

University of Technology Sydney
Faculty of Engineering and Information Technology

Error Exponent Analysis in Quantum Information Theory



Hao-Chung Cheng

Supervisor: Min-Hsiu Hsieh

Co-supervisor: Marco Tomamichel

This dissertation is submitted for the degree of

Doctor of Philosophy

October 2018

Certification of Original Authorship

I certify that this thesis “Error Exponent Analysis in Quantum Information Theory” has been written by me. This thesis is the result of a research candidature conducted with another University as part of a collaborative Doctoral degree. Any help that I have received in my research and in the preparation of the thesis itself has been fully acknowledged. In addition, I certify that all information sources and literature used are quoted in the thesis

Production Note:

Signature: Signature removed prior to publication.

Date: 28 November 2018

Abstract

Error exponent analysis aims at evaluating the exponential behaviour of the performance of the underlying system given a certain fixed coding rate. It is arguably a significant research topic in information theory because the analysis characterizes the trade-offs between the error probability of an information task, the size of the coding scheme, and the coding rate that determines the efficiency of the task. In this thesis, we give an exposition of error exponent analysis to two important quantum information processing protocols—classical data compression with quantum side information, and classical communications over quantum channels.

We first prove substantial properties of various exponent functions, which allow us to better characterize the error behaviours of the tasks. Second, we establish accurate achievability and optimality finite blocklength bounds for the optimal error probability, providing useful and measurable benchmarks for future quantum information technology design. Finally, we extend the error exponent analysis to a more general setting where the coding rate is not fixed anymore, a research topic known as moderate deviation analysis. In other words, we show that the data recovery can be reliable when the compression rate approaches the conditional entropy slowly, and the reliable communication over a classical-quantum channel is possible as the transmission rate approaches channel capacity slowly.

This line of research lies in the intersection of statistical analysis, matrix analysis, and information theory. Thus, the techniques employed in this studies could potentially be applicable to various areas such as classical and quantum information community, detection and estimation theory, statistics, and secrecy.

Keywords: error exponent analysis, moderate deviation analysis, quantum information theory, classical-quantum channel, Slepian-Wolf coding, quantum side information, reliability function, large deviation theory, matrix analysis.

Acknowledgements

I sincerely thank my supervisor Min-Hsiu Hsieh and co-supervisor Marco Tomamichel for guiding me into the research field of quantum information theory. Under their supervision, I learn the knowledge and techniques of quantum information, quantum machine learning, quantum Markovian process, entropies, and matrix analysis. I cannot finish this thesis without their help.

I want to thank University of Technology Sydney and Centre for Quantum Software and Information (UTS:Q|SI) for generously providing me the financial support not only for my living in Sydney, Australia, but also for the travel funding to many academic conferences. I'm eternally grateful.

I would like to thank all the members, staff, and students in UTS:Q|SI for all your support of my study in Sydney. All of you teach me a lot. I also want to thank my dear friends: Deborah, Summer, James, Ellen, Ching-Yi, Xin, Yinan, Kun, Anny, and Rachel. You make my life in Sydney fruitful.

I want to thank my collaborators Prof. Nilanjana Datta, Eric P. Hanson, Li Gao, Barış Nakiboğlu, and Jon Tyson. I'm so happy and grateful when working with you.

Last but not least, I want to thank my dear family. Thank you for supporting me doing what I like as always. This thesis is dedicated to you all.

Contents

List of Figures	iv
List of Tables	v
1 Introduction	1
1.1 Backgrounds	1
1.2 Quantum Information Processing Protocols	4
1.2.1 Information Storage with a Quantum Helper (Source Coding)	5
1.2.2 Information Transmission over a Quantum Channel (Channel Coding)	7
1.3 Main Contributions	9
1.4 Structure of the Thesis	11
<u>I Fundamentals</u>	13
2 Mathematical Tools	14
2.1 Matrix Analysis	14
2.2 Large Deviation Theory	19
3 Quantum Entropic Quantities and Notation	26
3.1 Quantum Rényi divergence	27
3.2 Conditional Rényi Entropy	29
3.3 Rényi and Augustin Information	30
4 Quantum Hypothesis Testing	39
4.1 Achievability	40
4.2 Optimality	41
4.2.1 Nussbaum-Szkoła Distributions	44
4.2.2 Proofs of Theorem 4.4 and Corollary 4.1	44
4.3 Moderate Deviation Analysis	47
4.3.1 Proof of Theorem 4.5	48
4.3.2 Proof of Theorem 4.6	52
<u>II Classical Information Storage with a Quantum Helper</u>	54
5 Error Exponent Functions (Source Coding)	55
5.1 Variational Representations	56
5.2 Properties of Auxiliary Functions	57
5.2.1 Proof of Proposition 5.1	58
5.2.2 Proof of Proposition 5.2	61
5.3 Properties of Error Exponent Functions and Saddle-Point	62

6	Achievability (Source Coding)	66
6.1	I.I.D. Sources	67
6.2	Type-Dependent Sources	69
7	Optimality (Source Coding)	73
7.1	One-Shot Converse Bound (Hypothesis Testing Reduction)	73
7.2	Proof of Main Result, Theorem 7.1	76
8	Moderate Deviation Analysis (Source Coding)	78
8.1	Asymptotic Expansion of Error Exponent around Slepian-Wolf Limit	81
III Classical Information Transmission over a Quantum Channel		84
9	Error Exponent Functions (Channel Coding)	85
9.1	Variational Representations	87
9.2	Properties of Auxiliary Functions	90
9.2.1	Proof of Proposition 9.1	93
9.2.2	Proof of Proposition 9.2	98
9.2.3	Proof of Proposition 9.3	100
9.2.4	Proof of Proposition 9.4	100
9.3	Properties of Error Exponent Functions and Saddle-Point	102
9.3.1	Proof of Proposition 9.5	104
9.3.2	Proof of Proposition 9.6	110
10	Achievability (Channel Coding)	112
10.1	Random Codes with I.I.D. Ensemble	113
10.2	Random Codes with Constant Composition Ensemble	116
11	Optimality (Channel Coding)	120
11.1	Literature Review of Classical Sphere-Packing Bound	121
11.2	A Weak Sphere-Packing Bound via Wolfowitz Strong Converse	123
11.2.1	Proof of Wolfowitz's Strong Converse, Proposition 11.1	125
11.3	A Strong Sphere-Packing Bound	126
11.3.1	One-Shot Converse Bound (Hypothesis Testing Reduction)	127
11.3.2	Chebyshev's Type Converse Bound	127
11.3.3	A Sharp Converse Bound	130
11.3.4	Uniform Continuity	133
11.3.5	Proofs of Main Result, Theorem 11.1 and Corollary 11.1	137
11.4	Symmetric Classical-Quantum Channels	139
12	Moderate Deviation Analysis (Channel Coding)	142
12.1	Proof of Achievability, Theorem 12.1	143
12.2	Proof of Optimality, Theorem 12.2	144
12.3	Asymptotic Expansions of Error-Exponent around Capacity	148
13	Conclusions and Open problems	152
13.1	Open Problems	153
13.1.1	Properties of Error Exponent Functions and Auxiliary Functions	153
13.1.2	Achievability: Random Coding Bound	154
13.1.3	Optimality: Sphere-Packing Bound	155
13.1.4	Moderate Deviation Analysis	156

Bibliography

157

List of Figures

1.1	We are given n copies of a classical source X which is correlated with a quantum system B . We compress the source into an index set \mathcal{I}_n via the encoder \mathcal{E}_n , and then perform a decoding via \mathcal{D}_n which has access to the side information ρ_{B^n} . This yields the output \hat{X}_n with associated alphabets \mathcal{X}^n . The decoder \mathcal{D}_n here is a family of positive operator-valued measurement (POVM) $\left\{ \Pi_{X^n}^{(w^n)} \right\}_{w^n \in \mathcal{I}^n}$. The red-dotted lines indicate classical information, while the blue-solid lines stand for quantum information.	7
1.2	We encode the (classical) message m to an n -blocklength sequence x^n . Then, input sequence will be mapped to an n -product channel output state $W_{\mathbf{x}^n}^{\otimes n}$. Lastly, the decoder, a positive operator-valued measurement (POVM), measures the channel output state to obtain the estimated message \hat{m} . The red-dotted lines indicate classical information, while the blue-solid lines stand for quantum information.	8
1.3	Structure of the thesis.	12
9.1	This figure illustrates three cases of the strong sphere-packing exponent $E_{\text{sp}}(R)$ over $R \geq 0$. In the first case $0 = R_\infty < C_{\mathcal{W}}$ (the left figure), $E_{\text{sp}}(R)$ is only infinite at $R = 0$ and finite otherwise. In the second case $0 < R_\infty < C_{\mathcal{W}}$ (the central figure), $E_{\text{sp}}(R) = +\infty$ for $R < R_\infty$, and $E_{\text{sp}}(R) < +\infty$ for $R \geq R_\infty$. In the third case $0 < R_\infty = C_{\mathcal{W}}$ (the right figure), $E_{\text{sp}}(R) = +\infty$ for $R < C_{\mathcal{W}}$, and $E_{\text{sp}}(R) = 0$ for $R \geq C_{\mathcal{W}}$. Without loss of generality, we assume $R_\infty < C_{\mathcal{W}}$ to exclude the last case throughout this paper.	105
13.1	Sphere-packing exponents in two quantum information processing protocols.	153

List of Tables

1.1	This table compares the asymptotic error behaviors of quantum hypothesis testing and classical-quantum channel coding in three error probability regimes: (i) large error (central limit theorem), (ii) medium error (moderate deviation principle), and (iii) small error (large deviation principle). The quantity S_n denotes the sum of n independent and identically distributed random variables with zero mean and variance v . The exponent Λ^* is the Legendre-Fenchel transform of the normalized cumulant generating function of S_n [1]. The error $\hat{\alpha}_{\exp\{-nr\}}$ is defined as the minimum type-I error with the type-II error smaller than $\exp\{-nr\}$. The quantities D and V in the hypothesis testing column denote the quantum relative entropy and the relative entropy variance, respectively. The optimal error probability with blocklength n and rate R is denoted by $\epsilon^*(n, R)$. The quantities C and V in the channel coding column indicate the channel capacity and the channel dispersion, respectively. The sequence $(a_n)_{n \in \mathbb{N}}$ satisfies Eq. (1.7). The quantity $E(R)$ is the reliability function of the classical-quantum channel [2], and has not been fully characterized yet.	5
11.1	Different sphere-packing bounds are compared by (i) the bound is finite blocklength or asymptotical; (ii) whether or not they are dependent on the constant composition codes; (iii) & (iv) the asymptotics of $f(n)$ and $g(n)$; (v) the corresponding c-q generalizations. The parameter t in rows (e) and (f) is some value in the range $t > 1/2$; and (vi) whether their error exponent expressions for c-q channels are in the strong form (Eq. (1.4)) or weak form (Eq. (12.51)).	121
13.1	The comparison of the error exponent analysis for Slepian-Wolf coding with quantum side information and classical-quantum channel coding. We note that we only obtained suboptimal achievability results (i.e. with the exponent $E_r^\dagger(R)$ instead of $E_r(R)$). . . .	152