendible entanglement of channels.

The two important quantities that we will use in this section are the smooth-min unextendible entanglement of a channel and the α-geometric unextendible entanglement of the channel.

The smooth-min unextendible entanglement of a channel is defined in terms of the smooth-min relative entropy of channels as follows:

$$E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \coloneqq \frac{1}{2} \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} D^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to E}) \tag{4.7.24}$$

$$= \frac{1}{2} \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \sup_{\rho_{RA}\in\mathcal{S}(RA)} D^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}(\rho_{RA})\,\|\,\mathcal{M}_{A\to E}(\rho_{RA})), \tag{4.7.25}$$

where the smooth-min relative entropy of states was defined in (4.5.25). The smooth-min relative entropy of channels can be written as a semidefinite program [WW19b, Appendix B-3], and the set $\mathcal{F}(\mathcal{N})$ can also be described by semidefinite constraints. This allows us to write the smooth-min unextendible entanglement of a channel as a semidefinite program (see Appendix 4.H).

Proposition 4.6 *The smooth-min unextendible entanglement of a channel is bounded as follows:*

$$-\frac{1}{2}\log_2(1-\varepsilon) \leq E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}) \leq \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), \tag{4.7.26}$$

where $d := \min\{\dim(A), \dim(B)\}$.

Proof: See Appendix 4.F. □

The α-geometric unextendible entanglement of channels was explored in [SW24b] in the context of zero-error private communication. It is defined for a parameter $\alpha \in (0,1) \cup (1,2]$ as follows:

$$\widehat{E}_\alpha^u(\mathcal{N}_{A\to B}) := \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \frac{1}{2}\widehat{D}_\alpha(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) \tag{4.7.27}$$

$$= \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \sup_{\rho_{RA}\in\mathcal{S}(RA)} \frac{1}{2}\widehat{D}_\alpha(\mathcal{N}_{A\to B}(\rho_{RA})\|\mathcal{M}_{A\to B}(\rho_{RA}))\,, \tag{4.7.28}$$

where the α-geometric Rényi relative entropy of states is defined for all $\alpha \in (0,1)\cup(1,\infty)$ as follows [Mat13]:

$$\widehat{D}_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\log_2 \operatorname{Tr}\left[\sigma\left(\sigma^{-\frac{1}{2}}\rho\sigma^{-\frac{1}{2}}\right)^\alpha\right]. \tag{4.7.29}$$

We list some properties of the α-geometric unextendible entanglement of channels that are relevant to this work. We refer the interested reader to [SW24b] for a more detailed discussion of these properties:

1. **Monotonicity in α:** The α-geometric unextendible entanglement of channels increases monotonically with increasing α. That is,

$$\widehat{E}_\alpha^u(\mathcal{N}_{A\to B}) \geq \widehat{E}_\beta^u(\mathcal{N}_{A\to B}) \qquad \forall \alpha,\beta \in (0,1)\cup(1,2], \quad \alpha \geq \beta. \tag{4.7.30}$$

2. **Subadditivity:** The α-geometric unextendible entanglement of channels is subadditive under tensor products of channels. That is, the following inequality holds for all $\alpha \in (0,1) \cup (1,2]$:

$$\widehat{E}^u_\alpha(\mathcal{N}_{A\to B} \otimes \mathcal{M}_{A\to B}) \leq \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) + \widehat{E}^u_\alpha(\mathcal{M}_{A\to B}), \tag{4.7.31}$$

where $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A\to B}$ are quantum channels.

3. **Limiting case when $\alpha \to 1$:** The α-geometric unextendible entanglement converges to the unextendible entanglement induced by the Belavkin–Staszewski relative entropy as $\alpha \to 1$. That is,

$$\widehat{E}^u(\mathcal{N}_{A\to B}) := \lim_{\alpha\to 1} \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) = \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \frac{1}{2}\widehat{D}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}), \tag{4.7.32}$$

where the Belavkin–Staszewski relative entropy of states is defined as follows [BS82]:

$$\widehat{D}(\rho\|\sigma) := \begin{cases} \operatorname{Tr}\left[\rho \log_2\left(\sqrt{\rho}\sigma^{-1}\sqrt{\rho}\right)\right] & \text{if } \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \\ +\infty & \text{otherwise} \end{cases}, \tag{4.7.33}$$

and where σ^{-1} is taken on the support of σ and the logarithm is evaluated on the support of ρ. The rightmost equality in (4.7.32) follows directly from [DKQ+23, Proposition 36].

4. **Semidefinite program:** The α-geometric unextendible entanglement of a channel can be computed using a semidefinite program for rational values of $\alpha \in (1,2]$ (see Appendix 4.H).

The α-geometric unextendible entanglement of a channel can be related with the smooth-min unextendible entanglement using the inequality in (4.6.68). The α-geometric Rényi relative entropy of states is known to be larger than or equal to the α-sandwiched

Rényi relative entropy of states for all $\alpha \in (0,1) \cup (1,\infty)$ [Tom15, WWW24]. The inequality in (4.6.68) then implies the following inequality, which holds for all $\alpha \in (1,\infty)$ and $\varepsilon \in [0,1)$:

$$D^{\varepsilon}_{\min}(\rho\|\sigma) \leq \widetilde{D}_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right) \tag{4.7.34}$$

$$\leq \widehat{D}_{\alpha}(\rho\|\sigma) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{4.7.35}$$

We will restrict our discussion to $\alpha \in (1,2]$, as this is the interval for which the α-geometric Rényi relative entropy obeys the data-processing inequality. Setting $\rho \to (\mathrm{id}_R \otimes \mathcal{N})(\rho_{RA})$ and $\sigma \to (\mathrm{id}_R \otimes \mathcal{M})(\rho_{RA})$, where $\mathcal{N}$ and $\mathcal{M}$ are quantum channels, leads to the following inequality:

$$D^{\varepsilon}_{\min}((\mathrm{id}_R \otimes \mathcal{N})(\rho_{RA})\|(\mathrm{id}_R \otimes \mathcal{M})(\rho_{RA})) \leq \widehat{D}_{\alpha}((\mathrm{id}_R \otimes \mathcal{N})(\rho_{RA})\|(\mathrm{id}_R \otimes \mathcal{M})(\rho_{RA})) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{4.7.36}$$

Since the above inequality holds for every state ρ, we can take a supremum over all states and conclude the following inequality:

$$D^{\varepsilon}_{\min}(\mathcal{N}\|\mathcal{M}) \leq \widehat{D}_{\alpha}(\mathcal{N}\|\mathcal{M}) + \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{4.7.37}$$

Now taking an infimum over all $\mathcal{M} \in \mathcal{F}(\mathcal{N})$, we arrive at the following inequality, which holds for all $\alpha \in (1,2]$ and $\varepsilon \in [0,1)$:

$$E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) = \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \frac{1}{2} D^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) \tag{4.7.38}$$

$$\leq \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} \frac{1}{2} \widehat{D}_{\alpha}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) + \frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right) \tag{4.7.39}$$

$$= \widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) + \frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right). \tag{4.7.40}$$

4.7.3 Upper bounds on the one-shot private capacity of a channel

In this section, we discuss the application of the smooth-min unextendible entanglement and the max-unextendible entanglement of channels to obtaining upper bounds on the one-shot, one-way distillable key of a channel.

Smooth-min unextendible entanglement upper bound

Consider the following quantity:

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) := 2^{-2E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B})}. \tag{4.7.41}$$

Lemma 4.5 implies the following inequality:

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \leq \sup_{\substack{\rho_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A})\\ \Theta\in 1\text{WL}}} J^{\varepsilon}_{\min}\Big(\Big(\Theta_{(A\to B)\to(\hat{A}\to B'B'')}(\mathcal{N}_{A\to B})\Big)(\rho_{A'A''\hat{A}})\Big), \tag{4.7.42}$$

where $J^{\varepsilon}_{\min}(\cdot)$ for states was defined in (4.5.26). The supremum in the above inequality is over every state $\rho_{A'A''\hat{A}}$ and one-way LOCC superchannel $\Theta_{(A\to B)\to(\hat{A}\to B'B'')}$. The inequality in (4.7.42), along with Theorem 4.2 and Lemma 4.3, yields an upper bound on the one-shot forward-assisted private capacity of a channel, which we state in Theorem 4.4 below.

Theorem 4.4 (Unextendibility bound on one-shot private capacity) *Consider a quantum channel $\mathcal{N}_{A\to B}$ and a parameter $\varepsilon \in [0,1]$ such that*

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) > \varepsilon, \tag{4.7.43}$$

where $J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})$ is defined in (4.7.41). Then the one-shot, one-way distillable key of the channel, which is equal to the one-shot private capacity of the channel according to (4.7.10), is bounded from above by the following quantity:

$$P^{\varepsilon,\to}(\mathcal{N}_{A\to B}) = K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(\mathcal{N})(1-J^{\varepsilon}_{\min}(\mathcal{N}))}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}(\mathcal{N})-\varepsilon}\right)^2+1\right]. \tag{4.7.44}$$

Proof: Let $\mathcal{N}_{A\to B}$ be a quantum channel, and let $\varepsilon \in [0,1]$ be a parameter such that

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) > \varepsilon. \tag{4.7.45}$$

Using the equality relating the one-shot, one-way distillable key of a channel and the one-shot, one-way distillable key of a state from (4.7.5), we arrive at the following:

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) = \sup_{\Theta\in 1\text{WL},\psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A})} K_D^{\varepsilon,\to}(\Theta(\mathcal{N}_{A\to B})(\psi_{A'A''\hat{A}})) \tag{4.7.46}$$

$$\leq \sup_{\substack{\psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A}),\\ \Theta\in 1\text{WL}}} \left\{ \begin{array}{c} \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2+1\right] : \\ J^{\varepsilon}_{\min} = J^{\varepsilon}_{\min}((\Theta(\mathcal{N}))(\psi_{A'A''\hat{A}})) \end{array} \right\}, \tag{4.7.47}$$

where $J^{\varepsilon}_{\min}(\cdot)$ for states is defined in (4.5.26). The inequality in (4.7.47) follows from Theorem 4.2. Note that the above inequality holds only if $J^{\varepsilon}_{\min} > \varepsilon$, but since we have assumed that $J^{\varepsilon}_{\min}(\mathcal{N}) > \varepsilon$, the quantity $J^{\varepsilon}_{\min}$ is guaranteed to be strictly greater than ε due to (4.7.42).

Let us define

$$J^{\varepsilon,s}_{\min}(\mathcal{N}_{A\to B}) := \sup_{\substack{\psi_{A'A''\hat{A}}\in\mathcal{S}(A'A''\hat{A}),\\ \Theta\in 1\text{WL}}} J^{\varepsilon}_{\min}((\Theta(\mathcal{N}))(\psi_{A'A''\hat{A}}))\,. \tag{4.7.48}$$

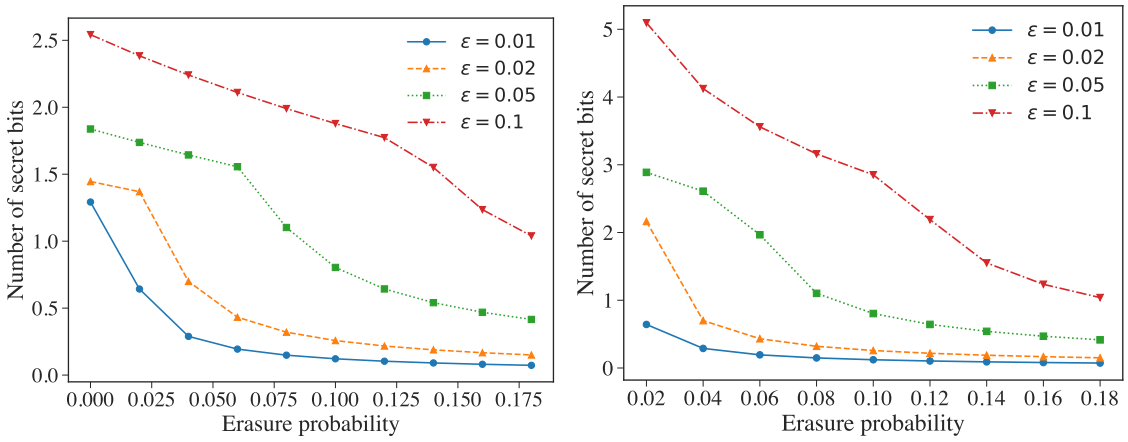
Then the inequality in (4.7.47) can be written as follows:

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon,s}_{\min}(\mathcal{N})\left(1-J^{\varepsilon,s}_{\min}(\mathcal{N})\right)}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon,s}_{\min}(\mathcal{N})-\varepsilon}\right)^2+1\right]. \tag{4.7.49}$$

The inequality in (4.7.42) states that $J^{\varepsilon}_{\min}(\mathcal{N}) \leq J^{\varepsilon,s}_{\min}(\mathcal{N})$. Therefore, by applying Lemma 4.3, we arrive at the following inequality:

$$K_D^{\varepsilon,\to}(\mathcal{N}_{A\to B}) \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(\mathcal{N})\left(1-J^{\varepsilon}_{\min}(\mathcal{N})\right)}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}(\mathcal{N})-\varepsilon}\right)^2+1\right]. \tag{4.7.50}$$

Finally, using the fact that the one-shot forward-assisted private capacity of a channel is equal to the one-shot one-way distillable key of the channel, we conclude the statement of the theorem. □



(a) Two-dimensional erasure channel (b) Three-dimensional erasure channel

Figure 4.9: Upper bound on the number of private bits that can be transmitted over a single use of an erasure channel assisted by local operations and forward-classical communication. The upper bound given in Theorem 4.4 is plotted against the erasure probability of an erasure channel for different values of ε.

In Figure 4.9, we plot the upper bounds on the one-shot forward-assisted private capacity of a two-dimensional and a three-dimensional erasure channel for different erasure probabilities and different values of ε. The erasure channel is mathematically defined as follows:

$$\mathcal{E}^{p}_{A\to B}(\rho_{RA}) = (1-p)\rho_{RB} + p\,\mathrm{Tr}_A[\rho_{RA}]\otimes|e\rangle\langle e|_B, \tag{4.7.51}$$

where $|e\rangle_B$ is the erasure symbol, which is orthogonal to every state in the span of $\{|i\rangle\langle j|\}_{i,j=0}^{d-1}$, and d is the dimension of the system A. The parameter $p \in [0,1]$ is the erasure probability of the channel.

The simplified upper bounds obtained in Corollaries 4.1 and 4.2 can be used to obtain simplified upper bounds on the one-shot forward-assisted private capacity of a channel. The inequality in (4.7.42), the equality in (4.7.5), and the application of Lemma 4.3 together lead to simplified upper bounds on the one-shot forward-assisted private capacity of a channel, stated in the corollary below.

Corollary 4.4 *Fix $\varepsilon \in [0,1]$. Let $\mathcal{N}_{A\to B}$ be a channel such that the following inequality holds:*

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) > \varepsilon, \tag{4.7.52}$$

where $J^{\varepsilon}_{\min}(\mathcal{N})$ is defined in (4.7.41). Then the one-shot forward-assisted private capacity of a channel is bounded from above as follows:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leq -\log_2\left(\sqrt{J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})} - \sqrt{\varepsilon}\right). \tag{4.7.53}$$

If $J^{\varepsilon}_{\min}(\mathcal{N}) > \sqrt{\varepsilon}$ then the following inequality also holds:

$$P^{\varepsilon,\rightarrow}(\mathcal{N}_{A\to B}) \leq -\frac{1}{2}\log_2\left(J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) - \sqrt{\varepsilon}\right). \tag{4.7.54}$$

α-Geometric unextendible entanglement upper bound

The subadditivity of the α-geometric unextendible entanglement of channels, as given in (4.7.31), can be used to obtain an upper bound on the n-shot, forward-assisted private capacity of a channel.

Consider an arbitrary quantum channel $\mathcal{N}_{A\to B}$. Recall the definition of $J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B})$ from (4.7.41). The inequality in (4.7.40) implies that the following inequality holds for all $\alpha \in (1,2]$ and $\varepsilon \in [0,1)$:

$$J^{\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \geq 2^{-2\widehat{E}^{u}_{\alpha}(\mathcal{N}) - \frac{\alpha}{\alpha-1}\log_2\left(\frac{1}{1-\varepsilon}\right)} \tag{4.7.55}$$

$$= (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2\widehat{E}^{u}_{\alpha}(\mathcal{N})}. \tag{4.7.56}$$

Now consider the following quantity:

$$J^{\varepsilon}_{\min}(\mathcal{N}^{\otimes n}_{A\to B}) \geq (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2\widehat{E}^{u}_{\alpha}(\mathcal{N}^{\otimes n})} \tag{4.7.57}$$

$$\geq (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2n\widehat{E}^{u}_{\alpha}(\mathcal{N})}, \tag{4.7.58}$$

where the second inequality follows from the subadditivity of the α-geometric unextendible entanglement of channels (see (4.7.31)).

Let us define the following quantity:

$$\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B}) \coloneqq (1-\varepsilon)^{\frac{\alpha}{\alpha-1}} 2^{-2n\widehat{E}_{\alpha}^{u}(\mathcal{N})}, \tag{4.7.59}$$

which, according to (4.7.58), is a lower bound on $J_{\min}^{\varepsilon}(\mathcal{N}_{A\to B})$. If α is a rational number in the interval $(1,2]$, then $\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B})$ can be computed using a semidefinite program, by employing the algorithms given in [FS17] (see Appendix 4.H for a special case). The application of Lemma 4.3 to Theorem 4.4, along with the inequality in (4.7.58), directly leads to a single-letter, semidefinite computable upper bound on the n-shot forward-assisted private capacity of a channel, which we state formally in Corollary 4.5 below.

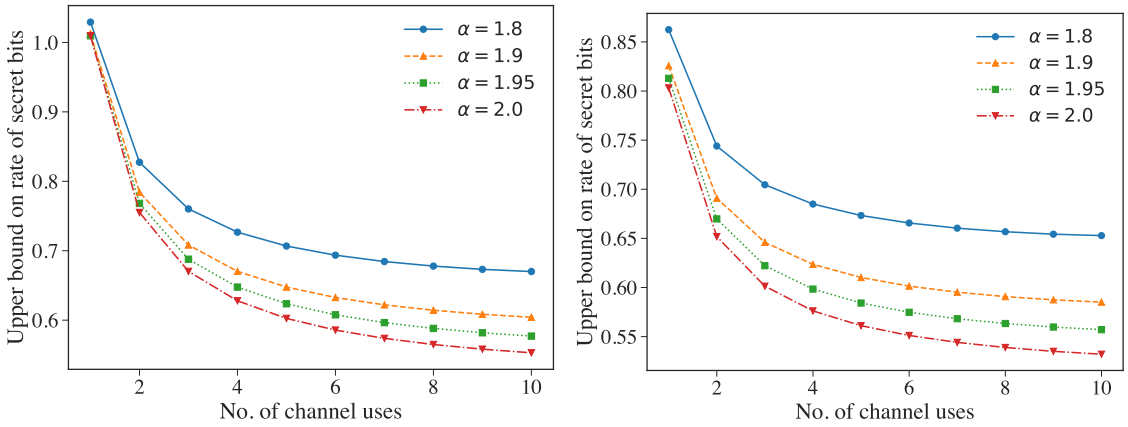
Corollary 4.5 *Fix $\varepsilon \in (0,1)$. Let $\mathcal{N}_{A\to B}$ be a quantum channel such that the following inequality holds for some $\alpha \in (1,2]$:*

$$\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B}) > \varepsilon \tag{4.7.60}$$

where $\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B})$ is defined in (4.7.59). Then the n-shot forward-assisted private capacity of a channel $\mathcal{N}_{A\to B}$ is bounded from above by the following quantity:

$$P^{\varepsilon,\to}(\mathcal{N}_{A\to B}^{\otimes n}) \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B})\left(1-\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B})\right)}+\sqrt{\varepsilon(1-\varepsilon)}}{\widehat{J}_{\alpha}^{\varepsilon,n}(\mathcal{N}_{A\to B})-\varepsilon}\right)^2+1\right]. \tag{4.7.61}$$

We turn to the erasure channel once again to demonstrate our results stated in Corollary 4.5. An erasure channel with erasure probability greater than or equal to $\frac{1}{2}$ (see (4.7.51)) is a two-extendible channel, and hence, its α-geometric unextendible entanglement is equal to zero for all $\alpha \in (0,1)\cup(1,2]$. If the erasure probability is less than $\frac{1}{2}$, then the explicit form of the α-geometric unextendible entanglement can be derived, which we state in Proposition 4.7 below.



(a) Erasure probability = 0.2 (b) Erasure probability = 0.3

Figure 4.10: Upper bound on the n-shot private capacity of an erasure channel with the error parameter $\varepsilon = 10^{-7}$. The bounds are computed for different values of α using Corollary 4.5, where the α-geometric unextendible entanglement of the erasure channel is computed using Proposition 4.7.

Proposition 4.7 *For all $\alpha \in (0,1) \cup (1,2]$, the α-geometric unextendible entanglement of a d-dimensional erasure channel, with erasure probability p, evaluates to the following:*

$$\widehat{E}^{u}_{\alpha}\left(\mathcal{E}^{p}_{A\to B}\right) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(\left(p+\frac{b_{\text{opt}}}{d^2}\right)^{1-\alpha}(1-p)^{\alpha}+(1-p-b_{\text{opt}})^{1-\alpha}p^{\alpha}\right) \tag{4.7.62}$$

for all $p \in \left(0, \frac{1}{d^{1/\alpha}+1}\right]$, where

$$b_{\text{opt}} := \frac{d^2\left((1-p)^2 - p^2 d^{2/\alpha}\right)}{pd^{2/\alpha}+(1-p)d^2}. \tag{4.7.63}$$

For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}^{u}_{\alpha}\left(\mathcal{E}^{p}_{A\to B}\right) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(p^{1-\alpha}(1-p)^{\alpha}+(1-p)^{1-\alpha}p^{\alpha}\right). \tag{4.7.64}$$

Proof: See Appendix 4.G. □

In Figure 4.10 we plot the upper bound on the n-shot, forward-assisted private capacity of erasure channels computed using Corollary 4.5. The α-geometric unextendible entanglement of the erasure channel is computed using Proposition 4.7. The n-shot forward-

assisted private capacity of a channel is expected to increase with the number of channel uses. In Figure 4.10 however, the computed value of the upper bound on the n-shot forward-assisted private capacity decreases with the number of channel uses, which indicates that the upper bound improves with an increasing number of channel uses.

Private communication over a channel in the asymptotic setting

In this section we study private communication over quantum channels using one-way LOCC superchannels in the asymptotic setting.

First, let us consider the task of secret-key distillation from quantum channels in a setting similar to the one discussed in Section 4.6.3. In the asymptotic setting, a one-way LOCC protocol to distill secret keys from a channel $\mathcal{N}_{A\to B}$ is described by a sequence of positive integers $\{k_n\}_{n\in\mathbb{N}}$, a sequence of bipartite private states $\left\{\gamma^{k_n}_{A'A''B'B''}\right\}_{n\in\mathbb{N}}$, a sequence of one-way LOCC superchannels $\left\{\Theta^{n,1\text{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}\right\}_{n\in\mathbb{N}}$, a sequence of states $\left\{\rho^n_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}$, and a sequence of error parameters $\{\varepsilon_n\}_{n\in\mathbb{N}}$. A sequence of tuples, $\left\{\left(k_n, \gamma^{k_n}_{A'A''B'B''}, \Theta^{n,1\text{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}, \rho^n_{A'A''\hat{A}}, \varepsilon_n\right)\right\}_{n\in\mathbb{N}}$, describes a one-way LOCC secret-key distillation protocol for a channel $\mathcal{N}_{A\to B}$ if the following inequality holds for all $n\in\mathbb{N}$:

$$F\left(\gamma^{k_n}, \left(\Theta^{n,1\text{WL}}(\mathcal{N}^{\otimes n})\right)(\rho^n)\right) \geq 1-\varepsilon_n, \tag{4.7.65}$$

and $\varepsilon_n \to 0$ as $n\to\infty$. We are interested in the maximum rate at which secret bits can be distilled from a channel $\mathcal{N}_{A\to B}$ using any such one-way LOCC secret-key distillation protocol.

Similar to the discussion in Section 4.6.3, we impose an additional constraint on the sequence of error parameters ε_n, that $\varepsilon_n \leq 2^{-an}$ for some fixed error exponent $a>0$. We define the quantity "a-exponential one-way distillable key of a channel" as the maximum

rate at which secret bits can be distilled from a channel using a one-way LOCC secret-key distillation protocol, with a being the error exponent.

Definition 4.8 *Fix $a > 0$. The a-exponential one-way distillable key of a channel $\mathcal{N}_{A\to B}$ is defined as follows:*

$$K^{\rightarrow}_{D,a}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{\{k_n\}_{n\in\mathbb{N}},\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\Theta^{n,1\mathrm{WL}}\right\}_{n\in\mathbb{N}},\left\{\rho^n_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}}} \liminf_{n\to\infty} \left\{ \frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}, \Theta^{n,1\mathrm{WL}}(\mathcal{N}^{\otimes n})(\rho^n)\right) \geq 1 - 2^{-an} \right\}, \quad (4.7.66)$$

where the supremum is over all sequences of integers $\{k_n\}_{n\in\mathbb{N}}$, all sequences of bipartite states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$, all sequences of one-way LOCC superchannels $\left\{\Theta^{n,1\mathrm{WL}}_{(A^n\to B^n)\to A'B'A''B''}\right\}_{n\in\mathbb{N}}$, and all sequences of states $\{\rho_{A'A''\hat{A}}\}_{n\in\mathbb{N}}$. The bipartite state $\gamma^{k_n}_{A'B'A''B''}$ holds $\log_2 k_n$ secret bits.

We define the converse of a-exponential one-way distillable key of the channel $\mathcal{N}_{A\to B}$ as follows:

$$\widetilde{K}^{\rightarrow}_{D,a}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\substack{\{k_n\}_{n\in\mathbb{N}},\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}} \\ \left\{\Theta^{n,1\mathrm{WL}}\right\}_{n\in\mathbb{N}},\left\{\rho^n_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}}} \limsup_{n\to\infty} \left\{ \frac{\log_2 k_n}{n} : F\left(\gamma^{k_n}, \Theta^{n,1\mathrm{WL}}(\mathcal{N}^{\otimes n})(\rho^n)\right) \geq 1 - 2^{-an} \right\}. \quad (4.7.67)$$

We can also consider the task of private communication over channels in this setting. We define the a-exponential forward-assisted private capacity of a channel as follows:

Definition 4.9 *Fix $a > 0$. The a-exponential forward-assisted private capacity of a channel $\mathcal{N}_{A\to B}$ is defined as follows:*

$$P^{\rightarrow}_{a}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\{\mathcal{X}_n\}_{n\in\mathbb{N}},\left\{\Theta^{n,1\mathrm{WL}}\right\}_{n\in\mathbb{N}}} \liminf_{n\to\infty} \left\{ \frac{\log_2 |\mathcal{X}_n|}{n} : p_{\mathrm{err}}\left(\mathcal{N}^{\otimes n}, \Theta^{n,1\mathrm{WL}}\right) \leq 2^{-an} \right\}, \quad (4.7.68)$$

where the supremum is over all sequences of message sets $\{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and all sequences of one-way LOCC superchannels $\left\{\Theta^{n,1\mathrm{WL}}_{(A^n\to B^n)\to(X\to\hat{X})}\right\}_{n\in\mathbb{N}}$.

We define the converse of a-exponential forward-assisted private capacity of the channel $\mathcal{N}_{A\to B}$ as follows:

$$\widetilde{P}_a^{\rightarrow}(\mathcal{N}_{A\to B}) \coloneqq \sup_{\{\mathcal{X}_n\}_{n\in\mathbb{N}},\left\{\Theta^{n,1\mathrm{WL}}\right\}_{n\in\mathbb{N}}} \limsup_{n\to\infty} \left\{ \frac{\log_2 |\mathcal{X}_n|}{n} : p_{\mathrm{err}}\left(\mathcal{N}^{\otimes n}, \Theta^{n,1\mathrm{WL}}\right) \leq 2^{-an} \right\}. \tag{4.7.69}$$

Using the arguments mentioned before (4.7.10), we can see that the following equalities hold:

$$K_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B}) = P_a^{\rightarrow}(\mathcal{N}_{A\to B}) \tag{4.7.70}$$

$$\widetilde{K}_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B}) = \widetilde{P}_a^{\rightarrow}(\mathcal{N}_{A\to B}). \tag{4.7.71}$$

Therefore, any bounds obtained on the a-exponential distillable key of a channel hold for the a-exponential private capacity of the channel as well.

Theorem 4.5 *Consider an arbitrary quantum channel $\mathcal{N}_{A\to B}$. Let $d \coloneqq \min\{\dim(A), \dim(B)\}$ with $\dim(A)$ and $\dim(B)$ being the dimensions of systems A and B, respectively. Fix $a \in (2\log_2 d, \infty)$. Then the following bound holds:*

$$\widetilde{P}_a^{\rightarrow}(\mathcal{N}_{A\to B}) = \widetilde{K}_{D,a}^{\rightarrow}(\mathcal{N}_{A\to B}) \leq \widehat{E}^u(\mathcal{N}_{A\to B}), \tag{4.7.72}$$

where $\widehat{E}^u(\mathcal{N}_{A\to B})$ is the unextendible entanglement of the channel $\mathcal{N}_{A\to B}$ induced by the Belavkin–Staszewski relative entropy defined in (4.7.32).

Proof: The proof is similar to the proof of Theorem 4.3. We sketch out the main arguments here.

Let $\mathcal{N}_{A\to B}$ be an arbitrary quantum channel, with input and output dimensions $\dim(A)$ and $\dim(B)$ respectively, from which we wish to distill secret keys. Let $\left\{\Theta^{n,1\mathrm{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}\right\}_{n\in\mathbb{N}}$ be a sequence of one-way LOCC superchannels, let $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$ be

a sequence of bipartite private states, and let $\left\{\rho^n_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}$ be a sequence of quantum states such that the following condition holds for all $a > 2\log_2 d$ and $n \in \mathbb{N}$:

$$F\left(\gamma^{k_n}_{A'B'A''B''}, \left(\Theta^{n,\mathrm{1WL}}(\mathcal{N}^{\otimes n}_{A\to B})\right)\left(\rho^n_{A'A''\hat{A}}\right)\right) \geq 1 - 2^{-an}, \tag{4.7.73}$$

where $d := \min\{\dim(A), \dim(B)\}$.

Let us set $\varepsilon_n := 2^{-an}$ for convenience. Corollary 4.4 implies that the following inequality holds for all one-way LOCC secret-key distillation protocols such that (4.7.73) is satisfied:

$$\log_2 k_n \leq -\log_2\left(\sqrt{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})} - \sqrt{\varepsilon_n}\right) \tag{4.7.74}$$

$$= -\frac{1}{2}\log_2\left(J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})\right) - \log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})}}\right). \tag{4.7.75}$$

The quantity $J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})$ is bounded from below by the following quantity:

$$J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n}_{A\to B}) \geq \frac{1-\varepsilon_n}{d^{2n}}, \tag{4.7.76}$$

which is evident from Proposition 4.6. The inequalities in (4.7.75) and (4.7.76) allow us to use the mathematical arguments presented in (4.6.93)–(4.6.100) in order to conclude the following:

$$\limsup_{n\to\infty} -\frac{1}{n}\log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})}}\right) = 0. \tag{4.7.77}$$

Therefore, taking $\limsup_{n\to\infty}$ in (4.7.75) leads to the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leq \limsup_{n\to\infty}\left\{-\frac{1}{2n}\log_2\left(J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})\right) - \frac{1}{n}\log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})}}\right)\right\} \tag{4.7.78}$$

$$= \limsup_{n\to\infty} -\frac{1}{2n}\log_2\left(J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})\right) + \limsup_{n\to\infty} -\frac{1}{n}\log_2\left(1 - \sqrt{\frac{\varepsilon_n}{J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})}}\right) \tag{4.7.79}$$

$$= \limsup_{n\to\infty} -\frac{1}{2n}\log_2\left(J^{\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n})\right) \tag{4.7.80}$$

$$= \limsup_{n\to\infty} \frac{1}{n} E^{u,\varepsilon_n}_{\min}(\mathcal{N}^{\otimes n}), \tag{4.7.81}$$

where the second equality follows from (4.7.77).

Recall the relation between the smooth-min unextendible entanglement of a channel and the α-geometric unextendible entanglement of the channel from (4.7.40). The inequality in (4.7.40) combined with (4.7.81) leads to the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leq \limsup_{n\to\infty} \frac{1}{n}\left(\widehat{E}^u_\alpha(\mathcal{N}^{\otimes n}) - \frac{1}{2}\cdot\frac{\alpha}{\alpha-1}\log_2(1-\varepsilon_n)\right) \tag{4.7.82}$$

$$= \limsup_{n\to\infty} \frac{1}{n}\widehat{E}^u_\alpha(\mathcal{N}^{\otimes n}) + \limsup_{n\to\infty} -\frac{1}{2n}\cdot\frac{\alpha}{\alpha-1}\log_2(1-\varepsilon_n), \tag{4.7.83}$$

which holds for all $\alpha \in (1,2]$. Since $\varepsilon_n \to 0$ as $n \to \infty$,

$$\limsup_{n\to\infty} -\frac{1}{2n}\cdot\frac{\alpha}{\alpha-1}\log_2(1-\varepsilon_n) = 0. \tag{4.7.84}$$

Now using the subadditivity of the α-geometric unextendible entanglement of channels, we arrive at the following inequality:

$$\limsup_{n\to\infty} \frac{\log_2 k_n}{n} \leq \limsup_{n\to\infty} \frac{1}{n}\widehat{E}^u_\alpha(\mathcal{N}^{\otimes n}) \leq \widehat{E}^u_\alpha(\mathcal{N}). \tag{4.7.85}$$

The above inequality holds for every sequence $\{k_n\}_{n\in\mathbb{N}}$ for which there exists a sequence of private states $\left\{\gamma^{k_n}_{A'B'A''B''}\right\}_{n\in\mathbb{N}}$, a sequence of one-way LOCC superchannels $\left\{\Theta^{n,1\text{WL}}_{(A^n\to B^n)\to(\hat{A}\to B'B'')}\right\}_{n\in\mathbb{N}}$, and a sequence of states $\left\{\rho^n_{A'A''\hat{A}}\right\}_{n\in\mathbb{N}}$ such that (4.7.73) holds for all $a > 2\log_2 d$ and $n \in \mathbb{N}$. Therefore,

$$\widetilde{K}^{\rightarrow}_{D,a}(\mathcal{N}_{A\to B}) \leq \widehat{E}^u_\alpha(\mathcal{N}_{A\to B}) \qquad \forall \alpha \in (1,2], \tag{4.7.86}$$

which follows from the definition of $\widetilde{K}^{\rightarrow}_{D,a}(\mathcal{N}_{A\to B})$. Since the α-geometric unextendible entanglement of a channel increases monotonically with α, we can take $\lim_{\alpha\to 1^+}$ to obtain the tightest upper bound, which is the unextendible entanglement of the channel $\mathcal{N}_{A\to B}$ induced by the Belavkin–Staszewski relative entropy. Finally, using (4.7.71) leads to the statement of the theorem. □

4.8 Conclusion

In this paper we studied the task of secret-key distillation from bipartite states and point-to-point quantum channels using local operations and one-way classical communication. Using the resource theory of unextendible entanglement, which is a semidefinite relaxation of the resource theory of entanglement, we obtained efficiently computable upper bounds on several quantities of interest in the theory of private communication over a quantum network.

We derived efficiently computable upper bounds on the one-shot, one-way distillable key of a bipartite state using the resource theory of unextendible entanglement. We also derived upper bounds on the one-shot forward-assisted private capacity of a channel that can be computed using a semidefinite program. In both cases, these are the first instances of efficiently computable upper bounds on these quantities, to the best of our knowledge.

We extended our results to the i.i.d. setting and obtained single-letter efficiently computable upper bounds on the n-shot one-way distillable key of bipartite states and n-shot forward-assisted private capacity of point-to-point channels. Finally, we obtained efficiently computable upper bounds on the rate at which secret keys can be distilled from a bipartite state or a quantum channel using one-way LOCC when the error is required to decay exponentially with an error exponent larger than a fixed threshold.

The majority of bounds obtained in this work can be computed using semidefinite programs. We numerically computed the upper bounds on the one-shot, one-way distillable key and n-shot one-way distillable key for isotropic states to demonstrate our results. We also found analytical expressions for the upper bounds on the n-shot forward-assisted private capacity of erasure channels.

We obtained a family of upper bounds on the n-shot, one-way distillable key of a bipartite state in this work using the α-sandwiched Rényi relative entropy. However, a semidefinite representation of the α-sandwiched Rényi relative entropy is only known when $\alpha \to \infty$. As such, only one member from the family of upper bounds on the n-shot, one-way distillable key of a state is known to be efficiently computable.

Going forward from here, there are some open problems left for future investigation. The bounds obtained in this work are based on the resource theory of unextendible entanglement. It may be possible to obtain stronger bounds by studying entanglement measures that combine the concepts of unextendibility and the positive partial transpose (PPT) criterion. Furthermore, it can give insights into the asymptotic setting of private communication where there are no assumptions on the rate at which error decays. As another open problem of interest, finding semidefinite representations of the α-sandwiched Rényi relative entropies would improve our numerical findings here, as they can lead to tighter efficiently computable bounds on the n-shot, one-way distillable key of a state.

BIBLIOGRAPHY

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984. doi:10.1016/j.tcs.2014.05.025.

[BD10] Francesco Buscemi and Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, 2010. arXiv:0902.0158, doi:10.1109/TIT.2009.2039166.

[BD11] Fernando G. S. L. Brandao and Nilanjana Datta. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Transactions on Information Theory*, 57(3):1754–1760, 2011. arXiv:0905.2673, doi:10.1109/TIT.2011.2104531.

[BS82] V. P. Belavkin and P. Staszewski. C*-algebraic generalization of relative entropy and entropy. *Annales de l'I.H.P. Physique théorique*, 37(1):51–58, 1982. URL: http://eudml.org/doc/76163.

[CDP08] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Transforming quantum operations: Quantum supermaps. *Europhysics Letters*, 83(3):30004, July 2008. arXiv:0804.0180, doi:10.1209/0295-5075/83/30004.

[CEH+07] Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner. Unifying classical and quantum key distillation. In Salil P. Vadhan, editor, *Theory of Cryptography*, pages 456–478, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. arXiv:quant-ph/0608199, doi:10.1007/978-3-540-70936-7_25.

[Chr06] Matthias Christandl. The structure of bipartite quantum states - insights from group theory and cryptography, 2006. arXiv:quant-ph/0604183.

[CMW16] Tom Cooney, Milán Mosonyi, and Mark M. Wilde. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. *Communications in Mathematical Physics*, 344(3):797–829, 2016. arXiv:1408.3373, doi:10.1007/s00220-016-2645-4.

[CSW12] Matthias Christandl, Norbert Schuch, and Andreas Winter. Entanglement of the antisymmetric state. *Communications in Mathematical Physics*, 311(2):397–422, 2012. arXiv:0910.4151, doi:10.1007/s00220-012-1446-7.

[CW04] Matthias Christandl and Andreas Winter. "Squashed entanglement": an additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, 9/2/2024 2004. arXiv:quant-ph/0308088, doi:10.1063/1.1643788.

[CWY04] N. Cai, A. Winter, and R. W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2004. doi:10.1007/s11122-005-0002-x.

[Dat09] Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, 2009. arXiv:0803.2770, doi:10.1109/TIT.2009.2018325.

[DFW+18] María García Díaz, Kun Fang, Xin Wang, Matteo Rosati, Michalis Skotiniotis, John Calsamiglia, and Andreas Winter. Using and reusing coherence to realize quantum processes. *Quantum*, 2:100, October 2018. arXiv:1805.04045, doi:10.22331/q-2018-10-19-100.

[DKQ+23] Dawei Ding, Sumeet Khatri, Yihui Quek, Peter W. Shor, Xin Wang, and Mark M. Wilde. Bounding the forward classical capacity of bipartite quantum channels. *IEEE Transactions on Information Theory*, 69(5):3034–3061, 2023. arXiv:2010.01058, doi:10.1109/TIT.2022.3233924.

[DLL03] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu. Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block. *Physical Review A*, 68(4):042317, October 2003. arXiv:quant-ph/0308173, doi:10.1103/PhysRevA.68.042317.

[DPS04] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Physical Review A*, 69(2):022308, February 2004. arXiv:quant-ph/0308032, doi:10.1103/PhysRevA.69.022308.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, January 2005. doi:10.1098/rspa.2004.1372.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical*

Review Letters, 67(6):661–663, August 1991. doi:10.1103/PhysRevLett.67.661.

[FF21] Kun Fang and Hamza Fawzi. Geometric Rényi divergence and its applications in quantum channel capacities. *Communications in Mathematical Physics*, 384(3):1615–1677, May 2021. arXiv:1909.05758, doi:10.1007/s00220-021-04064-4.

[FS17] Hamza Fawzi and James Saunderson. Lieb's concavity theorem, matrix geometric means, and semidefinite optimization. *Linear Algebra and its Applications*, 513:240–263, 2017. URL: https://www.sciencedirect.com/science/article/pii/S0024379516304852, arXiv:1512.03401, doi:10.1016/j.laa.2016.10.012.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999. arXiv:quant-ph/9712042, doi:10.1109/18.761271.

[Gha10] Sevag Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information and Computation*, 10(3):343–360, March 2010. arXiv:0810.4507, doi:10.26421/qic10.3-4-11.

[Gou19] Gilad Gour. Comparison of quantum channels by superchannels. *IEEE Transactions on Information Theory*, 65(9):5880–5904, September 2019. arXiv:1808.02607, doi:10.1109/tit.2019.2907989.

[Gur03] Leonid Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '03, page 10–19, New York, NY, USA, 2003. Association for Computing Machinery. arXiv:quant-ph/0303055, doi:10.1145/780542.780545.

[HH99] Michal Horodecki and Pawel Horodecki. Reduction criterion of separability and limits for a class of distillation protocols. *Physical Review A*, 59(6):4206–4216, June 1999. arXiv:quant-ph/9708015, doi:10.1103/PhysRevA.59.4206.

[HHH+08a] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Debbie Leung, and Jonathan Oppenheim. Quantum key distribution based on private states:

Unconditional security over untrusted channels with zero quantum capacity. *IEEE Transactions on Information Theory*, 54(6):2604–2620, 2008. arXiv:quant-ph/0608195, doi:10.1109/TIT.2008.921870.

[HHH+08b] Karol Horodecki, Michal Horodecki, Pawel Horodecki, Debbie Leung, and Jonathan Oppenheim. Unconditional privacy over channels which cannot convey quantum information. *Physical Review Letters*, 100:110502, March 2008. arXiv:quant-ph/0702077, doi:10.1103/PhysRevLett.100.110502.

[HHHO05] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, April 2005. doi:10.1103/PhysRevLett.94.160502.

[HHHO09] Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189, doi:10.1109/tit.2008.2009798.

[HMZ16] Teiko Heinosaari, Takayuki Miyadera, and Mário Ziman. An invitation to quantum incompatibility. *Journal of Physics A: Mathematical and Theoretical*, 49(12):123001, February 2016. arXiv:1511.07548, doi:10.1088/1751-8113/49/12/123001.

[HSW23] Tharon Holdsworth, Vishal Singh, and Mark M. Wilde. Quantifying the performance of approximate teleportation and quantum error correction via symmetric 2-PPT-extendible channels. *Physical Review A*, 107(1):012428, Jan 2023. arXiv:2207.06931, doi:10.1103/PhysRevA.107.012428.

[KDWW19] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility limits the performance of quantum processors. *Physical Review Letters*, 123(7):070502, August 2019. arXiv:2108.03137, doi:10.1103/physrevlett.123.070502.

[KDWW21] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Resource theory of unextendibility and nonasymptotic quantum capacity. *Physical Review A*, 104(2):022401, August 2021. arXiv:1803.10710, doi:10.1103/physreva.104.022401.

[KKGW21] Sumeet Khatri, Eneet Kaur, Saikat Guha, and Mark M. Wilde. Second-order

coding rates for key distillation in quantum key distribution, 2021. arXiv:1910.03883.

[KS24] Gereon Koßmann and René Schwonnek. Optimising the relative entropy under semi definite constraints – a new tool for estimating key rates in QKD, 2024. arXiv:2404.17016.

[KW24] Sumeet Khatri and Mark M. Wilde. Principles of quantum communication theory: A modern approach, 2024. arXiv:2011.04672v2.

[LDS18] Felix Leditzky, Nilanjana Datta, and Graeme Smith. Useful states and entanglement distillation. *IEEE Transactions on Information Theory*, 64(7):4689–4708, 2018. arXiv:1701.03081, doi:10.1109/TIT.2017.2776907.

[LKDW18] Felix Leditzky, Eneet Kaur, Nilanjana Datta, and Mark M. Wilde. Approaches for approximate additivity of the Holevo information of quantum channels. *Physical Review A*, 97:012332, January 2018. doi:10.1103/PhysRevA.97.012332.

[LM15] Debbie Leung and William Matthews. On the power of PPT-preserving and non-signalling codes. *IEEE Transactions on Information Theory*, 61(8):4486–4499, 2015. arXiv:1406.7142, doi:10.1109/TIT.2015.2439953.

[Mat13] Keiji Matsumoto. A new quantum version of f-divergence, 2013. arXiv:1311.4722, doi:10.48550/ARXIV.1311.4722.

[MH11] Milán Mosonyi and Fumio Hiai. On the quantum Rényi relative entropies and related capacity formulas. *IEEE Transactions on Information Theory*, 57(4):2474–2487, 2011. arXiv:0912.1286, doi:10.1109/TIT.2011.2110050.

[MLDS+13] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. On quantum Rényi entropies: A new generalization and some properties. *Journal of Mathematical Physics*, 54(12):122203, December 2013. arXiv:1306.3142, doi:10.1063/1.4838856.

[MO21] Milán Mosonyi and Tomohiro Ogawa. Divergence radii and the strong converse exponent of classical-quantum channel coding with constant compositions. *IEEE Transactions on Information Theory*, 67(3):1668–1698, 2021. arXiv:1811.10599, doi:10.1109/TIT.2020.3041205.

[NO00] H. Nagaoka and T. Ogawa. Strong converse and Stein's lemma in quantum hypothesis testing. *IEEE Transactions on Information Theory*, 46:2428–2433, November 2000. URL: http://ieeexplore.ieee.org/document/887855/, doi:10.1109/18.887855.

[Pet86] Dénes Petz. Quasi-entropies for finite quantum systems. *Reports on Mathematical Physics*, 23(1):57–65, 1986. URL: https://www.sciencedirect.com/science/article/pii/0034487786900674, arXiv:1009.2679, doi:10.1016/0034-4877(86)90067-4.

[PV10] Yury Polyanskiy and Sergio Verdú. Arimoto channel coding converse and Rényi divergence. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1327–1333, 2010. doi:10.1109/ALLERTON.2010.5707067.

[QSW18] Haoyu Qi, Kunal Sharma, and Mark M. Wilde. Entanglement-assisted private communication over quantum broadcast channels. *Journal of Physics A: Mathematical and Theoretical*, 51(37):374001, August 2018. arXiv:1803.03976, doi:10.1088/1751-8121/aad5f3.

[RBL18] Denis Rosset, Francesco Buscemi, and Yeong-Cherng Liang. Resource theory of quantum memories and their faithful verification with minimal assumptions. *Physical Review X*, 8(2):021033, May 2018. arXiv:1710.04710, doi:10.1103/PhysRevX.8.021033.

[RR11] Joseph M. Renes and Renato Renner. Noisy channel coding via privacy amplification and information reconciliation. *IEEE Transactions on Information Theory*, 57(11):7377–7385, 2011. arXiv:1012.4814, doi:10.1109/TIT.2011.2162226.

[RR12] Joseph M. Renes and Renato Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Transactions on Information Theory*, 58(3):1985–1991, 2012. arXiv:1008.0452, doi:10.1109/TIT.2011.2177589.

[RSW17] Jaikumar Radhakrishnan, Pranab Sen, and Naqueeb Ahmad Warsi. One-shot private classical capacity of quantum wiretap channel: Based on one-shot quantum covering lemma, 2017. arXiv:1703.01932.

[Sio58] Maurice Sion. On general minimax theorems. *Pacific Journal of Mathematics*, 8(1):171–176, March 1958. doi:10.2140/pjm.1958.8.171.

[SW24a] Vishal Singh and Mark M. Wilde. No-go theorem for probabilistic one-way secret-key distillation, 2024. arXiv:2404.01392.

[SW24b] Vishal Singh and Mark M. Wilde. Unextendible entanglement of quantum channels, 2024. arXiv:2407.15944.

[TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, 2014. arXiv:1310.0129, doi:10.1109/TIT.2014.2330313.

[Tom15] Marco Tomamichel. *Quantum Information Processing with Finite Resources*. Springer Cham, 2015. arXiv:1504.00233, doi:10.1007/978-3-319-21891-5.

[Ume62] Hisaharu Umegaki. Conditional expectation in an operator algebra. IV. Entropy and information. *Kodai Mathematical Seminar Reports*, 14(2):59 – 85, 1962. doi:10.2996/kmj/1138844604.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. doi:10.1017/9781316848142.

[WBHK20] Mark M. Wilde, Mario Berta, Christoph Hirche, and Eneet Kaur. Amortized channel divergence for asymptotic quantum channel discrimination. *Letters in Mathematical Physics*, 110(8):2277–2336, 2020. arXiv:1808.01498, doi:10.1007/s11005-020-01297-7.

[Wer89] Reinhard F. Werner. An application of Bell's inequalities to a quantum state extension problem. *Letters in Mathematical Physics*, 17(4):359–363, 1989. doi:10.1007/BF00399761.

[Wil16] Mark M. Wilde. Squashed entanglement and approximate private states. *Quantum Information Processing*, 15(11):4563–4580, November 2016. arXiv:1606.08028, doi:10.1007/s11128-016-1432-7.

[Wil17] Mark M. Wilde. Position-based coding and convex splitting for private communication over quantum channels. *Quantum Information Processing*, 16(10):264, September 2017. arXiv:1703.01733, doi:10.1007/s11128-017-1718-4.

[WR12] Ligong Wang and Renato Renner. One-shot classical-quantum capacity and

hypothesis testing. *Physical Review Letters*, 108(20):200501, May 2012. arXiv:1007.5456, doi:10.1103/PhysRevLett.108.200501.

[WTB17] Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, 2017. arXiv:1602.08898, doi:10.1109/TIT.2017.2648825.

[WW19a] Xin Wang and Mark M. Wilde. Resource theory of asymmetric distinguishability. *Physical Review Research*, 1(3):033170, December 2019. arXiv:1905.11629, doi:10.1103/PhysRevResearch.1.033170.

[WW19b] Xin Wang and Mark M. Wilde. Resource theory of asymmetric distinguishability for quantum channels. *Physical Review Research*, 1(3):033169, December 2019. arXiv:1907.06306, doi:10.1103/PhysRevResearch.1.033169.

[WWW24] Kun Wang, Xin Wang, and Mark M. Wilde. Quantifying the unextendibility of entanglement. *New Journal of Physics*, 26(3):033013, March 2024. arXiv:1911.07433, doi:10.1088/1367-2630/ad264e.

[WWY14] 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, July 2014. arXiv:1306.1586, doi:10.1007/s00220-014-2122-x.

[Yan06] Dong Yang. A simple proof of monogamy of entanglement. *Physics Letters A*, 360(2):249–250, 2006. URL: https://www.sciencedirect.com/science/article/pii/S0375960106012801, arXiv:quant-ph/0604168, doi:10.1016/j.physleta.2006.08.027.

APPENDIX

4.A Proof of Proposition 4.1

In this section, we calculate the smooth-min unextendible entanglement of the maximally entangled state Φ_{AB}^d.

We first note that all extensions of the state Φ_{AB}^d are of the form $\Phi_{AB}^d \otimes \tau_E$ since Φ_{AB}^d is a pure state. Therefore, all states in the set $\mathcal{F}(\Phi_{AB}^d)$ are of the form $\pi_A \otimes \tau_E$, where π_A is the maximally mixed state and $E \cong B$. The unextendible entanglement of Φ_{AB}^d induced by the hypothesis testing relative entropy can be calculated as follows:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) = \inf_{\tau_B \in \mathcal{S}(B)} \frac{1}{2} D_{\min}^{\varepsilon}\left(\Phi_{AB}^d \| \pi_A \otimes \tau_B\right) \tag{4.A.1}$$

$$= \inf_{\tau_B} -\frac{1}{2} \log_2 \inf_{0 \leq \Lambda \leq I} \left\{ \operatorname{Tr}[\Lambda_{AB}(\pi_A \otimes \tau_B)] : \operatorname{Tr}\left[\Lambda_{AB}\Phi_{AB}^d\right] \geq 1 - \varepsilon \right\}. \tag{4.A.2}$$

Choosing $\Lambda_{AB} = (1-\varepsilon)\Phi_{AB}^d$, we find that

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^d\right) \geq \inf_{\tau_B} -\frac{1}{2} \log_2 \left((1-\varepsilon) \operatorname{Tr}\left[\Phi_{AB}^d (\pi_A \otimes \tau_B)\right] \right) \tag{4.A.3}$$

$$= \inf_{\tau_B} -\frac{1}{2} \log_2 \left(\frac{1-\varepsilon}{d} \operatorname{Tr}\left[\Phi_{AB}^d (I_A \otimes \tau_B)\right] \right) \tag{4.A.4}$$

$$= \inf_{\tau_B} -\frac{1}{2} \log_2 \left(\frac{1-\varepsilon}{d} \operatorname{Tr}[\pi_B \tau_B] \right) \tag{4.A.5}$$

$$= \inf_{\tau_B} -\frac{1}{2} \log_2 \left(\frac{1-\varepsilon}{d^2} \operatorname{Tr}[\tau_B] \right) \tag{4.A.6}$$

$$= -\frac{1}{2} \log_2 \left(\frac{1-\varepsilon}{d^2} \right). \tag{4.A.7}$$

The hypothesis testing relative entropy can also be computed using the following SDP:

$$D_{\min}^{\varepsilon}(\rho_{AB}) = -\log_2 \sup_{\mu \geq 0, Z \geq 0} \{ \mu(1-\varepsilon) - \operatorname{Tr}[Z] : \mu\rho \leq \sigma + Z \}. \tag{4.A.8}$$

The unextendible entanglement of the maximally entangled state induced by the hypothesis testing relative entropy can then be computed as follows:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^{d}\right) = \inf_{\tau_B \in \mathcal{S}(B)} -\frac{1}{2}\log_2 \sup_{\mu\geq 0, Z\geq 0} \left\{\mu(1-\varepsilon) - \mathrm{Tr}[Z] : \mu\Phi_{AB}^{d} \leq \pi_A \otimes \tau_B + Z_{AB}\right\} \tag{4.A.9}$$

Choosing τ_B to be the maximally mixed state, we arrive at the following inequality:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^{d}\right) \leq -\frac{1}{2}\log_2 \sup_{\mu\geq 0, Z\geq 0} \left\{\mu(1-\varepsilon) - \mathrm{Tr}[Z] : \mu\Phi_{AB}^{d} \leq \pi_{AB} + Z_{AB}\right\} \tag{4.A.10}$$

$$= \inf_{\mu\geq 0, Z\geq 0} -\frac{1}{2}\log_2 \left\{\mu(1-\varepsilon) - \mathrm{Tr}[Z] : \mu\Phi_{AB}^{d} \leq \pi_{AB} + Z_{AB}\right\}. \tag{4.A.11}$$

Note that the pair $\left(\mu = 1/d^2, Z = 0\right)$ lies in the feasible set of the aforementioned SDP. Therefore, setting $\mu = 1/d^2$ and $Z = 0$ leads to the following inequality:

$$E_{\min}^{u,\varepsilon}\left(\Phi_{AB}^{d}\right) \leq -\frac{1}{2}\log_2\left(\frac{1-\varepsilon}{d^2}\right) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \tag{4.A.12}$$

Combining (4.A.7) and (4.A.12) concludes the proof.

4.B Proof of Proposition 4.2

In this section we find the range of values that the smooth-min unextendible entanglement of a state can take.

The smooth-min relative entropy between two states is never smaller than $-\log_2(1-\varepsilon)$, which can be seen from the data-processing inequality of the smooth-min relative entropy as follows:

$$D_{\min}^{\varepsilon}(\rho\|\sigma) \geq D_{\min}^{\varepsilon}(\mathcal{R}^{\pi}(\rho)\,\|\mathcal{R}^{\pi}(\sigma)) \tag{4.B.1}$$

$$= D_{\min}^{\varepsilon}(\pi\|\pi) \tag{4.B.2}$$

$$= -\log_2 \inf_{0\leq\Lambda\leq I} \{\mathrm{Tr}[\Lambda\pi] : \mathrm{Tr}[\Lambda\pi] \geq 1-\varepsilon\} \tag{4.B.3}$$

$$= -\log_2(1-\varepsilon), \tag{4.B.4}$$

where $\mathcal{R}^\pi$ is a channel that traces out the state it acts on and replaces it with the maximally mixed state π. This leads to the following bound on the smooth-min unextendible entanglement of a bipartite state ρ_{AB}:

$$E_{\min}^{u,\varepsilon}(\rho_{AB}) = \inf_{\sigma\in\mathcal{F}(\rho)} \frac{1}{2} D_{\min}^{\varepsilon}(\rho_{AB}\|\sigma_{AB}) \geq -\frac{1}{2}\log_2(1-\varepsilon). \tag{4.B.5}$$

To find an upper bound on $E_{\min}^{u,\varepsilon}(\rho_{AB})$, we invoke (4.5.23). Since the hypothesis testing relative entropy is an example of generalized divergence, (4.5.23) implies the following inequality:

$$E_{\min}^{u,\varepsilon}(\rho_{AB}) \leq E_{\min}^{u,\varepsilon}\left(\Phi_{A_0B_0}^d\right) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), \tag{4.B.6}$$

where $d \coloneqq \min\{\dim(A), \dim(B)\}$. The equality in (4.B.6) follows from Proposition 4.1.

4.C Proof of Equation (4.6.28)

In this appendix, we show that (4.6.27) implies (4.6.28).

Let us analyze the expression on the right-hand side of (4.6.27) in the interval $q \in [0,1]$ and for $k \in \mathbb{N}$. In what follows, we find the inflection points of the expression by setting the derivative equal to zero:

$$0 = \frac{\partial}{\partial q}\left(\sqrt{\frac{q}{k^2}} + \sqrt{(1-q)\left(1-\frac{1}{k^2}\right)}\right)^2 \tag{4.C.1}$$

$$= 2\left(\sqrt{\frac{q}{k^2}} + \sqrt{(1-q)\left(1-\frac{1}{k^2}\right)}\right)\left(\frac{1}{2k\sqrt{q}} - \frac{1}{2\sqrt{1-q}}\sqrt{1-\frac{1}{k^2}}\right). \tag{4.C.2}$$

Solving the above equation for q, we find that

$$\frac{1}{2k\sqrt{q}} = \frac{1}{2\sqrt{1-q}}\sqrt{1-\frac{1}{k^2}} \tag{4.C.3}$$

$$\implies \sqrt{1-q} = \sqrt{q(k^2-1)} \tag{4.C.4}$$

$$\implies 1-q = q(k^2-1) \tag{4.C.5}$$

$$\implies q = \frac{1}{k^2}. \tag{4.C.6}$$

It is easy to verify that the function of q given on the right-hand side of (4.6.27) achieves its maximum value at this inflection point. Therefore, the function is monotonically increasing for $q \in [0, \frac{1}{k^2}]$, and it is monotonically decreasing for $q \in [\frac{1}{k^2}, 1]$. Equivalently, the derivative in (4.C.2) is non-negative for $q \in [0, \frac{1}{k^2}]$, and it is non-positive for $q \in [\frac{1}{k^2}, 1]$.

Now let us find the values of q that satisfy (4.6.27). We can rewrite the inequality in (4.6.27) as follows:

$$1-\varepsilon \leq \frac{q}{k^2} + (1-q)\left(1-\frac{1}{k^2}\right) + 2\sqrt{q(1-q)}\sqrt{\frac{1}{k^2}\left(1-\frac{1}{k^2}\right)}. \tag{4.C.7}$$

Rearranging the terms, we arrive at the following inequality:

$$q\left(1-\frac{2}{k^2}\right) - \varepsilon + \frac{1}{k^2} \leq 2\sqrt{q(1-q)}\sqrt{\frac{1}{k^2}\left(1-\frac{1}{k^2}\right)}. \tag{4.C.8}$$

The right-hand side of the above equation is always non-negative for all $q \in [0,1]$ and $k \in \mathbb{N}$. If the left-hand side of the above inequality is negative, then the above inequality is satisfied. As such, the above inequality is satisfied if the following condition holds:

$$q\left(1-\frac{2}{k^2}\right) - \varepsilon + \frac{1}{k^2} \leq 0 \implies q \leq \frac{\varepsilon - \frac{1}{k^2}}{1-\frac{2}{k^2}} \quad \forall\, k \geq 2. \tag{4.C.9}$$

If $\varepsilon - \frac{1}{k^2} \geq 0$ then the inequality in (4.C.8) is satisfied for all $q \in \left[0, \frac{\varepsilon - k^{-2}}{1-2k^{-2}}\right]$ and $k \geq 2$.

Now let us consider the case where the left-hand side of (4.C.8) is non-negative, which is true for $k \geq 2$ if $\varepsilon \leq \frac{1}{k^2}$ or $q \geq \left(\varepsilon - \frac{1}{k^2}\right) / \left(1 - \frac{2}{k^2}\right)$. We can square both sides to get the

following inequality:

$$\left(q\left(1-\frac{2}{k^2}\right)-\varepsilon+\frac{1}{k^2}\right)^2 \leq \left(2\sqrt{q(1-q)}\sqrt{\frac{1}{k^2}\left(1-\frac{1}{k^2}\right)}\right)^2 \tag{4.C.10}$$

$$= \frac{4}{k^2}\left(1-\frac{1}{k^2}\right)q(1-q). \tag{4.C.11}$$

Setting

$$d \coloneqq 1-\frac{2}{k^2}, \tag{4.C.12}$$

$$e \coloneqq \varepsilon-\frac{1}{k^2}, \tag{4.C.13}$$

$$f \coloneqq \frac{4}{k^2}\left(1-\frac{1}{k^2}\right), \tag{4.C.14}$$

we can rewrite the above inequality as follows:

$$(d\cdot q-e)^2 \leq f\cdot q(1-q) \tag{4.C.15}$$

$$\implies d^2q^2+e^2-2deq \leq fq-fq^2 \tag{4.C.16}$$

$$\implies (d^2+f)q^2-(2de+f)q+e^2 \leq 0. \tag{4.C.17}$$

The above inequality is in the standard form of a quadratic inequality. Let us first find each of the coefficients. The coefficient of q^2 evaluates to the following:

$$d^2+f = \left(1-\frac{2}{k^2}\right)^2+\frac{4}{k^2}\left(1-\frac{1}{k^2}\right) \tag{4.C.18}$$

$$= 1+\frac{4}{k^4}-\frac{4}{k^2}+\frac{4}{k^2}-\frac{4}{k^4} \tag{4.C.19}$$

$$= 1. \tag{4.C.20}$$

The coefficient of q evaluates to the following:

$$-2de-f = -2\left(1-\frac{2}{k^2}\right)\left(\varepsilon-\frac{1}{k^2}\right)-\frac{4}{k^2}\left(1-\frac{1}{k^2}\right) \tag{4.C.21}$$

$$= -2\left(\varepsilon-\frac{1}{k^2}-\frac{2\varepsilon}{k^2}+\frac{2}{k^4}\right)-\frac{4}{k^2}+\frac{4}{k^4} \tag{4.C.22}$$

$$= -2\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right). \tag{4.C.23}$$

Finally, the term independent of q is equal to the following:

$$e^2 = \left(\varepsilon - \frac{1}{k^2}\right)^2 \tag{4.C.24}$$

$$= \varepsilon^2 + \frac{1}{k^4} - \frac{2\varepsilon}{k^2}. \tag{4.C.25}$$

The quadratic inequality in (4.C.11) can now be written as follows:

$$q^2 - 2q\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right) + \varepsilon^2 + \frac{1}{k^4} - \frac{2\varepsilon}{k^2} \leq 0. \tag{4.C.26}$$

The discriminant of the above quadratic expression can be evaluated as follows:

$$(-2de - f)^2 - 4(d^2 + f)e^2$$

$$= 4\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right)^2 - 4\left(\varepsilon^2 + \frac{1}{k^4} - \frac{2\varepsilon}{k^2}\right) \tag{4.C.27}$$

$$= 4\left(\varepsilon^2 + \left(\frac{1-2\varepsilon}{k^2}\right)^2 + 2\varepsilon\left(\frac{1-2\varepsilon}{k^2}\right) - \varepsilon^2 - \frac{1}{k^4} + \frac{2\varepsilon}{k^2}\right) \tag{4.C.28}$$

$$= 4\left(\frac{1+4\varepsilon^2-4\varepsilon}{k^4} - \frac{1}{k^4} + \frac{2\varepsilon}{k^2}(2-2\varepsilon)\right) \tag{4.C.29}$$

$$= 4\left(\frac{4\varepsilon(\varepsilon-1)}{k^4} + \frac{4\varepsilon(1-\varepsilon)}{k^2}\right) \tag{4.C.30}$$

$$= 16\frac{(k^2-1)\varepsilon(1-\varepsilon)}{k^4}. \tag{4.C.31}$$

We can now factor the quadratic expression in (4.C.26) as follows:

$$\left(q - \alpha_{q+}\right)\left(q - \alpha_{q-}\right) \leq 0, \tag{4.C.32}$$

where

$$\alpha_{q\pm} = \frac{1}{2}\left(2\left(\varepsilon + \frac{1-2\varepsilon}{k^2}\right) \pm \frac{\sqrt{16(k^2-1)\varepsilon(1-\varepsilon)}}{k^2}\right) \tag{4.C.33}$$

$$= \varepsilon + \frac{1-2\varepsilon}{k^2} \pm \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2}. \tag{4.C.34}$$

Now we are in a position to identify the range of values that q can take for all $\varepsilon \in [0,1]$ and $k \geq 2$.

- If $\varepsilon \in \left[0, \frac{1}{k^2}\right]$, then

$$\alpha_{q-} \leq q \leq \alpha_{q+}, \tag{4.C.35}$$

  where α_{q-} and α_{q+} are defined in (4.C.34).

- If $\varepsilon \in \left[\frac{1}{k^2}, 1\right]$, then

$$q \in \left[0, \min\left\{\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}}, 1\right\}\right] \cup \left[\alpha_{q-}, \alpha_{q+}\right]. \tag{4.C.36}$$

We can identify the values of ε such that the two intervals in (4.C.36) overlap. Let us first find the values of ε that satisfy the following inequality:

$$\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}} \leq \alpha_{q+} = \varepsilon + \frac{1 - 2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2}. \tag{4.C.37}$$

We can rearrange the terms of the above inequality to get the following inequality:

$$\frac{k^2\varepsilon - 1}{k^2 - 2} - \frac{(k^2-2)\varepsilon + 1}{k^2} \leq \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2} \tag{4.C.38}$$

$$\implies \frac{k^4\varepsilon - k^2 - (k^2-2)^2\varepsilon - k^2 + 2}{k^2(k^2-2)} \leq \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2} \tag{4.C.39}$$

$$\implies \frac{4(k^2-1)\varepsilon + 2(1-k^2)}{k^2-2} \leq 2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)} \tag{4.C.40}$$

$$\implies \frac{(k^2-1)(2\varepsilon-1)}{k^2-2} \leq \sqrt{(k^2-1)\varepsilon(1-\varepsilon)}. \tag{4.C.41}$$

The above inequality is satisfied for all $\varepsilon \in [0, 1/2]$ and $k \geq 2$. Now assuming that $\varepsilon \geq 1/2$ and $k \geq 2$, we can square both sides of the above inequality to get the following inequality:

$$\frac{(k^2-1)(2\varepsilon-1)^2}{(k^2-2)^2} \leq \varepsilon(1-\varepsilon). \tag{4.C.42}$$

Setting $a := (k^2-1)/(k^2-2)^2$, we can rewrite the above inequality as follows:

$$a(2\varepsilon-1)^2 \leq \varepsilon(1-\varepsilon) \tag{4.C.43}$$

$$\implies (4a+1)\varepsilon^2 - (4a+1)\varepsilon + a \leq 0. \tag{4.C.44}$$

Note that a is a positive number, which implies that $4a+1$ is also a positive number. Therefore, the above quadratic inequality can be factored as follows:

$$\left(\varepsilon - \frac{1}{2}\left(1 + \frac{1}{\sqrt{4a+1}}\right)\right)\left(\varepsilon - \frac{1}{2}\left(1 - \frac{1}{\sqrt{4a+1}}\right)\right) \leq 0. \tag{4.C.45}$$

Substituting the value of a, the quantity $\sqrt{4a+1}$ evaluates to the following:

$$\sqrt{4a+1} = \frac{k^2}{k^2-2}. \tag{4.C.46}$$

Therefore, the inequality in (4.C.45) can be written as follows:

$$\left(\varepsilon - \frac{1}{2}\left(1 + \frac{k^2-2}{k^2}\right)\right)\left(\varepsilon - \frac{1}{2}\left(1 - \frac{k^2-2}{k^2}\right)\right) \leq 0 \tag{4.C.47}$$

$$\implies \left(\varepsilon - \left(1 - \frac{1}{k^2}\right)\right)\left(\varepsilon - \frac{1}{k^2}\right) \leq 0. \tag{4.C.48}$$

The above inequality is satisfied only when $\varepsilon \in \left[1/k^2, 1 - 1/k^2\right]$. To get the above inequality we assumed that $\alpha \geq 1/2$. Since $1 - \frac{1}{k^2} \geq \frac{1}{2}$ for all $k \geq 2$ and every $\varepsilon \in [0, 1/2]$ satisfies the inequality in (4.C.37), we conclude that the inequality in (4.C.37) is satisfied if and only if $\varepsilon \in \left[0, 1 - \frac{1}{k^2}\right]$.

Now let us find the values of ε for which the following inequality is satisfied:

$$\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}} \leq \alpha_{q^-} = \varepsilon + \frac{1-2\varepsilon}{k^2} - \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2}. \tag{4.C.49}$$

Following the same steps as above, we arrive at the following inequality:

$$\frac{(k^2-1)(2\varepsilon-1)}{k^2-2} \leq -\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}, \tag{4.C.50}$$

which is similar to (4.C.41). This inequality is not satisfied by any value of $\varepsilon \geq 1/2$. Under the assumption that $\varepsilon \leq 1/2$, we can square both sides of the above inequality to get the following inequality:

$$\frac{(k^2-1)(2\varepsilon-1)^2}{(k^2-2)^2} \geq \varepsilon(1-\varepsilon). \tag{4.C.51}$$

From the solution of (4.C.42), we know that the opposite of this quadratic inequality is satisfied when $\varepsilon \in \left[\frac{1}{k^2}, 1 - \frac{1}{k^2}\right]$. Therefore, the inequality in (4.C.51) is satisfied when $\varepsilon \in \left[0, \frac{1}{k^2}\right] \cup \left[1 - \frac{1}{k^2}, 1\right]$. Recall that we assumed $\varepsilon \in [0, 1/2]$ to arrive at (4.C.51) from (4.C.50). Therefore, for every $k \geq 2$, we conclude that (4.C.49) is satisfied for all $\varepsilon \in \left[0, \frac{1}{k^2}\right]$.

Now we have a clearer picture of the range of values q that satisfy (4.6.27) for some fixed value of $\varepsilon \in [0, 1]$ and integer $k \geq 2$, which is given as follows:

$$q \in \begin{cases} \left[\alpha_{q-}, \alpha_{q+}\right] & \text{if } \varepsilon \in \left[0, \frac{1}{k^2}\right] \\ \left[0, \alpha_{q+}\right] & \text{if } \varepsilon \in \left[\frac{1}{k^2}, 1 - \frac{1}{k^2}\right], \\ \left[0, \min\left\{\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}}, 1\right\}\right] & \text{if } \varepsilon \in \left[1 - \frac{1}{k^2}, 1\right] \end{cases} \tag{4.C.52}$$

where α_{q+} and α_{q-} are defined in (4.C.34). Observe that $\frac{\varepsilon - \frac{1}{k^2}}{1 - \frac{2}{k^2}} \geq 1$ for all $\varepsilon \in \left[1 - \frac{1}{k^2}, 1\right]$. Therefore, we can rewrite the above condition as follows:

$$q \in \begin{cases} \left[\alpha_{q-}, \alpha_{q+}\right] & \text{if } \varepsilon \in \left[0, \frac{1}{k^2}\right] \\ \left[0, \alpha_{q+}\right] & \text{if } \varepsilon \in \left[\frac{1}{k^2}, 1 - \frac{1}{k^2}\right]. \\ [0, 1] & \text{if } \varepsilon \in \left[1 - \frac{1}{k^2}, 1\right] \end{cases} \tag{4.C.53}$$

As such, if $\varepsilon \leq 1 - \frac{1}{k^2}$, then q is bounded from above by the following quantity:

$$q \leq \varepsilon + \frac{1 - 2\varepsilon}{k^2} + \frac{2\sqrt{(k^2 - 1)\varepsilon(1 - \varepsilon)}}{k^2}, \tag{4.C.54}$$

and otherwise, when $\varepsilon > 1 - \frac{1}{k^2}$, we only have the trivial bound $q \leq 1$.

4.D Proof of Theorem 4.2

First let us note that the condition $\varepsilon < J^{\varepsilon}_{\min}(\rho_{AB})$ is only satisfied if $\varepsilon < \frac{1}{2}$. This is because $J^{\varepsilon}_{\min}(\rho_{AB}) \leq 1 - \varepsilon$, as stated in Proposition 4.2. So we restrict to $\varepsilon < \frac{1}{2}$ for the remainder of

the proof.

Let $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ be a one-way LOCC channel that acts on ρ_{AB} to give a state $\sigma_{A'B'A''B''}$ such that $F(\sigma_{A'B'A''B''}, \gamma^k_{A'B'A''B''}) \geq 1-\varepsilon$ for some bipartite private state $\gamma^k_{A'B'A''B''}$. That is,

$$\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}(\rho_{AB}) = \sigma_{A'B'A''B''}. \tag{4.D.1}$$

The smooth-min unextendible entanglement of a bipartite state does not increase under the action of a one-way LOCC channel [WWW24, Theorem 2]. Therefore,

$$\begin{aligned} E^{u,\varepsilon}_{\min}(\rho_{AB}) &\geq E^{u,\varepsilon}_{\min}(\mathcal{L}^{\rightarrow}(\rho_{AB})) && (4.D.2)\\ &= E^{u,\varepsilon}_{\min}(\sigma_{A'B'A''B''})\,. && (4.D.3)\end{aligned}$$

Consequently,

$$J^{\varepsilon}_{\min}(\rho_{AB}) \leq J^{\varepsilon}_{\min}(\sigma_{A'B'A''B''})\,. \tag{4.D.4}$$

Since $\varepsilon < \frac{1}{2}$, we can use Remark 4.3 to state that one cannot distill any secret bits from a state ρ_{AB} with an error tolerance of ε if $J^{\varepsilon}_{\min}(\rho_{AB}) > \varsigma(\varepsilon, 2)$, where ς is defined in (4.6.5).

Let us now consider the case when one-shot, one-way secret-key distillation is possible. Proposition 4.3 implies that the following inequality holds for all $\varepsilon \in \left[0, \frac{1}{2}\right)$:

$$J^{\varepsilon}_{\min}(\rho_{AB}) \leq \varsigma(\varepsilon, k) = \varepsilon + \frac{1-2\varepsilon}{k^2} + \frac{2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}}{k^2} \tag{4.D.5}$$

if $F\left(\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}(\rho_{AB})\,, \gamma^k_{A'B'A''B''}\right) \geq 1-\varepsilon$ for some one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$ and some private state $\gamma^k_{A'B'A''B''}$ with $k \geq 2$. We will use $J^{\varepsilon}_{\min}$ as a shorthand for $J^{\varepsilon}_{\min}(\rho_{AB})$ in the remainder of the proof for convenience. Rearranging the terms in (4.D.5), we arrive at the following inequality:

$$\begin{aligned} k^2(J^{\varepsilon}_{\min} - \varepsilon) &\leq 1 - 2\varepsilon + 2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)} && (4.D.6)\\ \implies (k^2-1)(J^{\varepsilon}_{\min} - \varepsilon) + J^{\varepsilon}_{\min} - \varepsilon &\leq 1 - 2\varepsilon + 2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)} && (4.D.7)\end{aligned}$$

$$\implies (k^2-1)(J^{\varepsilon}_{\min}-\varepsilon)+J^{\varepsilon}_{\min}+\varepsilon-1\leq 2\sqrt{(k^2-1)\varepsilon(1-\varepsilon)}. \tag{4.D.8}$$

The above inequality is always satisfied if the left-hand side is non-positive, that is, if

$$(k^2-1)(J^{\varepsilon}_{\min}-\varepsilon)+J^{\varepsilon}_{\min}+\varepsilon-1\leq 0. \tag{4.D.9}$$

Note that $J^{\varepsilon}_{\min}+\varepsilon-1$ is always non-positive due to (4.5.31). Therefore, if $J^{\varepsilon}_{\min}\leq\varepsilon$, then the above inequality holds for all $k\in\mathbb{N}$. If $J^{\varepsilon}_{\min}>\varepsilon$, then (4.D.9) is satisfied when the following condition holds:

$$k^2-1\leq\frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}. \tag{4.D.10}$$

Consequently, if the inequality in (4.D.10) holds, then the inequality in (4.D.8) also holds for all $J^{\varepsilon}_{\min}\in[0,1-\varepsilon]$.

Now let us assume that $(k^2-1)(J^{\varepsilon}_{\min}-\varepsilon)+J^{\varepsilon}_{\min}+\varepsilon-1>0$. Then we can square both sides of (4.D.8) to get the following inequality:

$$\Big((k^2-1)(J^{\varepsilon}_{\min}-\varepsilon)+J^{\varepsilon}_{\min}+\varepsilon-1\Big)^2\leq 4(k^2-1)\varepsilon(1-\varepsilon). \tag{4.D.11}$$

We write the above inequality as follows:

$$(d\cdot x+e)^2\leq f\cdot x, \tag{4.D.12}$$

where we have made the following assignments:

$$x:=k^2-1, \tag{4.D.13}$$

$$d:=J^{\varepsilon}_{\min}-\varepsilon, \tag{4.D.14}$$

$$e:=J^{\varepsilon}_{\min}+\varepsilon-1, \tag{4.D.15}$$

$$f:=4\varepsilon(1-\varepsilon). \tag{4.D.16}$$

We can write the inequality in (4.D.12) as the following quadratic inequality in x:

$$d^2x^2+e^2+2de\cdot x\leq f\cdot x \tag{4.D.17}$$

$$\implies d^2x^2 + (2de - f)x + e^2 \leq 0. \tag{4.D.18}$$

The coefficient of x^2 evaluates to the following:

$$d^2 = (J^{\varepsilon}_{\min} - \varepsilon)^2. \tag{4.D.19}$$

The coefficient of x evaluates to the following:

$$2de - f = 2(J^{\varepsilon}_{\min} - \varepsilon)(J^{\varepsilon}_{\min} + \varepsilon - 1) - 4\varepsilon(1 - \varepsilon) \tag{4.D.20}$$

$$= -2J^{\varepsilon}_{\min}(1 - J^{\varepsilon}_{\min}) - 2\varepsilon(1 - \varepsilon). \tag{4.D.21}$$

In what follows, we compute the discriminant of the above quadratic expression:

$$(2de - f)^2 - 4d^2e^2 = 4d^2e^2 + f^2 - 4def - 4d^2e^2 \tag{4.D.22}$$

$$= f^2 - 4def \tag{4.D.23}$$

$$= 16\varepsilon^2(1 - \varepsilon)^2 - 16(J^{\varepsilon}_{\min} - \varepsilon)(J^{\varepsilon}_{\min} + \varepsilon - 1)\varepsilon(1 - \varepsilon) \tag{4.D.24}$$

$$= 16\varepsilon(1 - \varepsilon)\left[\varepsilon(1 - \varepsilon) - (J^{\varepsilon}_{\min})^2 + J^{\varepsilon}_{\min} - \varepsilon(1 - \varepsilon)\right] \tag{4.D.25}$$

$$= 16\varepsilon(1 - \varepsilon)J^{\varepsilon}_{\min}(1 - J^{\varepsilon}_{\min}). \tag{4.D.26}$$

Note that the coefficient of x^2, that is $(J^{\varepsilon}_{\min} - \varepsilon)^2$, is always positive since we have assumed that $J^{\varepsilon}_{\min} > \varepsilon$, which allows us to factor the quadratic expression in (4.D.11) as follows:

$$(x - \beta_{x-})\,(x - \beta_{x+}) \leq 0, \tag{4.D.27}$$

where

$$\beta_{x\pm} := \frac{2J^{\varepsilon}_{\min}(1 - J^{\varepsilon}_{\min}) + 2\varepsilon(1 - \varepsilon) \pm 4\sqrt{\varepsilon(1 - \varepsilon)J^{\varepsilon}_{\min}(1 - J^{\varepsilon}_{\min})}}{2(J^{\varepsilon}_{\min} - \varepsilon)^2} \tag{4.D.28}$$

$$= \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1 - J^{\varepsilon}_{\min})} \pm \sqrt{\varepsilon(1 - \varepsilon)}}{J^{\varepsilon}_{\min} - \varepsilon}\right)^2. \tag{4.D.29}$$

The inequality in (4.D.27) is satisfied if and only if $\beta_{x-} \leq x \leq \beta_{x+}$. Combining (4.D.10) and (4.D.27), we conclude that (4.D.8) is satisfied if and only if

$$k^2 - 1 \in \left[0, \frac{1 - \varepsilon - J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min} - \varepsilon}\right] \cup [\beta_{x-}, \beta_{x+}]\,. \tag{4.D.30}$$

Recall that we had assumed $k^2 - 1 > \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$ to arrive at (4.D.11), and the inequality in (4.D.8) holds for all $0 \leq k^2 - 1 \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$. In what follows, we shall show that $\beta_{x-} \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \leq \beta_{x+}$ for all $\varepsilon < J^{\varepsilon}_{\min} \leq 1-\varepsilon$.

First, let us consider the following inequality:

$$\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} \leq \sqrt{\varepsilon(1-\varepsilon)} \tag{4.D.31}$$

$$\iff J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) \leq \varepsilon(1-\varepsilon) \tag{4.D.32}$$

$$\iff (J^{\varepsilon}_{\min})^2 - J^{\varepsilon}_{\min} + \varepsilon(1-\varepsilon) \geq 0. \tag{4.D.33}$$

The above inequality can be factored as follows:

$$(J^{\varepsilon}_{\min} - \varepsilon)\,(J^{\varepsilon}_{\min} - (1-\varepsilon)) \geq 0. \tag{4.D.34}$$

Therefore, the inequality in (4.D.31) is satisfied if and only if $J^{\varepsilon}_{\min} \leq \varepsilon$ or $J^{\varepsilon}_{\min} \geq 1-\varepsilon$, with the inequality being saturated if $J^{\varepsilon}_{\min} = \varepsilon$ or $J^{\varepsilon}_{\min} = 1-\varepsilon$. Thus, we conclude that the following inequality holds for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$:

$$\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} \geq \sqrt{\varepsilon(1-\varepsilon)}. \tag{4.D.35}$$

Now we prove that $\beta_{x-} \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$, provided that $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$. Consider that

$$\beta_{x-} \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \tag{4.D.36}$$

$$\iff \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2 \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \tag{4.D.37}$$

$$\iff \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}\right)^2 \leq (J^{\varepsilon}_{\min}-\varepsilon)\,(1-\varepsilon-J^{\varepsilon}_{\min}) \tag{4.D.38}$$

$$\iff \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}\right)^2 \leq J^{\varepsilon}_{\min} - (J^{\varepsilon}_{\min})^2 - \varepsilon + \varepsilon^2 \tag{4.D.39}$$

$$\iff \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}\right)^2 \leq J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) - \varepsilon(1-\varepsilon) \tag{4.D.40}$$

$$\iff \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)} \leq \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}. \tag{4.D.41}$$

$$\iff 0 \leq 2\sqrt{\varepsilon(1-\varepsilon)}. \tag{4.D.42}$$

To arrive at the penultimate inequality, we have used the fact that

$$\begin{aligned} &J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) - \varepsilon(1-\varepsilon) \\ &\qquad = \left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}\right)\left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}\right). \end{aligned} \tag{4.D.43}$$

Since the last inequality $0 \leq 2\sqrt{\varepsilon(1-\varepsilon)}$ holds trivially for $\varepsilon \in [0,1]$, we conclude that $\beta_{x-} \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$ for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$.

To show that $\beta_{x+} \geq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}$, we consider the following inequality:

$$\beta_{x+} = \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2 \geq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}. \tag{4.D.44}$$

Following the same steps as before, the above inequality can be transformed into the following inequality:

$$\left(\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}\right)^2 \geq J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min}) - \varepsilon(1-\varepsilon) \tag{4.D.45}$$

$$\iff \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)} \geq \sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}, \tag{4.D.46}$$

which holds for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$ and $\varepsilon \in [0,1]$. Hence, we conclude the following:

$$\left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} - \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2 \leq \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon} \tag{4.D.47}$$

$$\leq \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2 \tag{4.D.48}$$

Recall from (4.D.30) that (4.D.8) is satisfied for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$ if and only if $k^2 - 1 \in \left[0, \frac{1-\varepsilon-J^{\varepsilon}_{\min}}{J^{\varepsilon}_{\min}-\varepsilon}\right] \cup [\beta_{x-}, \beta_{x+}]$. The inequalities in (4.D.47) and (4.D.48) further reveal that the inequality in (4.D.8) is satisfied for all $J^{\varepsilon}_{\min} \in (\varepsilon, 1-\varepsilon]$ if and only if the following condition holds:

$$0 \leq k^2 - 1 \leq \left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})} + \sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2. \tag{4.D.49}$$

The quantity $\log_2 k$ is interpreted as the number of secret bits that can be distilled from the state ρ_{AB} using the one-way LOCC channel $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$. Therefore, we rewrite the condition in (4.D.49) as the following upper bound on $\log_2 k$:

$$\log_2 k \leq \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J^{\varepsilon}_{\min}(1-J^{\varepsilon}_{\min})}+\sqrt{\varepsilon(1-\varepsilon)}}{J^{\varepsilon}_{\min}-\varepsilon}\right)^2+1\right] \tag{4.D.50}$$

Since the inequality in (4.D.50) holds for every integer $k \geq 2$, every private state $\gamma^k_{A'B'A''B''}$, and every one-way LOCC channels $\mathcal{L}^{\rightarrow}_{AB\to A'B'A''B''}$, we conclude (4.6.39).

4.E Proof of Lemma 4.3

In this section we show that the following function:

$$f(J,\varepsilon) := \frac{1}{2}\log_2\left[\left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right)^2+1\right] \tag{4.E.1}$$

decreases monotonically with increasing J and increases monotonically with increasing ε for all $\varepsilon \in [0,1]$ and $J \in (\varepsilon, 1-\varepsilon]$.

First, let us analyze the monotonicity of $f(J,\varepsilon)$ in J. The logarithm function is monotonic in its argument. Therefore, we only need to check the monotonicity of the following function:

$$g(J,\varepsilon) := \left(\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right)^2. \tag{4.E.2}$$

Note that the quantity $\frac{\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}$ is non-negative for all $\varepsilon < J \leq 1$ and $0 \leq \varepsilon \leq 1$. Therefore, $g(J,\varepsilon)$ is monotonic in J if $\sqrt{g(J,\varepsilon)}$ is monotonic in J in the given domain.

Let us compute the derivative of $\sqrt{g(J,\varepsilon)}$ with respect to J.

$$\frac{d}{dJ}\sqrt{g(J,\varepsilon)} = \frac{1}{(J-\varepsilon)^2}\left((J-\varepsilon)\left(\frac{1}{2}\cdot\frac{1-2J}{\sqrt{J(1-J)}}\right)-\left(\sqrt{J(1-J)}+\sqrt{\varepsilon(1-\varepsilon)}\right)\right). \tag{4.E.3}$$

Set $h \coloneqq J - \varepsilon$ so that $h \in (0, 1 - 2\varepsilon]$. The first term of the above expression can then be expressed as follows:

$$(J-\varepsilon)\left(\frac{1}{2}\cdot\frac{1-2J}{\sqrt{J(1-J)}}\right) = \frac{h(1-2h-2\varepsilon)}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{4.E.4}$$

$$= \frac{h(2-2h-2\varepsilon)}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} - \frac{h}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{4.E.5}$$

$$= \frac{h\sqrt{1-h-\varepsilon}}{\sqrt{h+\varepsilon}} - \frac{h}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{4.E.6}$$

$$\leq \sqrt{(h+\varepsilon)(1-h-\varepsilon)} - \frac{h}{2\sqrt{(h+\varepsilon)(1-h-\varepsilon)}} \tag{4.E.7}$$

$$= \sqrt{J(1-J)} - \frac{J-\varepsilon}{2\sqrt{J(1-J)}}, \tag{4.E.8}$$

where we have used the fact that $h \leq h + \varepsilon$ to arrive at the inequality. Substituting the above inequality in (4.E.3),

$$\frac{d}{dJ}\sqrt{g(J,\varepsilon)} \leq \frac{1}{(J-\varepsilon)^2}\left(\sqrt{J(1-J)} - \frac{J-\varepsilon}{2\sqrt{J(1-J)}} - \sqrt{J(1-J)} - \sqrt{\varepsilon(1-\varepsilon)}\right) \tag{4.E.9}$$

$$= -\frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{J(1-J)}} + \sqrt{\varepsilon(1-\varepsilon)}\right), \tag{4.E.10}$$

which is negative for all $J \in (\varepsilon, 1-\varepsilon]$ and $\varepsilon \in [0,1]$. Therefore, $\sqrt{g(J,\varepsilon)}$ decreases monotonically with J in the given domain, and consequently, $f(J,\varepsilon)$ decreases monotonically with J in the same domain.

Now let us analyze the monotonicity of $f(J,\varepsilon)$ in ε. Once again, we only need to determine the monotonicity of $\sqrt{g(J,\varepsilon)}$ in ε to determine the monotonicity of $f(J,\varepsilon)$ in ε. Taking the derivative of $\sqrt{g(J,\varepsilon)}$, we arrive at the following equality:

$$\frac{d}{d\varepsilon}\sqrt{g(J,\varepsilon)} = \frac{d}{d\varepsilon}\left(\frac{\sqrt{J(1-J)} + \sqrt{\varepsilon(1-\varepsilon)}}{J-\varepsilon}\right) \tag{4.E.11}$$

$$= \frac{1}{(J-\varepsilon)^2}\left((J-\varepsilon)\left(\frac{1}{2}\cdot\frac{1-2\varepsilon}{\sqrt{\varepsilon(1-\varepsilon)}}\right) + \sqrt{J(1-J)} + \sqrt{\varepsilon(1-\varepsilon)}\right) \tag{4.E.12}$$

$$= \frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{\varepsilon(1-\varepsilon)}} - \frac{\varepsilon(J-\varepsilon)}{\sqrt{\varepsilon(1-\varepsilon)}} + \sqrt{J(1-J)} + \sqrt{\varepsilon(1-\varepsilon)}\right) \tag{4.E.13}$$

$$= \frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{\varepsilon(1-\varepsilon)}} + \frac{\varepsilon(1-\varepsilon)-\varepsilon(J-\varepsilon)}{\sqrt{\varepsilon(1-\varepsilon)}} + \sqrt{J(1-J)}\right) \tag{4.E.14}$$

$$= \frac{1}{(J-\varepsilon)^2}\left(\frac{J-\varepsilon}{2\sqrt{\varepsilon(1-\varepsilon)}} + \frac{\varepsilon(1-J)}{\sqrt{\varepsilon(1-\varepsilon)}} + \sqrt{J(1-J)}\right). \tag{4.E.15}$$

The above expression is strictly positive for all $\varepsilon \in [0,1]$ and all $J \in (\varepsilon, 1-\varepsilon]$. Therefore, $\sqrt{g(J,\varepsilon)}$ is monotonically increasing in ε in the given domain, and consequently, $f(J,\varepsilon)$ is monotonically increasing in ε in the same domain.

4.F Proof of Proposition 4.6

In this section, we show that the smooth-min unextendible entanglement of a channel lies in the following range:

$$-\frac{1}{2}(1-\varepsilon) \leq E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}) \leq \log_2 d - \frac{1}{2}(1-\varepsilon). \tag{4.F.1}$$

The lower bound on the smooth-min unextendible entanglement can be obtained from Proposition 4.2 and Lemma 4.5. For every quantum state ρ_{RA},

$$E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}) \geq E_{\min}^{u,\varepsilon}(\mathcal{N}_{A\to B}(\rho_{RA})) \tag{4.F.2}$$

$$\geq -\frac{1}{2}\log_2(1-\varepsilon)\,, \tag{4.F.3}$$

where the first inequality follows from Lemma 4.5 and the second inequality follows from Proposition 4.2.

To obtain an upper bound on the smooth-min unextendible entanglement of a channel, consider the smooth-min unextendible entanglement of the identity channel. Recall the inequality in (4.6.68). Setting $\rho \to \mathrm{id}_{A\to B}(\rho_{RA})$, $\sigma \to \mathcal{M}_{A\to E}(\rho_{RA})$, and $\alpha \to \infty$, we arrive at the following inequality:

$$D_{\min}^{\varepsilon}(\mathrm{id}_{A\to B}(\rho_{RA})\|\mathcal{M}_{A\to E}(\rho_{RA})) \leq D_{\max}(\mathrm{id}_{A\to B}(\rho_{RA})\|\mathcal{M}_{A\to E}(\rho_{RA})) - \log_2(1-\varepsilon), \tag{4.F.4}$$

where $\mathcal{M}_{A\to E}$ is an arbitrary quantum channel and systems B and E are isomorphic. Since the above inequality holds for every state ρ_{RA}, we can take a supremum over all states and arrive at the following inequality between the smooth-min relative entropy of channels and the max-relative entropy of channels:

$$D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\|\mathcal{M}_{A\to E}) \leq D_{\max}(\mathrm{id}_{A\to B}\|\mathcal{M}_{A\to E}) - \log_2(1-\varepsilon). \tag{4.F.5}$$

In [DFW+18, WBHK20], it was shown that the following equality holds for the max-relative entropy of channels:

$$D_{\max}(\mathcal{N}_{A\to B}\|\mathcal{M}_{A\to B}) = D_{\max}\left(\mathcal{N}_{A\to B}\left(\Phi^d_{RA}\right)\middle\|\mathcal{M}_{A\to B}\left(\Phi^d_{RA}\right)\right), \tag{4.F.6}$$

where d is the dimension of the input system of the channel and Φ^d_{RA} is the maximally entangled state with Schmidt rank d. Therefore, we can rewrite (4.F.5) as follows:

$$D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\|\mathcal{M}_{A\to E}) \leq D_{\max}\left(\Phi^d_{RB}\middle\|\mathcal{M}_{A\to E}\left(\Phi^d_{RA}\right)\right) - \log_2(1-\varepsilon). \tag{4.F.7}$$

Any channel that lies in the set $\mathcal{F}(\mathrm{id}_{A\to B})$ is a trace and replace channel; that is, it is of the following form:

$$\mathcal{M}_{A\to E}(\cdot) = \mathrm{Tr}[\cdot]\,\sigma_E, \tag{4.F.8}$$

where σ_E is a quantum state. Therefore, the inequality in (4.F.7) leads to the following inequality:

$$\inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B}\|\mathcal{M}_{A\to E}) \leq \inf_{\mathcal{M}\in\mathcal{F}(\mathcal{N})} D_{\max}\left(\Phi^d_{RB}\middle\|\mathcal{M}_{A\to E}\left(\Phi^d_{RA}\right)\right) - \log_2(1-\varepsilon) \tag{4.F.9}$$

$$= \inf_{\sigma_E\in\mathcal{S}(E)} D_{\max}\left(\Phi^d_{RB}\middle\|\pi_R\otimes\sigma_E\right) - \log_2(1-\varepsilon), \tag{4.F.10}$$

where π_R is the maximally mixed state. Moreover, an arbitrary extension of the maximally entangled state is of the following form $\Phi^d_{AB}\otimes\tau_E$ because the maximally entangled state is a pure state. As such, every state in the set $\mathcal{F}\left(\Phi^d_{RB}\right)$ can be written as $\pi_R\otimes\tau_E$ for some

$\tau_E \in \mathcal{S}(E)$. Therefore, the max-unextendible entanglement of the maximally entangled state can be written as follows:

$$E^u_{\max}\left(\Phi^d_{AB}\right) = \inf_{\tau_E \in \mathcal{S}(E)} \frac{1}{2} D_{\max}\left(\Phi^d_{RB} \middle\| \pi_R \otimes \tau_E\right) \tag{4.F.11}$$

$$\geq \frac{1}{2} D^{\varepsilon}_{\min}(\mathrm{id}_{A\to B} \| \mathcal{M}_{A\to E}) + \frac{1}{2}\log_2(1-\varepsilon) \tag{4.F.12}$$

$$= E^{u,\varepsilon}_{\min}(\mathrm{id}_{A\to B}) + \frac{1}{2}\log_2(1-\varepsilon), \tag{4.F.13}$$

where the first inequality follows from (4.F.10) and the last equality follows from the definition of smooth-min unextendible entanglement of channels.

The max-unextendible entanglement of a maximally entangled state with Schmidt rank d is equal to $\log_2 d$ as shown in [WWW24, Proposition 11]. Therefore,

$$E^{u,\varepsilon}_{\min}(\mathrm{id}_{A\to B}) \leq \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \tag{4.F.14}$$

The converse of the above inequality is also true as Lemma 4.5 implies the following inequality:

$$E^{\varepsilon,u}_{\min}(\mathrm{id}_{A\to B}) \geq E^{\varepsilon,u}_{\min}\left(\mathrm{id}_{A\to B}\left(\Phi^d_{AB}\right)\right) \tag{4.F.15}$$

$$= E^{\varepsilon,u}_{\min}\left(\Phi^d_{AB}\right) \tag{4.F.16}$$

$$= \log_2 d - \frac{1}{2}\log_2(1-\varepsilon), \tag{4.F.17}$$

where the final equality follows from Proposition 4.1. Therefore,

$$E^{u,\varepsilon}_{\min}(\mathrm{id}_{A\to B}) = \log_2 d - \frac{1}{2}\log_2(1-\varepsilon). \tag{4.F.18}$$

Since

$$E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) \leq \min\left\{E^{u,\varepsilon}_{\min}(\mathrm{id}_{A\to C}), E^{u,\varepsilon}_{\min}(\mathrm{id}_{B\to D})\right\}, \tag{4.F.19}$$

where $\dim(A) = \dim(C)$ and $\dim(B) = \dim(D)$, we conclude the second inequality in the statement of the proposition.

4.G Proof of Proposition 4.7

In this section we derive an expression for the α-geometric unextendible entanglement of the d-dimensional erasure channel, for $\alpha \in (0,1) \cup (1,2]$. An upper bound on the α-geometric unextendible entanglement of the d-dimensional erasure channel was obtained in [SW24b, Appendix J]. Here we show that the inequality stated in [SW24b] is, in fact, an equality.

Lemma 4.5 implies the following inequality:

$$\mathbf{E}^u\Big(\mathcal{E}^p_{A\to B}\Big(\Phi^d_{RA}\Big)\Big) = \mathbf{E}^u\Big((1-p)\,\Phi^d_{AB} + p\frac{I_A}{d}\otimes|e\rangle\langle e|_B\Big) \leq \mathbf{E}^u\Big(\mathcal{E}^p_{A\to B}\Big), \tag{4.G.1}$$

where Φ^d_{RA} is the maximally entangled state of Schmidt rank $d \in \mathbb{N}$, $|e\rangle$ is the erasure symbol, and $\mathcal{E}^p_{A\to B}$ is a d-dimensional erasure channel with erasure probability $p \in [0,1]$. The bipartite state obtained after sending one share of a maximally entangled state through an erasure channel is called an erased state, which we denote as follows:

$$\eta^p_{AB} \coloneqq (1-p)\,\Phi^d_{AB} + p\frac{I_A}{d}\otimes|e\rangle\langle e|_B. \tag{4.G.2}$$

In what follows, we will obtain an analytical expression for the α-geometric unextendible entanglement of a d-dimensional erased state η^p_{AB} and show that it matches the upper bound on the α-geometric unextendible entanglement of the erasure channel $\mathcal{E}^p_{A\to B}$ obtained in [SW24b, Appendix J]. The inequality in (4.G.1) then simply implies that the α-geometric unextendible entanglement of the erasure channel $\mathcal{E}^p_{A\to B}$ is equal to the α-geometric unextendible entanglement of the erased state η^p_{AB}, thus establishing the equality stated in Proposition 4.7.

Let us analyze the generalized unextendible entanglement of an erased state. We will restrict our discussion to $p < \frac{1}{2}$ since $\widehat{E}^u_\alpha\big(\eta^p_{AB}\big) = 0$ for all $p \geq \frac{1}{2}$.

Lemma 4.6 *For $p \in [0, 1/2)$, let η^p_{AB} be the erased state defined in (4.G.2). The generalized unextendible entanglement of the erased state is equal to the following:*

$$\mathbf{E}^u\left(\eta^p_{AB}\right) = \inf_{b\in[0,1-p]} \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{p,b}_{AE'}\right), \tag{4.G.3}$$

where

$$\omega^{p,b}_{AB} = p\,\Phi^d_{AB} + b\,\frac{I_A \otimes \Pi_B}{d^2} + (1-p-b)\frac{I_A}{d} \otimes |e\rangle\langle e|_B \tag{4.G.4}$$

and

$$\Pi := |0\rangle\langle 0| + \cdots + |d-1\rangle\langle d-1|. \tag{4.G.5}$$

Proof: Let $\eta^p_{AB} := (1-p)\,\Phi^d_{AB} + p\frac{I_A}{d} \otimes |e\rangle\langle e|_B$ be an erased state. Consider the following purification of η^p_{AB}:

$$|\psi^\eta\rangle_{ABE} := \sqrt{1-p}|\Phi^d\rangle_{AB} \otimes |e\rangle_E + \sqrt{p}|\Phi^d\rangle_{AE} \otimes |e\rangle_B, \tag{4.G.6}$$

where systems B and E are isomorphic to each other. For clarity, we define the following projector:

$$\Pi := |0\rangle\langle 0| + \cdots |d-1\rangle\langle d-1|, \tag{4.G.7}$$

which is the projector onto the subspace orthogonal to $|e\rangle\langle e|$. The maximally mixed state of a d-dimensional system is defined as $\pi := \frac{\Pi}{d}$. Since system A does not have any component of the erasure symbol, $I_A = \Pi_A$.

Using the correspondence between a purification and an extension of a state established in [CW04], we can write an arbitrary extension of the erased state as $\mathcal{N}_{E\to E'}\left(\psi^\eta_{ABE}\right)$. Therefore, any state $\sigma_{AE'} \in \mathcal{F}(\eta^p_{AB})$ can be written as follows:

$$\sigma_{AE'} = \mathrm{Tr}_B\left[\mathcal{N}_{E\to E'}\left(\psi^\eta_{ABE}\right)\right] \tag{4.G.8}$$

$$= \mathcal{N}_{E\to E'}\left(\mathrm{Tr}_B\left[\psi^\eta_{ABE}\right]\right) \tag{4.G.9}$$

$$= \mathcal{N}_{E\to E'}\Big((1-p)\pi_A \otimes |e\rangle\langle e|_E + p\,\Phi^d_{AE}\Big) \tag{4.G.10}$$

$$= (1-p)\pi_A \otimes \mathcal{N}_{E\to E'}(|e\rangle\langle e|_E) + p\,\mathcal{N}_{E\to E'}\Big(\Phi^d_{AE}\Big), \tag{4.G.11}$$

where systems B, E, and E' are all isomorphic to each other.

Let us consider the following partially dephasing channel:

$$\Delta_{E'}(\cdot) = \Pi_{E'}(\cdot)\,\Pi_{E'} + |e\rangle\langle e|_{E'}(\cdot)\,|e\rangle\langle e|_{E'}. \tag{4.G.12}$$

Applying this dephasing channel on $\sigma_{AE'}$ leads to a state of the following form:

$$\Delta_{E'}(\sigma_{AE'}) = (1-x)\rho_{AE'} + x\pi_A \otimes |e\rangle\langle e|_{E'}, \tag{4.G.13}$$

where $x \in [0,1]$ and $\rho_{AE'}$ is a quantum state such that $\rho_{AE'}|e\rangle_{E'} = 0$.

Let U_A be an arbitrary unitary operator acting on the Hilbert space of system A. The corresponding operator acting on the Hilbert space of system E' has the following property:

$$U^\dagger_{E'} U_{E'} = U_{E'} U^\dagger_{E'} = \Pi_{E'}. \tag{4.G.14}$$

We can promote $U_{E'}$ to a unitary operator on the Hilbert space of system E' as follows:

$$V^U_{E'} = U_{E'} + |e\rangle\langle e|_{E'}. \tag{4.G.15}$$

Note that

$$V^U_{E'}\rho_{AE'}\left(V^U_{E'}\right)^\dagger = U_{E'}\rho_{AE'}U^\dagger_{E'}, \tag{4.G.16}$$

and

$$V^U_{E'}|e\rangle\langle e|_{E'}\left(V^U_{E'}\right)^\dagger = |e\rangle\langle e|_{E'}. \tag{4.G.17}$$

Now consider the following twirling channel:

$$\mathcal{T}_{AE'} := \int dU \left(\overline{U}_A \otimes V^U_{E'}\right)(\cdot)\left(\overline{U}_A \otimes V^U_{E'}\right)^\dagger, \tag{4.G.18}$$

which can be implemented by local operations and common randomness (LOCR). The action of this twirling channel on the dephased state in (4.G.13) results in the following state:

$$\mathcal{T}_{AE'} \circ \Delta_{E'}(\sigma_{AE'}) = (1-x)\mathcal{T}_{AE'}(\rho_{AE'}) + x \int dU U_A \pi_A U_A^\dagger \otimes |e\rangle\langle e|_{E'} \tag{4.G.19}$$

$$= (1-x) \int dU \left(\overline{\mathcal{U}}_A \otimes \mathcal{U}_{E'}\right)(\rho_{AE'}) + x\pi_A \otimes |e\rangle\langle e|_{E'} \tag{4.G.20}$$

$$= q\Phi^d_{AE'} + (1-q-x)\frac{\Pi_A \otimes \Pi_{E'} - \Phi^d_{AE'}}{d^2-1} + x\pi_A \otimes |e\rangle\langle e|_{E'}, \tag{4.G.21}$$

where $q \coloneqq (1-x)\operatorname{Tr}\left[\rho_{AE'}\Phi^d_{AE'}\right]$. In the above, the second equality follows from (4.G.16), and the final equality is a consequence of the following equality [HH99]:

$$\int dU \left(\overline{\mathcal{U}}_A \otimes \mathcal{U}_{E'}\right)(\tau_{AE'}) = \operatorname{Tr}\left[\tau_{AE'}\Phi^d_{AE'}\right]\Phi^d_{AE'} + \operatorname{Tr}\left[\tau_{AE'}\left(\Pi_A \otimes \Pi_{E'} - \Phi^d_{AE'}\right)\right]\frac{\Pi_A \otimes \Pi_{E'} - \Phi^d_{AE'}}{d^2-1}, \tag{4.G.22}$$

which holds for every quantum state $\tau_{AE'}$. We can rewrite (4.G.21) as follows:

$$\omega^{a,b}_{AE'} \coloneqq \mathcal{T}_{AE'} \circ \Delta_{E'}(\sigma_{AE'}) = a\,\Phi^d_{AE'} + b\,\pi_{AE'} + (1-a-b)\pi_A \otimes |e\rangle\langle e|_{E'}, \tag{4.G.23}$$

where $a = q - \frac{1-q-x}{d^2-1}$ and $b = \frac{(1-q-x)d^2}{d^2-1}$.

The generalized unextendible entanglement of the erased state can now be written as follows:

$$\mathbf{E}^u\left(\eta^p_{AB}\right) = \inf_{\sigma \in \mathcal{F}(\eta^p)} \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\sigma_{AE'}\right) \tag{4.G.24}$$

$$\geq \inf_{\sigma \in \mathcal{F}(\eta^p)} \frac{1}{2}\mathbf{D}\left(\mathcal{T}_{AB} \circ \Delta_B\left(\eta^p_{AB}\right)\middle\|\mathcal{T}_{AE'} \circ \Delta_{E'}(\sigma_{AE'})\right) \tag{4.G.25}$$

$$= \inf_{\sigma \in \mathcal{F}(\eta^p)} \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\mathcal{T}_{AE'} \circ \Delta_{E'}(\sigma_{AE'})\right), \tag{4.G.26}$$

where the inequality follows from the data-processing inequality of the generalized divergence and the final equality follows from the fact that the erased state is invariant under the action of the dephasing channel Δ_B as well as the twirling channel $\mathcal{T}_{AB}$. The

inequality in (4.G.26) implies that for every state $\sigma_{AE'} \in \mathcal{F}\left(\eta^p_{AB}\right)$ there exists a state $\omega^{a,b}_{AE'}$, defined in (4.G.23), such that

$$\frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\sigma_{AE'}\right) \geq \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{a,b}_{AE'}\right). \tag{4.G.27}$$

Therefore, it suffices to restrict the infimum in (4.G.24) to the following optimization:

$$\mathbf{E}^u\left(\eta^p_{AB}\right) = \inf_{a\in\mathcal{A},b\in\mathcal{B}} \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{a,b}_{AE'}\right), \tag{4.G.28}$$

where sets $\mathcal{A}$ and $\mathcal{B}$ correspond to the sets of parameters a and b such that $\omega^{a,b}_{AE'} \in \mathcal{F}\left(\eta^p_{AB}\right)$.

Now let us find the range of values that a and b can take such that $\omega^{a,b}_{AE'}$, defined in (4.G.23), lies in the set $\mathcal{F}\left(\eta^p_{AB}\right)$. Note that

$$\omega^{a,b}_{AE'} = \mathcal{T}_{AE'} \circ \Delta_{E'} \circ \mathcal{N}_{E\to E'}\left(p\,\Phi^d_{AE} + (1-p)\pi_A \otimes |e\rangle\langle e|_E\right). \tag{4.G.29}$$

For every $\mathcal{N}_{E\to E'}$, the channel $\mathcal{T}_{AE'} \circ \Delta_{E'} \circ \mathcal{N}_{E\to E'}$ acts on $\pi_A \otimes |e\rangle\langle e|_E$ and Φ^d_{AE} as follows:

$$\mathcal{T}_{AE'} \circ \Delta_{E'} \circ \mathcal{N}_{E\to E'}(\pi_A \otimes |e\rangle\langle e|_E) = y\pi_{AE'} + (1-y)\pi_A \otimes |e\rangle\langle e|_{E'}, \tag{4.G.30}$$

$$\mathcal{T}_{AE'} \circ \Delta_{E'} \circ \mathcal{N}_{E\to E'}\left(\Phi^d_{AE}\right) = y'\Phi^d_{AE'} + y''\pi_{AE'} + (1-y'-y'')\pi_A \otimes |e\rangle\langle e|_{E'}, \tag{4.G.31}$$

where $y \in [0,1]$, $y' \in [0,1]$ and $y'' \in [0, 1-y']$. The state $\omega^{a,b}_{AE'}$ can hence be written as follows:

$$\begin{aligned}\omega^{a,b}_{AE'} = py'\,\Phi^d_{AE} + (y(1-p) + py'')\pi_{AE'} \\ + ((1-y)(1-p) + p(1-y'-y''))\pi_A \otimes |e\rangle\langle e|_{E'},\end{aligned} \tag{4.G.32}$$

for some $y \in [0,1]$, $y' \in [0,1]$ and $y'' \in [0, 1-y']$. Comparing with (4.G.23), it is clear that $a \leq p$. Therefore, if $\omega^{a,b}_{AE'} \in \mathcal{F}\left(\eta^p_{AB}\right)$, then a must be less than or equal to p.

Now we will show that $\omega^{a,b}_{AE'} \in \mathcal{F}\left(\eta^p_{AB}\right)$ for all $a \in [0,p]$ and $b \in [0, 1-a]$. Consider the following extension of the state $\omega^{a,b}_{AE'}$:

$$\omega^{a,b,c,g}_{ABE'} = \left(a\,\Phi^d_{AE'} + c\,\pi_{AE'}\right) \otimes |e\rangle\langle e|_B + \left(g\,\Phi^d_{AB} + f\,\pi_{AB}\right) \otimes |e\rangle\langle e|_{E'} + (b-c)\Phi^d_{AB} \otimes \pi_{E'}, \tag{4.G.33}$$

where $g+f = 1-a-b$ and $a, b \geq 0$ follow from (4.G.23) and $c, g, f \geq 0$ and $c \leq b$ ensure that $\omega^{a,b,c,g}_{ABE'}$ is positive semi-definite. It can be easily verified that $\mathrm{Tr}_B\left[\omega^{a,b,c,g}_{ABE'}\right] = \omega^{a,b}_{AE'}$. Moreover, if $a + c = p$ and $f = 0$, then $\mathrm{Tr}_{E'}\left[\omega^{a,b,c,g}_{ABE'}\right] = \eta^p_{AB}$ (and also $g + b - c = 1 - p$ as a consequence). Therefore, for all $a \in [0, p]$, there exists $b \in [0, 1-a]$ such that $\omega^{a,b}_{AE'} \in \mathcal{F}\left(\eta^p_{AB}\right)$. As such, $\omega^{a,b}_{AE'} \in \mathcal{F}\left(\eta^p_{AB}\right)$ if and only if $a \in [0, p]$ and $b \in [0, 1-a]$. Invoking (4.G.28), we can write the generalized unextendible entanglement of an erased state η^p_{AB} as follows:

$$\mathbf{E}^u\left(\eta^p_{AB}\right) = \inf_{\substack{a\in[0,p],\\ b\in[0,1-a]}} \frac{1}{2}\mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{a,b}_{AE'}\right). \tag{4.G.34}$$

Consider the following channel:

$$\mathcal{R}^s_{AE'}(\cdot) = |e\rangle\langle e|_{E'}(\cdot)\,|e\rangle\langle e|_{E'} + (1-s)\,\mathrm{Tr}[\Pi_{E'}(\cdot)\,\Pi_{E'}]\,\Phi^d_{AE'} + s\ \mathrm{id}_{AE'}(\Pi_{E'}(\cdot)\,\Pi_{E'}), \tag{4.G.35}$$

where $s \in [0, 1]$. The channel $\mathcal{R}^s_{AE'}$ can be realized by applying the POVM $\{\Pi_{E'}, |e\rangle\langle e|_{E'}\}$ on the state of system E'. If the outcome corresponding to the POVM element $\Pi_{E'}$ occurs, then the state is replaced by the maximally entangled state $\Phi^d_{AE'}$ with probability $1 - s$ and otherwise, with probability s, the identity channel is applied. The erased state $\eta^p_{AE'}$ is invariant under the action of the channel $\mathcal{R}^s_{AE'}$ for all $s \in [0, 1]$. The channel $\mathcal{R}^s_{AE'}$ acts on $\omega^{a,b}_{AE'}$ as follows:

$$\mathcal{R}^s_{AE'}\left(\omega^{a,b}_{AE'}\right) = ((1-s)b + a)\Phi^d_{AE'} + sb\,\pi_{AE'} + (1-a-b)\pi_A \otimes |e\rangle\langle e|_{E'} \tag{4.G.36}$$

$$= \omega^{a+(1-s)b,sb}_{AE'}. \tag{4.G.37}$$

Fix $s = (a + b - p)/b$. The data-processing inequality of the generalized divergence yields the following inequality:

$$\mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{a,b}_{AE'}\right) \geq \mathbf{D}\left(\mathcal{R}^s_{AB}\left(\eta^p_{AB}\right)\middle\|\mathcal{R}^s_{AE'}\left(\omega^{a,b}_{AE'}\right)\right) \tag{4.G.38}$$

$$= \mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{a+(1-s)b,sb}_{AE'}\right) \tag{4.G.39}$$

$$= \mathbf{D}\left(\eta^p_{AB}\middle\|\omega^{p,a+b-p}_{AE'}\right). \tag{4.G.40}$$

If $\omega_{AE'}^{a,b} \in \mathcal{F}\left(\eta_{AB}^{p}\right)$, then $\omega_{AE'}^{p,a+b-p}$ also lies in set $\mathcal{F}\left(\eta_{AB}^{p}\right)$. Therefore, the bivariate infimum in (4.G.34) can be restricted to a single variable infimum as follows:

$$\mathbf{E}^{u}\left(\eta_{AB}^{p}\right) = \inf_{b\in[0,1-p]} \frac{1}{2}\mathbf{D}\left(\eta_{AB}^{p}\middle\|\omega_{AE'}^{p,b}\right). \tag{4.G.41}$$

This concludes the proof. □

Lemma 4.6 allows us to obtain an analytical expression for the α-geometric unextendible entanglement of the erased state, which we present in Proposition 4.8 stated below.

Proposition 4.8 *For all $\alpha \in (0,1)\cup(1,2]$, the α-geometric unextendible entanglement of a d-dimensional erased state η_{AB}^{p}, defined in Lemma 4.6, evaluates to the following:*

$$\widehat{E}_{\alpha}^{u}\left(\eta_{AB}^{p}\right) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(\left(p+\frac{b_{\text{opt}}}{d^2}\right)^{1-\alpha}(1-p)^{\alpha} + (1-p-b_{\text{opt}})^{1-\alpha}p^{\alpha}\right) \tag{4.G.42}$$

for all $p \in \left(0, \frac{1}{d^{1/\alpha}+1}\right]$, where

$$b_{\text{opt}} := \frac{d^2\left((1-p)^2 - p^2 d^{2/\alpha}\right)}{pd^{2/\alpha} + (1-p)d^2}. \tag{4.G.43}$$

For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}_{\alpha}^{u}\left(\eta_{AB}^{p}\right) = \frac{1}{2}\cdot\frac{1}{\alpha-1}\log_2\left(p^{1-\alpha}(1-p)^{\alpha} + (1-p)^{1-\alpha}p^{\alpha}\right). \tag{4.G.44}$$

Proof: The α-geometric unextendible entanglement of the erased state can be computed using Lemma 4.6 as follows:

$$\widehat{E}_{\alpha}^{u}\left(\eta_{AB}^{p}\right) = \inf_{b\in[0,1-p]} \frac{1}{2}\widehat{D}_{\alpha}\left(\eta_{AB}^{p}\middle\|\omega_{AB}^{p,b}\right), \tag{4.G.45}$$

where $\omega_{AB}^{p,b}$ is defined in (4.G.4) and $\alpha \in (0,1)\cup(1,2]$. Recall the definition of the α-geometric Rényi relative entropy given in (4.7.29). The α-geometric Rényi relative entropy

of η_{AB}^p with respect to $\omega_{AB}^{p,b}$ can be computed as follows:

$$\widehat{D}_\alpha\left(\eta_{AB}^p \middle\| \omega_{AB}^{p,b}\right) = \frac{1}{\alpha - 1} \log_2\left(\left(p + \frac{b}{d^2}\right)^{1-\alpha} (1-p)^\alpha + (1-p-b)^{1-\alpha} p^\alpha\right). \tag{4.G.46}$$

The above expression is minimized for

$$b = b_{\text{opt}} := \frac{d^2\left((1-p)^2 - p^2 d^{2/\alpha}\right)}{p d^{2/\alpha} + (1-p)d^2}. \tag{4.G.47}$$

Let us now find the range of p such that $b_{\text{opt}} \in [0, 1-p]$. Consider the following expression:

$$1 - p - b_{\text{opt}} = \frac{p d^{2/\alpha}(1 - p + p d^2)}{p d^{2/\alpha} + (1-p)d^2}. \tag{4.G.48}$$

The above expression is greater than or equal to zero for all $p \in [0,1]$. Therefore, $b_{\text{opt}} \leq 1-p$ for all $p \in [0,1]$. Moreover, $b_{\text{opt}} \geq 0$ if and only if $0 \leq (1-p)^2 - p^2 d^{2/\alpha}$, which holds for all $p \in \left[0, \frac{1}{d^{1/\alpha}+1}\right)$. If $b_{\text{opt}} \leq 0$, the value of $b \in [0, 1-p]$ that minimizes the expression in (4.G.46) is $b = 0$. Therefore, for all $\alpha \in (0,1) \cup (1,2]$, the α-geometric unextendible entanglement of a d-dimensional erased state η_{AB}^p evaluates to the following:

$$\widehat{E}_\alpha^u\left(\eta_{AB}^p\right) = \frac{1}{2} \cdot \frac{1}{\alpha - 1} \log_2\left(\left(p + \frac{b_{\text{opt}}}{d^2}\right)^{1-\alpha} (1-p)^\alpha + (1-p-b_{\text{opt}})^{1-\alpha} p^\alpha\right) \tag{4.G.49}$$

for all $p \in \left(0, \frac{1}{d^{1/\alpha}+1}\right]$, where b_{opt} is defined in (4.G.47). For all $p \in \left(\frac{1}{d^{1/\alpha}+1}, \frac{1}{2}\right]$,

$$\widehat{E}_\alpha^u\left(\eta_{AB}^p\right) = \frac{1}{2} \cdot \frac{1}{\alpha - 1} \log_2\left(p^{1-\alpha}(1-p)^\alpha + (1-p)^{1-\alpha} p^\alpha\right). \tag{4.G.50}$$

This concludes the proof. □

Proof: [Proof of Proposition 4.7] The α-geometric unextendible entanglement of the erased state serves as a lower bound on the α-geometric unextendible entanglement of the erasure channel, as is evident from (4.G.1). The expression for the α-geometric unextendible entanglement of the erased state η_{AB}^p derived in Proposition 4.8 was found to

be an upper bound on the α-geometric unextendible entanglement of a d-dimensional erasure channel with erasure probability p. We give a brief outline of the proof here.

Consider a quantum channel $\mathcal{P}^{b^*}_{A\to BE}$ with the following Choi operator:

$$\Gamma^{\mathcal{P},b^*}_{ABE} = pd\ \Phi^d_{AE} \otimes |e\rangle\langle e|_B + (1-p-b^*)\, d\ \Phi^d_{AB} \otimes |e\rangle\langle e|_E + b^* d\ \Phi^d_{AB} \otimes \pi_E. \tag{4.G.51}$$

The two relevant marginals of this Choi operator are as follows:

$$\Gamma^{\mathcal{E}}_{AB} = d\Big((1-p)\Phi^d_{AB} + p\ \pi_A \otimes |e\rangle\langle e|_B\Big), \tag{4.G.52}$$

which is the Choi operator of a d-dimensional erasure channel with erasure probability p, and

$$\Gamma^{\mathcal{M},b^*}_{AE} = d\Big(p\ \Phi^d_{AE} + (1-p-b^*)\pi_A \otimes |e\rangle\langle e|_E + b^*\pi_{AE}\Big). \tag{4.G.53}$$

The Choi operator $\Gamma^{\mathcal{M},b^*}_{AE}$ corresponds to a channel $\mathcal{M}^{b^*}_{A\to E}$ that lies in the set $\mathcal{F}\left(\mathcal{E}^p_{A\to B}\right)$ if $b^* \in [0, 1-p]$, where $\mathcal{E}^p_{A\to B}$ is a d-dimensional erasure channel with erasure probability p. By definition,

$$\widehat{E}^u_\alpha\left(\mathcal{E}^p_{A\to B}\right) \leq \frac{1}{2}\widehat{D}_\alpha\left(\mathcal{E}^p_{A\to B}\middle\|\mathcal{M}^{b^*}_{A\to E}\right) \tag{4.G.54}$$

for all $b^* \in [0, 1-p]$. Choosing $b^* = \min\{0, b_{\text{opt}}\}$, where b_{opt} is defined in (4.G.47), the α-geometric Rényi relative entropy of $\mathcal{E}^p_{A\to B}$ with respect to $\mathcal{M}^{b^*}_{A\to E}$ evaluates to the expression which is equal to the α-geometric unextendible entanglement of the erased state η^p_{AB} derived in Proposition 4.8. Since the α-geometric unextendible entanglement of the erasure channel $\mathcal{E}^p_{A\to B}$ cannot be less than the α-geometric unextendible entanglement of the erased state η^p_{AB}, we conclude that the two quantities are equal. □

4.H Semidefinite programs

In this section we present all the semidefinite programs that were used in this work.

1. **Smooth-min unextendible entanglement of a state:**

$$E^{u,\varepsilon}_{\min}(\rho_{AB}) = -\frac{1}{2}\log_2 \max\left\{\begin{array}{c} \mu(1-\varepsilon) - \mathrm{Tr}[Z_{AB}] : \\ \mu \geq 0, Z_{AB} \geq 0, \omega_{ABE} \geq 0, \\ \mu\rho_{AB} \leq \mathrm{Tr}_B[\omega_{ABE}] + Z_{AB}, \\ \mathrm{Tr}_E[\omega_{ABE}] = \rho_{AB} \end{array}\right\}. \tag{4.H.1}$$

2. **Max-unextendible entanglement of a state:** The semidefinite program for the max-unextendible entanglement of a state was given in [WWW24]. We include it here for completeness.

$$E^{u}_{\max}(\rho_{AB}) = -\frac{1}{2}\log_2 \max\left\{\begin{array}{c} \lambda : \\ \lambda\rho_{AB} \leq \mathrm{Tr}_B[\omega_{ABE}], \\ \omega_{ABE} \geq 0, \\ \mathrm{Tr}_E[\omega_{ABE}] = \rho_{AB} \end{array}\right\}. \tag{4.H.2}$$

3. **Smooth-min unextendible entanglement of a channel:** The smooth-min relative entropy of a channel $\mathcal{N}$ with respect to a channel $\mathcal{M}$ has a semidefinite program, which was given in [WW19b, Proposition 2]. We use it to write the semidefinite program for smooth-min unextendible entanglement of a channel as follows:

$$E^{u,\varepsilon}_{\min}(\mathcal{N}_{A\to B}) = -\frac{1}{2}\log_2 \max\left\{\begin{array}{c} \mu(1-\varepsilon) - \lambda : \\ \lambda \geq 0, \mu \geq 0, Y_{AB} \geq 0, \Gamma^{\mathcal{P}}_{ABE} \geq 0, \\ \mu\Gamma^{\mathcal{N}}_{AB} \leq \mathrm{Tr}_B\left[\Gamma^{\mathcal{P}}_{AB}\right] + Y_{AB} \\ \mathrm{Tr}_B[Y_{AB}] \leq \lambda I_A, \\ \mathrm{Tr}_E\left[\Gamma^{\mathcal{P}}_{ABE}\right] = \Gamma^{\mathcal{N}}_{AB} \end{array}\right\}, \tag{4.H.3}$$

   where $\Gamma^{\mathcal{N}}_{AB}$ is the Choi operator of the channel $\mathcal{N}_{A\to B}$ defined in (4.3.3).

4. **α-geometric unextendible entanglement of a channel:** Fix $\ell \in \mathbb{N}$. The α-geometric unextendible entanglement of a channel $\mathcal{N}_{A\to B}$ for $\alpha = 1 + 2^{-\ell}$ can be computed using

the following semidefinite program:

$$\widehat{E}^{u}_{\alpha}(\mathcal{N}_{A\to B}) = 2^{\ell} \min_{\substack{y\in\mathbb{R},\Gamma^{\mathcal{P}}_{ABE}\geq 0 \\ M_{AE},\{N^{i}_{AE}\}_{i=0}^{\ell},\in\text{Herm}}} \log_2 y, \tag{4.H.4}$$

subject to the constraints,

$$\text{Tr}_E\left[\Gamma^{\mathcal{P}}_{ABE}\right] = \Gamma^{\mathcal{N}}_{AB}, \tag{4.H.5}$$

$$\text{Tr}_E\left[M_{AE}\right] \leq y I_A, \tag{4.H.6}$$

$$\text{Tr}_B\left[\Gamma^{\mathcal{P}}_{ABE}\right] = N^{0}_{AE}, \tag{4.H.7}$$

$$\begin{bmatrix} M_{AE} & \Gamma^{\mathcal{N}}_{AB} \\ \Gamma^{\mathcal{N}}_{AB} & N^{\ell}_{AE} \end{bmatrix} \geq 0, \tag{4.H.8}$$

$$\begin{bmatrix} \Gamma^{\mathcal{N}}_{AE} & N^{i}_{AE} \\ N^{i}_{AE} & N^{i-1}_{AE} \end{bmatrix} \geq 0 \quad \forall i \in \{1,2,\ldots,\ell\}, \tag{4.H.9}$$

where $\Gamma^{\mathcal{N}}_{AB}$ is the Choi operator of the channel $\mathcal{N}_{A\to B}$ and the system E is isomorphic to the system B. To compute the α-geometric unextendible entanglement of the channel for other rational values of α see [FS17, Table 4].

4.I Proof of Proposition 4.4

In this section, we evaluate the smooth-min relative entropy of entanglement of isotropic states.

Consider an arbitrary d-dimensional isotropic state $\zeta^{F,d}_{AB}$. Let $\mathcal{T}_{AB}$ be the twirling channel defined in (4.6.13). Recall from (4.6.14) that this twirling channel transforms an arbitrary quantum state into an isotropic state. Also, an isotropic state is invariant under the

action of $\mathcal{T}_{AB}$. Let σ_{AB} be an arbitrary quantum state. Then the following inequality holds:

$$D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB}\middle\|\sigma_{AB}\right) \geq D^{\varepsilon}_{\min}\left(\mathcal{T}_{AB}\left(\zeta^{F,d}_{AB}\right)\middle\|\mathcal{T}_{AB}(\sigma_{AB})\right) \tag{4.I.1}$$

$$= D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB}\middle\|\zeta^{F',d}_{AB}\right) \tag{4.I.2}$$

for some $F' \in [0,1]$, where we have used the data-processing inequality for smooth-min relative entropy to arrive at the inequality in (4.I.1) and we have used (4.6.14) to arrive at the equality in (4.I.2).

The channel $\mathcal{T}_{AB}$ can be implemented using local operations and common randomness, and hence, $\mathcal{T}_{AB}$ transforms an arbitrary separable state σ_{AB} into a separable isotropic state $\zeta^{F',d}_{AB}$. It is known from [HH99, Section V] that an isotropic state $\zeta^{F',d}_{AB}$ is separable if and only if $F' \leq \frac{1}{d}$. Therefore, for every separable state σ_{AB}, the following inequality holds:

$$D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB}\middle\|\sigma_{AB}\right) \geq D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB}\middle\|\zeta^{F',d}_{AB}\right) \tag{4.I.3}$$

for some $F' \in \left[0, \frac{1}{d}\right]$. Since the above inequality holds for every separable state σ_{AB}, we can evaluate the smooth-min relative entropy of entanglement of an isotropic state by optimizing over separable isotropic states only. That is,

$$E^{\varepsilon}_{R}\left(\zeta^{F,d}_{AB}\right) = \inf_{F' \in \left[0,\frac{1}{d}\right]} D^{\varepsilon}_{\min}\left(\zeta^{F,d}_{AB}\middle\|\zeta^{F',d}_{AB}\right). \tag{4.I.4}$$

Using the definition of $D^{\varepsilon}_{\min}$ from (4.5.25), we can write the smooth-min relative entropy of entanglement of an isotropic state as follows:

$$E^{\varepsilon}_{R}\left(\zeta^{F,d}_{AB}\right) = \inf_{F' \in \left[0,\frac{1}{d}\right]} -\log_2 \inf_{0 \leq \Lambda_{AB} \leq I_{AB}} \left\{ \operatorname{Tr}\left[\Lambda_{AB}\zeta^{F',d}_{AB}\right] : \operatorname{Tr}\left[\Lambda_{AB}\zeta^{F,d}_{AB}\right] \geq 1-\varepsilon \right\}. \tag{4.I.5}$$

If $1-\varepsilon \leq F$, we can choose $\Lambda_{AB} = \frac{1-\varepsilon}{F}\Phi^{d}_{AB}$ to arrive at the following inequality:

$$E^{\varepsilon}_{R}\left(\zeta^{F,d}_{AB}\right) \geq \inf_{F' \in \left[0,\frac{1}{d}\right]} -\log_2\left(\frac{1-\varepsilon}{F}F'\right) \tag{4.I.6}$$

$$= -\log_2\left(\frac{1-\varepsilon}{F}\right) - \sup_{F' \in \left[0, \frac{1}{d}\right]} \log_2 F' \tag{4.I.7}$$

$$= -\log_2\left(\frac{1-\varepsilon}{F}\right) + \log_2 d, \tag{4.I.8}$$

where the final equality follows from the monotonicity of the logarithm function.

If $1 - \varepsilon > F$, we can choose Λ to be the following:

$$\Lambda_{AB} = \Phi^d_{AB} + \frac{1-\varepsilon-F}{1-F}\left(I_{AB} - \Phi^d_{AB}\right), \tag{4.I.9}$$

which is a valid measurement operator with $\operatorname{Tr}\left[\Lambda_{AB}\zeta^{F,d}_{AB}\right] = 1 - \varepsilon$. This choice of Λ yields the following lower bound on the smooth-min relative entropy of entanglement of an isotropic state:

$$E^{\varepsilon}_R\left(\zeta^{F,d}_{AB}\right) \geq \inf_{F' \in \left[0, \frac{1}{d}\right]} -\log_2\left(F' + \frac{1-\varepsilon-F}{1-F}(1-F')\right) \tag{4.I.10}$$

$$= -\log_2 \sup_{F' \in \left[0, \frac{1}{d}\right]} \left\{F'\left(1 - \frac{1-\varepsilon-F}{1-F}\right) + \frac{1-\varepsilon-F}{1-F}\right\} \tag{4.I.11}$$

$$= -\log_2 \sup_{F' \in \left[0, \frac{1}{d}\right]} \left\{(F'-1)\left(\frac{\varepsilon}{1-F}\right) + 1\right\} \tag{4.I.12}$$

$$= -\log_2\left(\left(\frac{1}{d} - 1\right)\left(\frac{\varepsilon}{1-F}\right) + 1\right) \tag{4.I.13}$$

$$= -\log_2\left(1 - \left(1 - \frac{1}{d}\right)\frac{\varepsilon}{1-F}\right). \tag{4.I.14}$$

Combining (4.I.8) and (4.I.14), we arrive at the following lower bound on the smooth-min relative entropy of entanglement of an isotropic state:

$$E^{\varepsilon}_R\left(\zeta^{F,d}_{AB}\right) \geq \begin{cases} -\log_2\left(1 - \left(1 - \frac{1}{d}\right)\frac{\varepsilon}{1-F}\right) & \text{if } 1 - \varepsilon \geq F \\ \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) & \text{otherwise} \end{cases}. \tag{4.I.15}$$

Let us now find an upper bound on the smooth-min relative entropy of entanglement of an isotropic state. Using the SDP formulation of the smooth-min relative entropy

from [WW19a, Eqn. (B2)], we can write the smooth-min relative entropy of entanglement of isotropic states as follows:

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F,d}\right) = \inf_{F' \in \left[0, \frac{1}{d}\right]} - \log_2 \sup_{\mu \geq 0, X_{AB} \geq 0} \left\{\mu(1-\varepsilon) - \mathrm{Tr}[X_{AB}] : \mu \zeta_{AB}^{F,d} \leq \zeta_{AB}^{F',d} + X_{AB}\right\} \tag{4.I.16}$$

$$= - \log_2 \sup_{\substack{F' \in \left[0, \frac{1}{d}\right], \\ \mu \geq 0, X_{AB} \geq 0}} \left\{\mu(1-\varepsilon) - \mathrm{Tr}[X_{AB}] : \mu \zeta_{AB}^{F,d} \leq \zeta_{AB}^{F',d} + X_{AB}\right\}, \tag{4.I.17}$$

where the last equality follows from the monotonicity of the logarithm function. The following choice constitutes a feasible point of the SDP in (4.I.17):

$$F' = \frac{1}{d}, \quad \mu = \frac{d-1}{d(1-F)}, \quad X_{AB} = \frac{Fd-1}{d(1-F)} \Phi_{AB}^d. \tag{4.I.18}$$

Clearly $\mu \geq 0$ for every $d \geq 1$, and $X_{AB} \geq 0$ since we have assumed $F > \frac{1}{d}$. Also, $\mu \zeta_{AB}^{F,d} = \zeta_{AB}^{F',d} + X_{AB}$ as we see below:

$$\mu \zeta_{AB}^{F,d} = \frac{d-1}{d(1-F)} F \, \Phi_{AB}^d + \frac{d-1}{d(1-F)} (1-F) \frac{I_{AB} - \Phi_{AB}^d}{d^2-1} \tag{4.I.19}$$

$$= \left(\frac{d-1}{d(1-F)} F + \frac{1}{d} - \frac{1}{d}\right) \Phi_{AB}^d + \frac{d-1}{d} \frac{I_{AB} - \Phi_{AB}^d}{d^2-1} \tag{4.I.20}$$

$$= \frac{1}{d} \Phi_{AB}^d + \left(1 - \frac{1}{d}\right) \frac{I_{AB} - \Phi_{AB}^d}{d^2-1} + \frac{Fd-1}{d(1-F)} \Phi_{AB}^d \tag{4.I.21}$$

$$= \zeta_{AB}^{\frac{1}{d},d} + \frac{Fd-1}{d(1-F)} \Phi_{AB}^d. \tag{4.I.22}$$

Therefore, we can write the following upper bound on the smooth-min relative entropy of entanglement:

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F,d}\right) \leq - \log_2 \left(\frac{d-1}{d(1-F)} (1-\varepsilon) - \frac{Fd-1}{d(1-F)} \right) \tag{4.I.23}$$

$$= \log_2 \left(\frac{\varepsilon(1-d) + d(1-F)}{d(1-F)} \right) \tag{4.I.24}$$

$$= - \log_2 \left(1 - \frac{\varepsilon}{1-F} \left(1 - \frac{1}{d}\right) \right). \tag{4.I.25}$$

The argument of logarithm in the above function expression is always positive if $1 - \varepsilon \geq F$, and it matches with the lower bound on the smooth-min relative entropy of entanglement of an isotropic state obtained in (4.I.14).

If $1-\varepsilon < F$, then we can choose the following feasible point of the SDP in (4.I.17):

$$F' = \frac{1}{d}, \quad \mu = \frac{1}{dF}, \quad X_{AB} = 0, \tag{4.I.26}$$

which leads to the following inequality:

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F,d}\right) \leq -\log_2\left(\frac{1-\varepsilon}{Fd}\right) \qquad \text{if } 1-\varepsilon < F \tag{4.I.27}$$

$$= \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) \qquad \text{if } 1-\varepsilon < F. \tag{4.I.28}$$

We can combine the inequalities in (4.I.25) and (4.I.28) to write the following inequality:

$$E_R^{\varepsilon}\left(\zeta_{AB}^{F,d}\right) \leq \begin{cases} -\log_2\left(1-\left(1-\frac{1}{d}\right)\frac{\varepsilon}{1-F}\right) & \text{if } 1-\varepsilon \geq F \\ \log_2 d + \log_2\left(\frac{F}{1-\varepsilon}\right) & \text{otherwise} \end{cases}. \tag{4.I.29}$$

Since the upper bound on the smooth-min relative entropy of entanglement of an isotropic state matches with the lower bound in (4.I.15), we conclude the statement of Proposition 4.4.