Some mathematical problems in quantum information theory

Yinan Li

11916855

Supervisor: Professor Runyao Duan

July, 2018

1 Abstract

The quantum information theory is the result of the efforts to generalize classical information theory to the quantum world. This report introduces some basic problems in quantum information theory, and concentrates on the recent and latest works in discrimination problem of quantum states and operations. The quantum state discrimination problem is identifying the unknown states from an arbitrary set a of known states. We care about the probability of inconclusive answer when we use the strategy named unambiguous discrimination. The quantum operation discrimination problem is identifying the unknown operation from several known operations, we care about which kind of operations can be perfectly distinguished. We also care about the protocols we used to identify states or operations. More precisely, we are trying to compare different protocols and interested in the optimal scheme as well. It will be a valuable choice to move attention to the strurcture of positive maps which has close connect with separability of states and quantum operations. We also care about the positivity of linear maps under tensor power.

Keywords: quantum information theory, quantum operation, discrimination, mathematics.

Contents

2 Introduction

Quantum mechanics is a fundamental branch of physics which deals with physical phenomena at nanoscopic scales, where the action is on the order of the Planck constant. With the effort of a lots of physicists like Einstein, Bohr, Planck, Dirac and Von Neumann, a complete mathematical description to this fantastic field has been developed and applied to industy world. Meanwhile, a branch of applied mathematics, electrical engineering and computer science involving the quantification of information named information theory was developed by Shannon to find fundamental limits on signal processing operations such as compressing data and on reliably storing and communicating data.

In Twentieth Century, with the rapid development of computers, Moore rised his famous conjecture, the "Moore's law". It was the observation that, over the history of computing hardware, the number of transistors in a dense integrated circuit has doubled approximately every two years. The exponential increase of transistors drived scientists to rise some other ways to achieve the computation theory rised by Turing in 1936. In 1980's, Manin, Feynman and Deutsch rised a new model of computer based on quantum mechanics. classical computer has a memory made up of bits, where each bit represents either a one or a zero. A quantum computer maintains a sequence of qubits. A single qubit can represent a one, a zero, or any quantum superposition of those two qubit states; a pair of qubits can be in any quantum superposition of 4 states, and three qubits in any superposition of 8 states. In general, a quantum computer with n qubits can be in an arbitrary superposition of up to 2^n different states simultaneously.

Together with quantum computer, scientists applied quantum mechanics in information theory. In 1992, Bennett and Wiesner rised a technique in their paper named "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states" called Superdense Coding. This technique was used to send two bits of classical information, i.e. two classical bits, using only one qubit. In 1993, Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters rised another technique in their paper named "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels" named Quantum Teleportation.

It was a process allowed transmit one qubit from one location to another with the help of classical communication, i.e sending two classical bits, and previously shared quantum entanglement between the sending and receiving location. This two techniques, together with some properties of quantum mechanics like entanglement, built the bases of quantum information theory.

In recent years, quantum information theory has developed rapidly and attracted lots of scientists. One of the fundamental problem is the distinguish problem. In 1990's, distinguish different quantum states has been researched and get some remarkable results. In the first decade of 21st century, there are some works focused on distinguish quantum channels, which helped to build the theoretical background for the expiremental realizations.

The research in the area of quantum information theory is significant and remarkable considering many reasons. For instance, quantum information theory gives a new model for scientists to build a brand new way to communication. It will be far more secure than any other classical channels. Furthermore, the research will help scientists understand the essences of lots of fantastic phenomenons which were discovered in expirements. Meanwhile, with the help of lots of newly discovered techniques and theories, it is worth to find the mathematical structure of quantum information theory which will give scientists lots of new way to solve problems connected with quantum information theory.

3 Literature Review

3.1 Quantum states discrimination

Quantum state discrimination is an essential problem in quantum information theory. However, the perfect discrimination among nonorthogonal pure states is forbidden by the laws of quantum mechanics. The reason has been demonstrated in chapter 2 of [1]. Instead of considering the discrimination of two states, a new strategy named unambiguous discrimination was rised. In this way we allowed a non-zero probability of inconclusive answer when distinguishing certainty linearly independent states. Unambiguous discrimination among two nonorthogonal quantum pure states with unequal priori probabilities was demonstrated by Jaeger and Shimony [2]. Chefles [3] showed that n quantum pure states can be unambiguously discriminated if and only if they are independent. For the general cases of unambiguous discrimination between n pure states with a prior probabilities, it was shown in [4] and [5] that it can be reduced to a semidefinite programming problem. For the mixed state discrimination, Feng [6] gave a sufficient and necessary condition of when states can be unambiguously discriminated and a series of lower bounds on the inconclusive probability.

In a quantum information communication scheme, the distinguish problem was mostly used when the two parties in the scheme, named Alice and Bob. Alice was trying to encode information into a quantum states in order that Bob can distinguish them. In this scheme sometimes we can only do local measurement to some parties of a state rather than a globe measurement to the whole state. In such a case, most of the time we allowed classical communication. We call this LOCC (Local Operation and Classical Communication) protocol. The LOCC protocol has been studied in lots of area of quantum information theory. The most famous one should be the process named “Quantum Teleportation” [7], which makes the LOCC protocol an important source. Naturally we will consider distinguish quantum states with LOCC protocol. In this situation, Bennet [8] showed that there exist sets of orthogonal product states that cannot be distinguished by LOCC. This surprising result shows that LOCC discrimination is more difficult to characterize mathematically. In 2008, Walgate [9] demonstrated that it is posible to LOCC distinguish two orthogonal quantum states which makes all perfectly distinguishable states are distinguishable by LOCC. Without only obtaining classical information from an unknown system, Li [10] rised a new strategy about LOCC discrimination. Without abandoning the unknown system when the discrimination failed, we can still use the remain system to distillation entanglement [11]. The idea is When discrimination fails, we transform different states into the same entangled state.

3.2 Quantum operation discrimination

A quantum operation, also called quantum channel, is a mathematical formalism used to describe a broad class of transformations that a quantum mechanical system can undergo. In the view of quantum mechanics and mathematics, quantum operation is a linear map maps a density operator in a quantum system to another. In order to maintain the properties of quantum mechanics, this linear map should be completely positive and trace preserving. In general, we use the Kraus operator $\{E_k\}$ to represent the operation $\mathcal{E}$ as $\mathcal{E}(\cdot) = \sum_k E_k \cdot E_k^\dagger$(see chapter 8 in [1]).

A problem closely related to quantum state discrimination is the discrimination of quantum operations. The goal of quantum operation discrimination is to find out the identity of an unknown device secretly chosen from two known quantum operations. Compared with the quantum state discrimination, quantum operation discrimination has some differences. First of all we can treat the quantum operation as a quantum device which can be used repeatly. Second, the input state of a quantum operation can be choosen freely, which makes it much more possible to obtain orthogonal states. Finally, perhaps most importantly, quantum operations can be used in many essentially different ways such as in parallel, in sequential or in any other scheme allowd by quantum mechanics. This problem has received great interest recently. In 2001, Acin [12] found that given two unitary operations, U_1 and U_2, there always exists a finite number N such that $U_1^{\otimes N}$ and $U_2^{\otimes N}$ are perfectly distinguishable. In 2005, Sacchi [13] proved that the use of entangled input states generally improves the discrimination.

Some excited result has been found in recent years. In 2007, Duan [14] proved that entanglement is not necessary for perfect discrimination between unitary operations. This work is remarkable since it didn't need entanglement to distinguish, which is a much more economic way. Furthermore, a sequential discrimination scheme made us develop different schemes which could make every sources we have useful. In 2009, Duan [15] provided a feasible necessary and sufficient condition for when an unknown quantum operation (quantum device) secretly selected from a set of known quantum operations can be identified perfectly within a finite number of queries, and thus complete the characterization of the perfect distinguishability of quantum operations. Let $\mathcal{E}_0$ and $\mathcal{E}_1$ be two quantum operations with kraus operators $\{E_{0i} : i = 1, \cdots, n_0\}$ and $\{E_{1j} : j = 1, \cdots, n_1\}$ respectly. Then $\mathcal{E}_0$ and $\mathcal{E}_1$ are perfectly distinguishable iff $\mathcal{E}_0$ and $\mathcal{E}_1$ are disjoint and $I_d \notin span\{E_{0i}^\dagger E_{1j}\}$. With this condition we can design an optimal protocol to achieve the discrimination with a minimal number of queries. In fact, with the condition we can prove that auxiliary systems or entanglement is not necessary when distinguish unitaries which was demonstrated in [14].

Similarly, we can also consider the Local distinguishability of multipartite unitary operations. Duan [16] found that any two different unitary operations acting on an arbitrary multipartite quantum system can be perfectly distinguished by local operations and classical communication when a finite number of runs is allowed. It is worth to mention that this work has strong connection with the mathematical notion named numerical range which has been researched for decades. For $A \in \mathcal{B}(\mathcal{H})$, the numerical range of A is a subset of complex numbers: $W(A) = \{\langle\psi| A |\psi\rangle : \langle\psi|\psi\rangle = 1\}$. Interestingly, a celebrated result due to Toeplitz and Hausdorff states that the numerical range of a bounded linear operation is always convex [17]. In a LOCC discrimination problem, we will need the definition of local numerical range of A which defined as $W^{local}(A) = \{\langle\psi| A |\psi\rangle : |\psi\rangle = \otimes_{k=1}^m |\psi_k\rangle\}$. Furthermore, if two multipartite unitary operations U_1 and U_2 can be distinguished by LOCC in the single-run scenario iff $0 \in W^{local}(U_1^\dagger U_2)$.

3.3 Other problems

3.3.1 Separablility of bipartite states

Consider a composite quantum system described in a bipartite Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$. A state ρ was called separable if it can be represent by a convex combination of a set of pure states, i.e. $\rho = \sum_{i=1}^{k} \lambda_i \rho_{1i} \otimes \rho_{2i}$. A state which can't be represent in this way is called an entangled state. Entanglement is one of the most important phenomenons in quantum mechanics and has shown its powerful feature in lots of area of quantum information theory. In chapter 2.6 of [1], it mentioned a work by Einstein, Podolsky and Rosen named EPR criterion in 1930's, which was aimed to show that quantum mechanics is incomplete, by identifying elements of reality that were not included in quantum mechanics. The way they attempted to do this was by introducing what they claimed was a sufficient condition for a physical property to be an element of reality, namely, that it be possible to predict with certainty the value that property will have, immediately before measurement. After 30 years' effort, an experimental test was proposed that could be used to check whether or not the picture of the world which EPR were hoping to force a return to is valid or not and the key to this experimental invalidation is a result known as Bell's inequality. In this way, we consider all the states with classical correlations, which has some similarities with the objects in our real world. This kind of states can't violate the Bell inequality. However, some states do violate the Bell inequality, like the EPR pairs, which are the states representated as $|\psi_\pm\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$ or $|\phi_\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$. These four states are clearly not separable states. Sometimes we use the "hidden variable" theory to describle the classical correlation. For all separable states, they admit the "hiden variable" theory. Interestingly, there are some states which violate the Bell's inequality, meanwhile they admit the "hidden variable" theory. In 1990's Werner [24] gave a constructive proof for such an interesting phenomenon and this kind of states were called the Werner states.

It is natrually to rise a question: "Whether a state is separable or not?" In 1996, Peres [18] and Horodecki [19] found that the partial transposition map can be used to check if a state is separable or not. In fact, in $2 \otimes 2$ and $2 \otimes 3$ systems, this criterion becomes a sufficient and necessary condition. While for high dimensional cases, a state ρ is separable if and only if for every positive map $\mathcal{P}$, the operator $(\mathbb{1} \otimes \mathcal{P})(\rho)$ remains positive. Clearly, there exists states which is not separable but has positive partial transposition. These kind of states are named bound entangled states. These states are interesting because they can not be used to obtain pure entanglement states by LOCC protocol [20].

3.3.2 The sturcture of positive maps

A linear map $\mathcal{P}$ between matrix spaces is called a positive map if it maps all the positive matrices to positive matrices. This kind of map has a wide range of applications. For instance, they are used to verify the separability of quantum states. Moreover, some special positive maps, like completely positive maps, can be used to represent all the process which can be achieved in a phyical expirement. Meanwhile, this kind of positive maps can also be represented by Kraus operators as it showed in 3.2. In fact, there is a isomorphism between linear maps and complex matrices rised by Choi [21]. This isomorphism send every linear maps $\mathcal{P}$ to complex matrices $(\mathbb{1} \otimes \mathcal{P})(|\Phi_+\rangle \langle\Phi_+|)$ where $|\Phi+\rangle$ is the maximally entangled state. It has been shown that the linear map can be fully characterized by its Choi matrix. With this isomorphism, Skwronek [22] showed that we can use the choi matrix to research the positivity of a linear map. Also it is well known that a linear map is positive if and only if its Choi matrix has non-negative local numerical range, a linear map is completely positive if and only if its Choi matrix is positive. It is worth to mention that in $2 \otimes 2$ or $2 \otimes 3$ cases, every positive map $\mathcal{P}$ can be represented as $\mathcal{P} = \Lambda_1 + \Lambda_2 \circ T$ where Λ_1 and Λ_2 are completely positive maps and T denotes the transposition map.

We also care about the positivity of a linear map after tensor with itself several times. Clearly a completely positive map remains positive after tensor any times, so is the composition of transposition map and any completely positive map which is called the completely co-positive map. We noticed that these kind of maps will not be local distinguished. We name a map n-tensor-stable positive map if it remains positive after tensor n times and a map tensor-stable positive map if it remains positive after tensor arbitrary times. We concern those maps which is tensor-stable positive but not completely positive or completely co-positive, which are named non-trivial tensor-stable positive map. Hermes [23] has shown that there exists n-tensor-stable positive maps but not completely positive or completely co-positive.

4 Conclusion

There still remain some open problems about quantum state discrimination. Considering former progress on this question, Feng [6] only gives a series of lower bound in unambiguous discrimination between mixed states. For arbitrary set of mixed states with priori probabilities, the optimal solution to its corresponding semidefinite programming problem is still unknown. We also cares about the local unambiguous discrimination of quantum states with remaining entanglement. For the bipartite stete, we have known that for any n entangled pure state this protocol can always be done, i.e. we can either distinguish them or obtain the EPR pairs with N copies [10]. While this problem has not been solved in Multipartite cases.

For the problems related to quantum operation discrimination, Though Duan [15] has risen a feasible sufficient and necessay condition, we still cares about to find a feasible algrithm to calculate the optimal scheme. Beside this, we also cares about the relation between quantum operation discrimination and numerical range. In fact, when solving the problem of discrimination unitary operations, we only need to calculate a matrix's numerical range [15], which can be also used to prove the useless of entanglement in such a discrimination problem. While for arbitrary quantum operation, the use of numerical range has not been identified. Furthermore, for the globe discrimination problem, we can treat them in a more mathematical way, we can consider the space A spanned by their Kraus operators. If these two operation can be distinguished, then first there will be no positive definite matrix in this space. We consider using the parallel scheme, the discrimination problem will become finding a positive semidefinite matrix in the orthogonol complement of $A^{\otimes n}$ where n is the copies we have. In fact for arbitrary matrix subspace A which does not have positive definite matrix, it is still unknown that if there exists a finite integer n such that there exists a positive semidefinite matrix in the orthogonol complement of $A^{\otimes}$. This will be an interesting mathematical question which highly connected with the discrimination problem.

We also cares about the discrimination under local operation and classical communication. From now on, only multipartite unitary operations has been solved. The feasible conidition for arbitrary multipartite operation has not been solved yet. We have known that the LOCC discrimination should always satisfies the globe discrimination's condition, the problem we cares about is whether there is any additional condition for LOCC protocol. Meanwhile, it is worth to translate such a problem to a local numerical range problem. Though we have known that the numerical range of a matrix is always convex, the properties and sturctures of local numerical range remains unknown. Furthermore, we also care about the structure of positive maps. The exists of a non-trivial tensor-stable positive map has not be proved. This problem is also connected to local numerical range under tensor powers.

My research mainly concentrates on the connection between quantum information theory and mathematics,aiming to improve the systematic quantum information theory. I will strengthen my mathematical background and try to solve the problems above. It will be valuable to find the beatiful structure of mathematics can be applied in lots of areas of quantum information theory.

References

[1] Nielsen, M.A. & Chuang, I.L. 2010, ‘Quantum computation and quantum information’, Cambridge University Press, New York.

[2] Jaeger, G. & Shimony, A. 1995, ‘Optimal distinction between two non-orthogonal quantum states’, Physics Letters A, vol. 197, no. 2, pp. 83-7.

[3] Chefles, A. 1998, ‘Unambiguous discrimination between linearly-independent quantum states’, ArXiv Preprint quant-ph/9807022.

[4] Sun, X., Zhang, S., Feng, Y. & Ying, M. 2002, ‘Mathematical nature of and a family of lower bounds for the success probability of unambiguous discrimination’, Physical Review A, vol. 65, no. 4, p. 044306.

[5] Eldar, Y.C. 2003, ‘A semidefinite programming approach to optimal unambiguous discrimination of quantum states’, Information Theory, IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 446-56.

[6] Feng, Y., Duan, R. & Ying, M. 2004, ‘Unambiguous discrimination between mixed quantum states’, Physical Review A, vol. 70, no. 1, p. 012308.

[7] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. & Wootters, W.K. 1993, ‘Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels’, Physical Review Letters, vol. 70, no. 13, p. 1895.

[8] Bennett, C.H., DiVincenzo, D.P., Fuchs, C.A., Mor, T., Rains, E., Shor, P.W., Smolin, J.A. & Wootters, W.K. 1999, ‘Quantum nonlocality without entanglement’, Physical Review A, vol. 59, no. 2, p. 1070.

[9] Walgate, J., Short, A.J., Hardy, L. & Vedral, V. 2000, ‘Local distinguishability of multipartite orthogonal quantum states’, Physical Review Letters, vol. 85, no. 23, p. 4972.

[10] Li, Y., Duan, R. & Ying, M. 2010, ‘Local unambiguous discrimination with remaining entanglement’, Physical Review A, vol. 82, no. 3, p. 032339.

[11] Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A. & Wootters, W.K. 1996, ‘Purification of noisy entanglement and faithful teleportation via noisy channels’, Physical Review Letters, vol. 76, no. 5, p. 722.

[12] Acín, A. 2001, ‘Statistical distinguishability between unitary operations’, Physical Review Letters, vol. 87, no. 17, p. 177901.

[13] Sacchi, M.F. 2005, ‘Optimal discrimination of quantum operations’, Physical Review A, vol. 71, no. 6, p. 062340.

[14] Duan, R., Feng, Y. & Ying, M. 2007, ‘Entanglement is not necessary for perfect discrimination between unitary operations’, Physical Review Letters, vol. 98, no. 10, p. 100503.

[15] Duan, R., Feng, Y. & Ying, M. 2009, ‘Perfect distinguishability of quantum operations’, Physical Review Letters, vol. 103, no. 21, p. 210501.

[16] Duan, R., Feng, Y. & Ying, M. 2008, ‘Local distinguishability of multipartite unitary operations’, Physical Review Letters, vol. 100, no. 2, p. 020503.

[17] Hom, R.A. & Johnson, C.R. 1991, ‘Topics in matrix analysis’, Cambridge University Press, New York.

[18] Peres, A. 1996, ‘Separability criterion for density matrices’, Physical Review Letters, vol. 77, no. 8, p. 1413.

[19] Horodecki, M., Horodecki, P. & Horodecki, R. 1996, ‘Separability of mixed states: necessary and sufficient conditions’, Physics Letters A, vol. 223, no. 1, pp. 1-8.

[20] Horodecki, P. & Horodecki, R. 2001, ‘Distillation and bound entanglement’, Quantum Information & Computation, vol. 1, no. 1, pp. 45-75.

[21] Choi, M.-D. 2000, ’Completely positive linear maps on complex matrices’, Quantum Computation and Quantum Information Theory: Reprint Volume with Introductory Notes for ISI TMR Network School, 12-23 July 1999, Villa Gualino, Torino, Italy, vol. 10, p. 174.

[22] Skowronek, L., Stormer, E. & Zyczkowski, K. 2009, ‘Cones of positive maps and their duality relations’, ArXiv Preprint arXiv:0902.4877.

[23] Müller-Hermes, A., Reeb, D. & Wolf, M.M. 2015, ‘Positivity of linear maps under tensor powers’, ArXiv Preprint arXiv:1502.05630.

[24] Werner, R.F. 1989, ‘Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model’, Physical Review A, vol. 40, no. 8, p. 4277.