

学位論文

Entanglement and Causal Relation
in Distributed Quantum Computation

(分散型量子計算における
エンタングルメントと因果関係)

平成 27 年 12 月博士 (理学) 申請

東京大学大学院理学系研究科
物理学専攻

秋笛 清石

学位論文

Entanglement and Causal Relation
in Distributed Quantum Computation

(分散型量子計算における
エンタングルメントと因果関係)

平成 27 年 12 月博士 (理学) 申請

東京大学大学院理学系研究科
物理学専攻

秋笛 清石

Abstract

Distributed quantum computation (DQC) is information processing performed over multiple quantum systems connected by a quantum network. DQC is one of the most promising candidates for realizing a scalable quantum computer. Quantum communication over the quantum network is indispensable for implementing joint quantum operations over several systems, which is necessary for performing efficient quantum computation in DQC. Since quantum communication is equivalent to entanglement and classical communication as a resource in DQC, we investigate two different aspects of entanglement and classical communication in DQC.

In the first part of this thesis, we study how to improve the performance of quantum computation over a given quantum network resource by analyzing entanglement resources represented by quantum networks. To date, quantum networks have been used mainly for quantum communication, i.e. transmitting quantum states between different nodes of the quantum network. For this purpose, *quantum network coding* aiming to improve the performance of quantum communication over a given quantum network has been recently developed. In contrast, we analyze what kinds of computation can be implemented over a given quantum network resource by introducing a new concept, quantum network coding for quantum computation. This is because computation can be regarded as a general operations including communication as its special case and it is expected to reduce communication resources in DQC by computing and communicating simultaneously.

We consider a setting of networks where quantum communication for each edge of a network is restricted to sending just one-qubit, but classical communication is unrestricted. Specifically, we analyze which k -qubit unitary operations are implementable over a certain class of networks described by two-dimensional lattices, *cluster networks*, by investigating transformations of a given cluster network into quantum circuits. We also analyze which k -qubit unitary operations are *not* implementable over the cluster networks by using a property of a class of joint quantum operations called *separable operations* (SEP). We show that any two-qubit unitary operation is implementable over the *butterfly network* and the *grail network*, which are fundamental primitive networks for classical network coding. Finally, we analyze probabilistic implementations of unitary operations over cluster networks and obtained necessary and sufficient conditions for implementability.

In the second part of this thesis, we study the role of quantum communication in DQC in terms of entanglement and causal relation in classical communication. We investigate resources substituting entanglement and classical communication consumed in entanglement assisted *local operations and classical communication* (LOCC). We start with analyzing the amount of the entanglement resource required for a specific DQC task known as local state discrimination. The task is

discriminating a state from a given set of orthonormal basis states by LOCC with help of entanglement. We show that entanglement required for the discrimination task allowing only one-round classical communication can be substituted by less entanglement by increasing the rounds of classical communication.

Then we develop a new framework to describe deterministic joint quantum operations in two-party DQC, by using a causal relation between the outputs and inputs of the local operations without predefined causal order but still within quantum mechanics, called “*classical communication without predefined causal order*” (CC*). We show that local operations and CC* (LOCC*) is equivalent to SEP, which cannot create entanglement from separable states. This result indicates that entanglement assisted LOCC implementing SEP can be simulated by LOCC*, where no entanglement is needed. By considering the correspondence between LOCC* and a probabilistic version of LOCC called stochastic LOCC (SLOCC), we show that LOCC* can be interpreted to enhance the success probability of probabilistic operations in SLOCC. We also investigate the relationship between LOCC* and another formalism for deterministic joint quantum operations without predefined partial order (the quantum process formalism) recently developed by Ognjan Oreshkov et al. Finally we construct an example of non-LOCC SEP by using LOCC*.

Acknowledgments

First, my deepest appreciation goes to my supervisor Professor Mio Murao for all discussions, encouragement, checking a lot of documents and her continuous support through the past five years. Her thought-provoking, accurate and instructive guidance have permitted me to grow my research and find the directions of my research. I deeply appreciate Dr. Go Kato and Dr. Masaki Owari as collaborators of a research in this thesis and their kind supports for my next career. I also appreciate Dr. Akihito Soeda as a collaborator of a research in this thesis and his suggestive comments. Their advices made enormous contribution to this thesis.

I am deeply grateful to Dr. Peter Turner for all discussions and checking a lot of documents, especially a proposal for Bourses du gouvernement français. I would like to appreciate Dr. Damian Markham for giving me an opportunity to stay his group in Télécom ParisTech and do a collaborative research for half a year. I would like to acknowledge to the examiners of this thesis, Dr. Hosho Katsura, Dr. Yasuhiko Arakawa, Dr. François Le Gall, Dr. Naoki Kawashima and Dr. Masato Koashi. I would like to thank Yuki Amano and Yumiko Wada for their administrative supports. I am also indebted to Dr. Harumichi Nishimura, Dr. Barbara Kraus, Dr. Rod Van Meter, Dr. Hiroyasu Tajima, Dr. Takahiko Satoh, Dr. Kenta Takata, Dr. Giulio Chiribella, Dr. Ognyan Oreshkov, Dr. Fabio Costa, Dr. Āaslav Brukner, Dr. Romain Alléaume, Dr. Eleni Diamanti, Dr. Tom Lawson, Dr. Marc Kaplan, Dr. Alexei Grinbaum, Ms. Christina Giarmatzi, Mr. Amin Baumeler and Mr. Issam Ibnouhsein for their valuable discussions and kind supports. I want to thank my colleagues, Dr. Michal Hajdusek, Dr. Yoshifumi Nakata, Dr. Takanori Sugiyama, Dr. Shojun Nakayama, Dr. Eyuri Wakakuwa, Mr. Kotaro Kato, Mr. Jisho Miyazaki, Mr. Kosuke Nakago, Dr. Fabian Furrer, Mr. Atsushi Shimbo, Mr. Hayata Yamasaki, Mr. Ryosuke Sakai, Mr. Hao Qin, Mr. Leonardo Disilvestro, Mr. Adrien Marie, Mr. Thrasyvoulos Karydis and Mr. Adel Sohbi for our discussions and their advice on my research.

I thank all people who I met in Paris when I did the collaborative research as Bourses du gouvernement français. Finally, my especial thanks goes to my family, my parents, Makine and Yoshihiro, my wife, Saori, and my son, Nagisa, for their devoted supports and encouragement.

Publications

Journal Articles

- A. Soeda, S. Akibue and M. Murao, Two-party LOCC convertibility of quadripartite states and Kraus-Cirac number of two-qubit unitaries, *J. Phys. A: Math. and Theo.*, **47**, 424036, (2014).
- S. Akibue and M. Murao, Network coding for distributed quantum computation over cluster and butterfly networks, arXiv:1503.07740, (2015).

Conference Talks

- S. Akibue, G. Kato, M. Owari and M. Murao, Globalness of separable maps in terms of classical temporal correlations and quantum spatial correlations, 14th AQIS, Kyoto, Japan, (2014).
- S. Akibue and M. Murao, Implementability of unitary operators over the cluster network with free classical communication, 15th AQIS, Seoul, Korea, (2015).
- S. Akibue, G. Kato, M. Owari and M. Murao, Globalness of separable maps in terms of time and space resources, 11th QPL, Kyoto, Japan, (2014).
- S. Akibue and D. Markham, Multipartite correlations with no causal order, New Horizon in Quantum Information Science, Kyoto, Japan, (2014).
- S. Akibue and M. Murao, Implementability of two-qubit unitary operators over the ladder network with free classical communication, 1st ParQ, Edinburgh, UK, (2013).

Conference Proceedings

- S. Akibue and M. Murao, Implementability of two-qubit unitary operations over the butterfly network and the ladder network with free classical communication, AIP conference proceedings, 0094-243X ; **1633**, pp.141f., (2014).

Contents

I	Introduction	1
1	Quantum information science	3
1.1	Overview of quantum information science	3
1.2	Distributed Quantum Computation (DQC)	5
1.3	Quantum entanglement	8
1.4	Space and time	11
1.5	Organization of this thesis	14
2	Preliminaries	17
2.1	Notation	17
2.2	Quantum information theory	18
2.2.1	Quantum mechanics	18
2.2.2	Schmidt decomposition	21
2.3	Quantum operations	21
2.4	Quantum computation models	25
2.4.1	Circuit model	25
2.5	Local Operations and Classical Communication (LOCC)	27
2.5.1	LOCC	28
2.5.2	Separable operation	30
2.5.3	Stochastic LOCC	31
2.5.4	Entanglement assisted LOCC	32
II	Quantum computation over quantum networks	37
3	Preliminaries of Part II	39
3.1	Network coding theory	39
3.1.1	Classical network coding	39
3.1.2	Quantum network coding	40
3.2	Measurement Based Quantum Computation (MBQC)	45
3.3	Classifications of unitary operators	47

3.3.1	Controlled unitary operation	47
3.3.2	Kraus-Cirac decomposition	48
3.3.3	Operator Schmidt decomposition	49
4	Computation over the cluster network	51
4.1	Possible computation	55
4.2	Upper bound of computation	58
4.3	Butterfly, grail and square networks	64
4.4	Probabilistic computation	68
5	Summary and Discussions of Part II	71
5.1	Summary	71
5.2	Discussions	71
III	Role of entanglement and causal relation in DQC	75
6	Resources for state discrimination	79
6.1	Entanglement resource for one-way LOCC	80
6.2	Entanglement resource for two-way LOCC	81
7	Resources for SEP	87
7.1	LOCC*	87
7.2	LOCC* and SEP	91
7.3	LOCC* and local post selection	94
7.4	LOCC* and quantum processes	95
7.5	LOCQP and SEP	96
8	Summary and Discussions of Part III	103
8.1	Summary	103
8.2	Discussion	104
IV	Conclusion	109
V	Appendix	113
A	Quantum computation over quantum networks	115
A.1	A LOCC protocol for controlled unitary operations	115
A.2	LOCC implementation of converted quantum circuits	118
A.3	Converted circuit of $(2, N)$ and $(3, N)$ -cluster network	120

A.4	Maximally entangled state conversion by SEP	122
A.5	Two conditions in Theorem 1	124
A.6	Network coding for the butterfly network	125
A.7	Analysis of four qubit states	127
B	Role of entanglement and causal relation in DQC	133
B.1	Entanglement for one-way LOCC	133
B.2	LOCC and causal order	136
B.3	The rigorous proof of B.2	137
B.4	Formal mathematical formulation of LOCC*	144
B.5	Equivalence of LOCC* and SEP	146
B.6	CC* and classical quantum processes	147
B.7	CQP and LOCC	149
B.8	Classical causally non-separable process	153
B.9	Multipartite LOCC*	153

Part I
Introduction

Chapter 1

Quantum information science

Quantum information science is an emerging interdisciplinary field of science intersecting quantum physics, information theory and computer science. In this chapter, we briefly review a historical overview of quantum information science. A concept of *distributed quantum computation* is introduced, and its potential contribution to future information technology and foundations of quantum information science is presented.

1.1 Overview of quantum information science

Quantum mechanics is one of the most significant discovery in science in the twentieth century. In the early twentieth century, many physicists explored a new theory of physics to capture phenomena that cannot be explained by classical physics such as Newtonian mechanics and electromagnetism. Erwin Schrödinger and Werner Karl Heisenberg have led early developments in formulating quantum theory in mid-1920s. In 1930s, a mathematically rigorous and pragmatic framework of quantum mechanics was established by John von Neumann and Paul Dirac, respectively [1, 2]. Quantum mechanics has improved the precision of predictions of empirical results. Moreover, it has substantially changed our understanding of nature since its axioms and consequences are very different from classical physics. Nowadays, many subfields of physics such as condensed matter physics, optical physics and particle physics, are based on quantum mechanics. Quantum mechanics has changed not only our understanding of nature but also that of more abstract concepts of *information* and *computation*.

In information theory, the main interest is to understand how much information we can transmit through a given *communication channel*, or just referred as a *channel*, physically implemented by an optical fiber, a LAN cable and so on. A foundation of information theory is built by a paper written by Claude Shannon

in 1948 [3]. He has developed a formalism to describe the amount of information irrespective of the meaning it conveys and the physical systems carrying information. And he has shown that the amount of information coincides with the optimal compression rate of information under certain setting. He also defined *channel capacity* as the amount of the optimal information transmission rate in a single time by using a channel. An extension of information theory considering quantum mechanical effects, quantum Shannon theory, has been developed [4, 5] and is still extensively developing.

In computer science, especially in computational complexity theory, understanding properties of computationally difficult problems in principle is the main interest. A “computationally difficult problem” is a problem that can be solved by following the right procedure, but takes an extremely long time or a large memory space to solve. For example, as far as we know, factoring a given 1000-bit number is such a typical problem. The computational difficulty of a problem is evaluated by the optimal time length (time complexity) or the optimal amount of the memory size (space complexity) to solve the problem by using the *Turing machine*, a calculation model invented by Alan Turing in 1936 [6]. The easy problem is defined as the problem that can be solved efficiently by Turing machine, i.e. the optimal time length and the optimal amount of the memory size for solving the problem is a polynomial in the size of the input of the problem.

Since the computational power of currently widely used silicon-based computers can be regarded as same as Turing machine, computationally difficult problems are intractable by the silicon-based computers. Then is it really hard to solve a computationally difficult problem no matter how we contrive to solve it? If the nature obeys classical physics, the answer is yes. Because classical physics can be simulated by the Turing machine efficiently¹. However, the nature is governed by quantum mechanics in a microscopic scale. It also seems difficult for Turing machine to simulate quantum mechanics. In contrast, there is a possibility that quantum mechanics is efficiently simulatable by using a quantum system. This implies that *quantum computer*, which uses the power of quantum mechanical effects, can be faster than classical computers such as silicon-based computers and Turing machine [7].

Indeed, quantum algorithms that run faster than all the known classical algorithms are proposed by [8, 9, 10]. A significant difference between quantum computation and classical computation is the basic unit of information. The basic unit of information of quantum computation is a quantum bit, called a *qubit*, and that of classical computation is a bit. A bit is a two-valued quantity, and a qubit

¹It takes hours proportional to Vt for Turing machine to simulate the time evolution of a physical system governed by classical physics, where V is the volume of the physical system and t is the time of the time evolution.

is a two-level quantum system e.g. a spin of an electron, polarization of a photon. While a bit can take only two states, 0 or 1, the state representing a qubit can be any superposition of 0 and 1 due to quantum mechanics.

We have seen that quantum mechanics provides a new paradigm to information theory and computer science. Aside from them, quantum mechanics also provides new cryptographic systems [11, 12], of which security is guaranteed by the law of physics in contrast to the commonly used cryptographic systems based on computational complexity. Quantum information science is a field of science to study information processing that uses quantum mechanical effects. A variety of new information processing schemes have been discovered and rapid progresses in technologies are realizing the schemes. Quantum information science also provides a new operational perspective of quantum mechanics by using frameworks developed in information theory and computer science.

1.2 Distributed Quantum Computation (DQC)

Distributed computation is computation over a networked computation system in which spatially separated computers are connected by communication channels in order to jointly perform a common task. Cluster computation is an example of distributed computation. In this thesis, we use “distributed computation” in a broader sense where each separated computer is not necessary to jointly perform a common task but they can perform their own task by communicating with each other. In this sense, telecommunication and internet are also examples of distributed computation.

Distributed quantum computation (DQC) is an information processing over multiple separated quantum systems connected by mediating quantum systems (quantum channels), which aims not only quantum computation but also more general distributed tasks, e.g. running a quantum cryptographic protocol. There are two reasons to assert that DQC will be an infrastructure of the future information society.

First, a practical quantum computer will be based on DQC. Many different kinds of physical systems have been studied in order to figure out their suitability for implementing quantum computation, such as ion traps [13], nuclear magnetic resonance [14], quantum dots [15] and linear optics [16]. Small quantum computers consisting of several qubits have been already implemented in some systems [17, 18], however none of these have achieved computation on a scale large enough for practical applications. Under such circumstances, it is said that DQC is one of the most promising candidates for a scalable quantum computer [19]. Moreover, once a practical quantum computer is constructed, it might be cloud computing between a server and end users since quantum computers are highly expensive and the size

of the computer will be large. A secure protocol using quantum communication between the server and the end users is proposed by [20], which can be regarded as DQC over the server and the end users. Second, quantum cryptography using quantum communication [11, 12], which can be regarded as DQC in our definition, is a promising technology for a secure society. In fact, some quantum cryptography systems have been already commercialized.

In some DQC tasks such as quantum cryptography, quantum communication between the spatially separated quantum systems is an indispensable subroutine. Quantum communication is also an essential resource for DQC for computation to obtain an advantage of quantum mechanical effects since DQC without quantum communication, namely, DQC consisting of a constant size of separated quantum systems connected by just classical communication can be efficiently simulated by classical computers². If we need to perform quantum communication by transmitting a quantum state through a quantum channel with small capacity, DQC has to be suspended until all the necessary communications are done, which causes a delay called a *bottleneck*. Quantum communication in DQC is not only transmitting a quantum state from one sender to one receiver via a quantum channel but also transmitting quantum states from many senders to many receivers via a quantum network consisting of quantum channels. When the scale and complexity of a quantum network grow, the collision of communication pathways between the multiple separated quantum systems causes a serious bottleneck problem, limiting the total performance of DQC.

Some bottleneck problems can be resolved when we can optimize quantum communication so that we reduce the frequency in using quantum channels, however, some bottleneck problems cannot be resolved no matter how we challenge to optimize the communication owing to the restriction originating from the laws of physics. For a given quantum network, we can define the performance of quantum communication as the set of possible quantum communication within the laws of physics. The performance of quantum communication may limit the total performance of DQC. In the first part of this thesis, we are going to investigate the first question:

- How does the topology of a quantum network consisting of quantum channels affect the performance of quantum communication?

The performance of quantum communication through a quantum channel from one sender to one receiver has been extensively studied in quantum Shannon theory [25]. Recently, the performance of quantum communication through quantum

²It is shown that there exists an advantage of quantum computation using quantum states with marginal quantum entanglement [21, 22, 23]. However, their protocol allows performing a global unitary operation during computation. In contrast, performing global unitary operations are impossible in DQC without using a quantum channel.

channels from many senders to one receiver, called a multiple-access quantum channel, has been also studied in [26, 27]. They concentrate on how the performance of quantum communication changes when the capacity of quantum channels is changed while the topology of a quantum network consisting of quantum channels is simple and fixed.

How about the performance of quantum communication over a quantum network consisting of quantum channels between many senders, many receivers and intermediate nodes in addition to senders and receivers? A crude idea to tackle this problem is just transmitting packets of compressed quantum states and routing the packets at the intermediate nodes like a mail delivery. However, in [28], it has been shown that processing the packets at the intermediate nodes called *network coding* improves communication performance comparing to routing the packets. In [29, 30], it was shown that the idea of network coding can be used for computation as well as communication, and communication can be regarded as a special case of computation.

By using the technique of network coding, we analyze implementability of a unitary operation over a given quantum network. In this thesis, we concentrate on how the performance of quantum communication (and generally, quantum computation) changes when the topology of a quantum network consisting of quantum bipartite channels is changed while the capacity of the quantum channels is fixed. A unitary operation is an elementary operation in quantum computation and the special class of unitary operations called permutation operations corresponds to transmitting quantum states. For simplicity, we consider quantum channels are noiseless and have 1-qubit capacity. We consider a one-shot scenario, i.e. we are allowed to use a given network only once, and concentrate on a *cluster network*, which is a certain class of the network consisting of intermediate nodes and the same number of senders and receivers. The cluster network is a subclass of *k-pair network*, which has been an actively studied network in both classical network coding and quantum network coding [31, 32, 33, 34]. Analyzing implementability of a unitary operation over the cluster network can reveal a potential of *measurement based quantum computation* (MBQC), an extensively studied model of quantum computation [35].

In the second part of this thesis, Role of entanglement and causal relation in DQC, we are going to investigate the second question:

- What is the role of quantum communication in DQC?

As we mentioned before, quantum communication is indispensable for some DQC tasks and necessary for obtaining a quantum advantage in DQC for computation. However, how quantum communication enhances DQC has not been fully understood yet³. Interpreting the role of quantum communication in a variety of

³For example, it is not obvious whether quantum communication is sufficient for obtaining a

perspectives enriches our understanding DQC and provides a guidance for constructing a new protocol of quantum information processing outperforming the classical counterpart.

Quantum communication can be implemented by quantum teleportation [36] by using *quantum entanglement* and classical communication. An entangled state can be shared by quantum communication and classical communication can be performed by quantum communication. Therefore, a pair of entanglement and classical communication is equivalent to quantum communication. Thus, we investigate the role of quantum entanglement and classical communication in DQC by comparing to another resource substituting them. Replacing one resource by another resource in a specific task is a commonly used method in quantum information science in order to understand a role of the resource as presented in the next section. We summarize what we do in the second part of this thesis in Fig. 1.1.

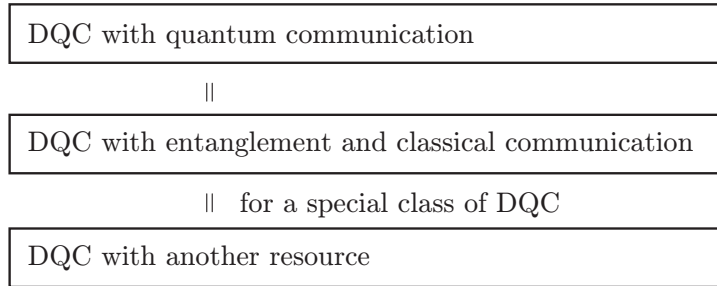


Figure 1.1: **An outline of the second part.** In the second part of this thesis, we investigate another resource substituting entanglement and classical communication (or quantum communication) for a task in a special class of DQC in order to understand a role of entanglement and classical communication in DQC.

1.3 Quantum entanglement

Quantum mechanics exhibits many counter-intuitive phenomena that cannot be described in classical physics. One of such phenomena is the existence of *nonlocal correlations* formulated by Bell and CHSH [37]. They have shown that a quantum mechanical state called an *entangled state* shared between spatially separated two parties can produce strong correlations that can never be achieved by any laws of physics based on local realism, e.g. classical mechanics. That is, entanglement has

quantum advantage in DQC for computation. This consideration is rooted in an open problem, whether quantum computation is strictly faster than classical computation.

a power to enhance correlation in space. However, entanglement shared between spacelike separated parties cannot be used for communication between the parties. Indeed, Popescu and Rohrlich [38] have shown that the nonlocal correlations in quantum mechanics is strictly weaker than correlations imposed by the no-signaling condition based on the law of causality of special relativity. For communication, two parties have to be within a distance where light can travel, namely, *timelike* separated in both quantum and classical cases.

A power of entanglement concerning time also arises when it is accompanied by classical communication. Quantum teleportation [36] is one of the examples. Quantum teleportation is a protocol to transmit quantum information represented by an arbitrary and unknown quantum state from a party (sender) to another timelike separated party (receiver) by using shared entanglement and classical communication from the sender to the receiver. As for transmitting quantum information, quantum teleportation achieves the same goal of direct quantum communication of quantum information, for example, directly sending a photon encoding quantum information through an optical fiber. But there is an interesting extra property concerning a time-line of events in quantum teleportation. Quantum communication between the parties (or quantum communication from a mediating third party to both two parties) is necessary in quantum teleportation to share a fixed entangled state between the sender and receiver, but this event can be done ahead of time before the event that the sender decides what quantum information to send. The time-limit of the event of the decision is determined by the timing of classical communication. In contrast in direct quantum communication, the event of decision should be before the event of quantum communication. Thus we can slightly “dodge” the time-line of the event of quantum communication in transmitting quantum information by using entanglement and classical communication. This observation is summarized in Fig. 1.2.

These two examples reveal aspects of the power of entanglement concerning space and time. The power of entanglement can be also understood by analyzing how much entanglement is consumed in a specific information processing task. For example, entanglement is indispensable for some information processing tasks, such as a specific type of quantum cryptography [12], quantum teleportation [36] and super dense coding [39]. It is considered to be necessary for giving quantum advantage in computation [40, 41] and enhances performances in several information processing tasks, such as classical communication [46] and communication complexity tasks [47, 48]. Analyzing the cost for replacing entanglement by another resource in a specific information processing task [46, 48] is another way to understand the power of entanglement.

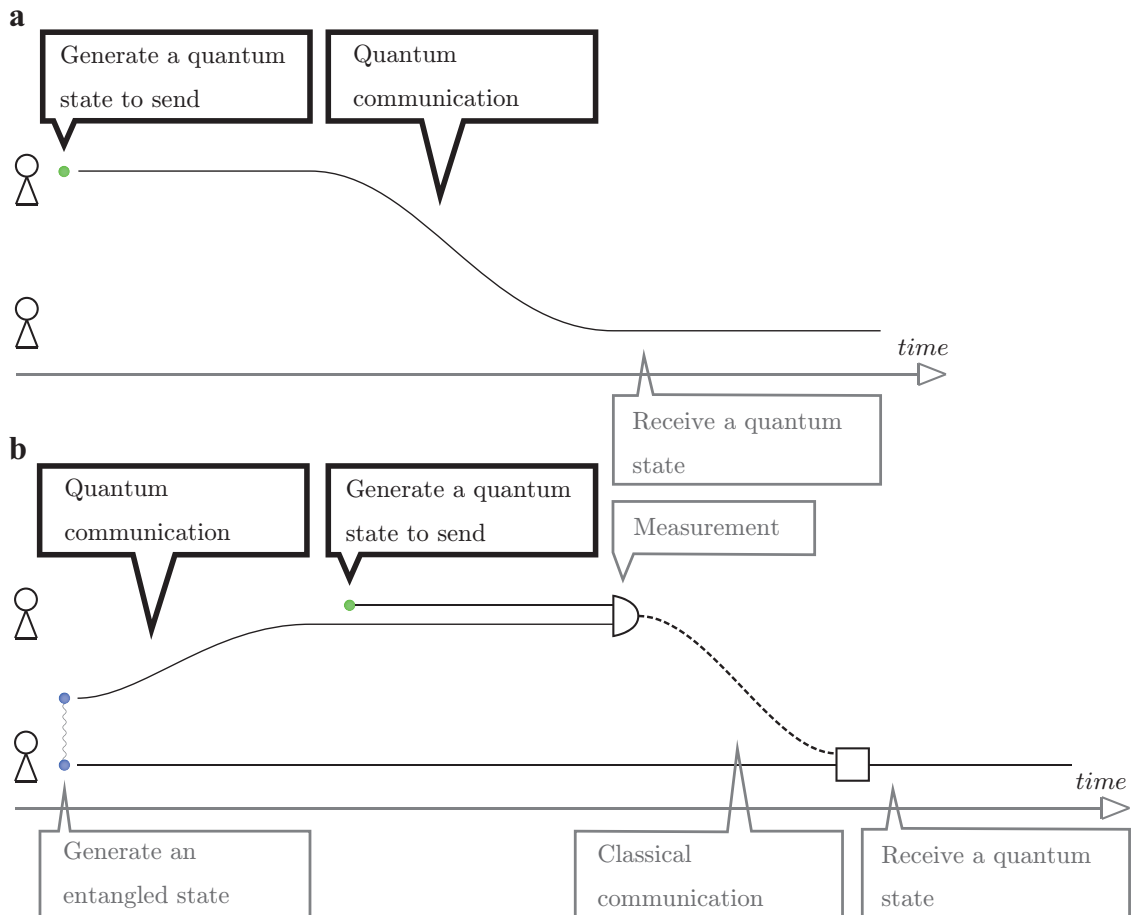


Figure 1.2: **A time-line of events.** (a) A time-line of events in direct quantum communication. The event of decision of what quantum information to send should be before the event of quantum communication. (b) A time-line of events in quantum teleportation. The event of decision can be after the event of quantum communication but should be before the event of classical communication. The detail protocol is shown in Fig. 2.3.

1.4 Space and time

Spacetime is considered as the background of our description of nature in classical physics and standard quantum field theory, and is considered as dynamically interacting with energy in general relativity. The difference in the treatment of spacetime is one of the reasons why the unification of quantum mechanics and general relativity into quantum gravity is difficult [49]. Space and time are also important notions in computer science. Time complexity (necessary time to compute a problem), space complexity (necessary amount of the memory size to compute a problem) and a tradeoff between them have been extensively studied [50, 51].

DQC can be considered as a joint quantum operation of several parties implemented by connecting each party's quantum operation on a separated system well localized in a spacetime coordinate by using given resources, such as quantum communication, entanglement and classical communication. For simplicity, we consider DQC between two parties, however, a generalization into several parties is straightforward. We regard each local operation at a spacetime coordinate belonging to one of the two parties. Quantum communication and classical communication can connect two local operations at timelike separated spacetime coordinates linking the output and input of the two operations. Special relativistic causality introduces a partial order between all the local operations by their spacetime coordinates. We consider local operations are totally ordered since the partial order can be always extended to a total order. Entanglement can be shared between any two spacetime coordinates if we assume that entanglement was generated at a spacetime coordinate far in the past, and it has been distributed from that spacetime coordinate. Since quantum communication can be replaced by quantum teleportation using entanglement assisted classical communication, local operations can be connected by using entanglement and classical communication. Some of entanglement is shared between different parties and some of entanglement is shared within each party. We consider a resource substituting entanglement shared between different parties and classical communication between them to understand the role of *global* resources. Examples of a joint quantum operation in DQC is given in Fig. 1.3.

The first idea for the alternative resource substituting entanglement and classical communication in DQC is *less* entanglement but *more* classical communication. If we are allowed to use more classical communication, it might be possible to reduce the entanglement usage. We analyze the cost for substituting entanglement by classical communication in a certain DQC task, *local state discrimination*, which has been extensively studied in quantum information science [42, 43, 45, 44]. Entanglement can be considered as spatial resource since it can generate spatial quantum correlation. On the other hand, the rounds of classical communication between two parties can be considered as temporal resource. We show that increas-

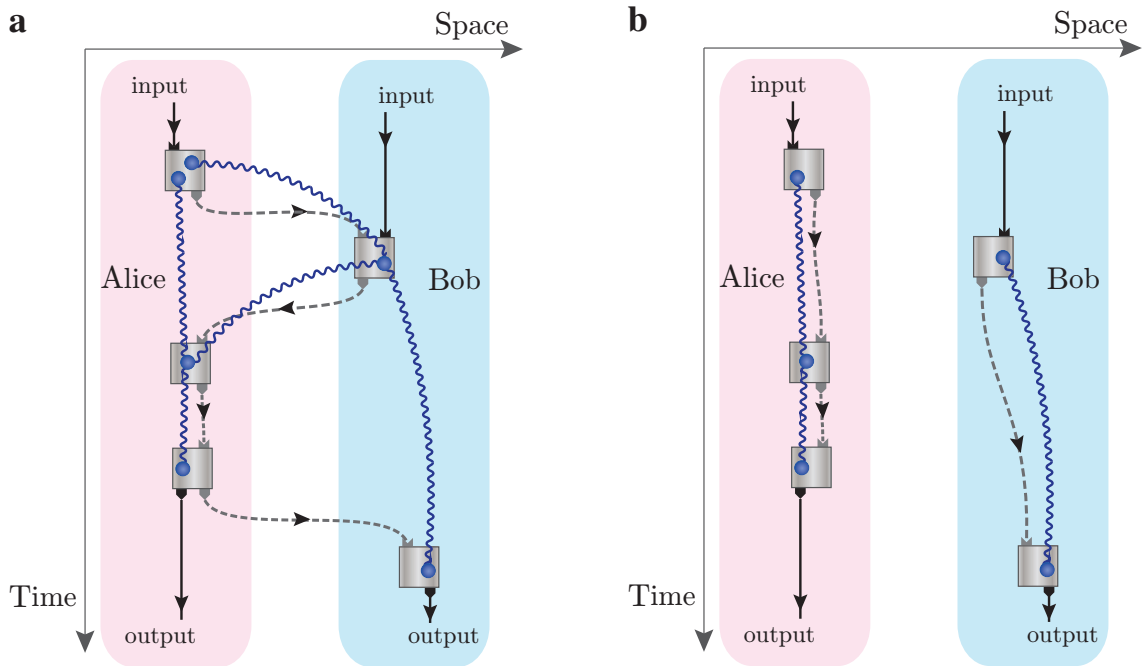


Figure 1.3: **Joint quantum operations in DQC.** Dotted arrows represent classical communication between local operations and circles connected by wavy lines represent entangled states between local operations. A box represents a local operation. The first party and the second party is named Alice and Bob, respectively. Entanglement shared between different parties and classical communication between them can be regarded as global resources. (a) A joint quantum operation in DQC with global resources, . (b) A joint quantum operation in DQC without global resources. We investigate a resource substituting global resources consumed in a joint quantum operation.

ing the temporal resource enables decreasing the spatial resource, equivalently, increasing the spatial resource enables decreasing the temporal resource, which can be interpreted as a power of entanglement for parallelizing information processing. Analyzing the cost for substituting entanglement by classical communication in other tasks are also investigated in [46, 48].

The set of quantum operations in DQC implementable without entanglement between the parties but with classical communication between them is equivalent to a class of quantum operations called *local operations and classical communication* (LOCC) [52, 53, 54, 55], which is widely used in quantum information for investigating entanglement and nonlocal properties. Thus, if an operation implementable in DQC is an element of LOCC, entanglement consumed in DQC can be replaced by classical communication by definition. That is, we can substitute a global *quantum* resource, entanglement, by a completely *classical* resource, classical communication. Can we substitute entanglement by a completely ‘classical’ resource in DQC when we want to implement a quantum operation which is not an element of LOCC? To study this question, we should clarify implicit assumptions made for classical communication and find out a way for generalization.

Classical communication can connect timelike separated local operations, which implies that special relativistic causality restricts the performance of classical communication, and the total performance of DQC. However, the performance of classical communication and the total performance of DQC might be changed in the general relativistic spacetime, which allows *closed timelike curves* (CTC) as a solution of Einstein’s field equations of gravitation, where we cannot define a partial order between spacetime coordinates [56]. In 1957, Richard Feynman gave the argument as follows: how can we analyze the gravitational field provided by a ball whose position is put into a quantum mechanical superposition? [57] Such an argument even implies the possibility of realizing a quantum mechanical superposition of spacetime structures if we crudely combine a consequence of quantum mechanics and general relativity.

Since the existence of the partial order of local operations in the spacetime may not be a fundamental requirement of nature, alternative representations of communication that are not based on the assumption of (the existence of) the partial order have been proposed [58, 61]. And it has been shown that there is a possibility of performing joint quantum operations without fixing the partial order of local operations [58, 59, 60] in the framework of quantum mechanics. The partial order of the spacetime coordinates are referred to as *causal order* in [58, 59, 60]. Note that they have not tried to analyze quantum mechanics in a curved spacetime [62] in this framework, but tried to construct an purely operational formalism without an assumption of the causal order introduced by special relativity but still consistent within standard quantum mechanics. Such a challenge would reveal

a potential of quantum mechanics and deepen our conceptual understanding of quantum mechanics and causality. Furthermore, such *causally neutral* frameworks give a new insight into existing quantum information processing which have been described by the operational formalism implicitly respecting special relativistic causality.

In this thesis, we extend classical communication in such a way that we generalize classical communication into a causal relation between the classical outputs and classical inputs of the local operations, which we call “*classical communication*” *without predefined causal order* denoted by CC^* . We name a new class of deterministic quantum operations in DQC with CC^* but still within quantum mechanics by $LOCC^*$. We show that $LOCC^*$ is equivalent to a certain class of deterministic quantum operations in DQC with entanglement and classical communication known as *separable operations* denoted by SEP [63], which has been introduced for mathematical simplicity to analyze nonlocal quantum tasks in place of LOCC. Note that there exist elements in SEP that are *not* implementable by LOCC [43, 44, 45, 64]. That is, if a quantum operation in DQC is an element of SEP but not an element of LOCC, the alternative classical resource is described by CC^* . Conventionally two assumptions are put on local operations: (a) they are partially ordered and (b) the choice of a local operation does not depend on resources connecting the local operation. However, when we substitute entanglement consumed in LOCC implementing an element in SEP by a completely ‘classical’ resource, CC^* is needed and the two assumptions of local operations have to be relaxed. Our perspective of understanding the power of entanglement also gives a new characterization of the gap between SEP and LOCC, which has not been well understood [55].

By considering the correspondence between $LOCC^*$ and a probabilistic version of LOCC called stochastic LOCC (SLOCC), we analyze the power of $LOCC^*$ in terms of enhancing the success probability of probabilistic operations in SLOCC. We also investigate the relationship between $LOCC^*$ and the quantum process formalism for joint quantum operations without partial order developed in [58]. Furthermore, we give an example of the quantum operation which is an element of SEP but not an element of LOCC. Entanglement and classical communication within special relativistic spacetime are necessary to perform such an operations, but by using CC^* , entanglement is not necessary.

1.5 Organization of this thesis

This thesis is composed of four parts.

In Part I, we review fundamental formulations of quantum mechanics and quantum information theory. In Section 2.3, we review the most general physical pro-

cess described by a quantum instrument and two mathematical ways to represent the quantum instrument: the Kraus representation and the Choi-Jamiolkowski representation, which are extensively used in this thesis. In Section 2.4, we review a model of quantum computation called the circuit model, and its graphical representation. In Section 2.5, we introduce a class of joint quantum operations called local operations and classical communication (LOCC) and related classes of LOCC called stochastic LOCC (SLOCC) and separable operations (SEP).

In Part II, we study how to improve the performance of quantum computation over a given quantum network resource by analyzing entanglement resources represented by quantum networks. In Chapter 3, we review network coding theory, a model of quantum computation called measurement based quantum computation (MBQC) and classifications of unitary operations in terms of the Kraus-Cirac decomposition and the operator Schmidt decomposition. In Chapter 4, we give a definition of a (k, N) -cluster network and analyze implementability of a k -qubit unitary operation over the cluster network in both a deterministic scenario and a probabilistic scenario. We also analyze implementability of a two-qubit unitary operation over the butterfly, grail and square networks.

In Part III, we study the role of quantum communication in DQC in terms of entanglement and causal relation in classical communication. We investigate resources substituting entanglement and classical communication consumed in entanglement assisted LOCC. In Chapter 6, we analyze the amount of the entanglement resource required for a specific DQC task known as local state discrimination. In Chapter 7, we develop a new framework to describe deterministic joint quantum operations in two-party DQC by using “classical communication” without predefined causal order denoted by CC^* . We show that $LOCC^*$ is equivalent to SEP. We also investigate the relationship between $LOCC^*$, SLOCC and quantum processes. By using $LOCC^*$, we give an element that resides in the gap between SEP and LOCC.

In Part IV, we summarize the results and outlooks.

Chapter 2

Preliminaries

2.1 Notation

The following notation will be used throughout this thesis.

\bar{a}	the complex conjugate of a .
a^T	the transpose of a . The transpose is basis dependent.
a^\dagger	the conjugate transpose of a .
\mathcal{H}	a finite dimensional Hilbert space.
$\mathbf{L}(\mathcal{H})$	the set of linear operators.
\mathbb{I}_A	the identity operator on \mathcal{H}_A .
$\mathbf{U}(\mathcal{H})$	the set of unitary operators. $\mathbf{U}(\mathcal{H}) = \{M \in \mathbf{L}(\mathcal{H}) M^\dagger M = \mathbb{I}\}$.
\mathbf{U}_c	the set of unitary operators locally unitarily equivalent to a two-qubit controlled phase operator.
$\mathbf{Pos}(\mathcal{H})$	the set of positive semi-definite operators. $\mathbf{Pos}(\mathcal{H}) = \{M \in \mathbf{L}(\mathcal{H}) M \geq 0\}$.
tr	the trace of a linear operator.
det	the determinant of a linear operator.
$\mathbf{D}(\mathcal{H})$	the set of density operators. $\mathbf{D}(\mathcal{H}) = \{M \in \mathbf{Pos}(\mathcal{H}) \text{tr}[M] = 1\}$.
$\mathbf{L}(\mathcal{H}_A : \mathcal{H}_B)$	the set of linear operators. $\mathbf{L} : \mathcal{H}_A \rightarrow \mathcal{H}_B$.
$\mathbf{C}(\mathcal{H}_A : \mathcal{H}_B)$	the set of linear CPTP maps. $\mathbf{C} : \mathbf{L}(\mathcal{H}_A) \rightarrow \mathbf{L}(\mathcal{H}_B)$
$\mathbf{U}(\mathcal{H}_A : \mathcal{H}_B)$	the set of isometry operators. $\mathbf{U}(\mathcal{H}_A : \mathcal{H}_B) = \{M \in \mathbf{L}(\mathcal{H}_A : \mathcal{H}_B) M^\dagger M = \mathbb{I}_A\}$.
$\text{Sch}\#_B^A(\psi\rangle)$	the Schmidt rank of $ \psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.
$\text{Op}\#_B^A(M)$	the operator Schmidt rank of $M \in \mathbf{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$.
$\text{KC}\#(U)$	the Kraus-Cirac number of a two qubit unitary operator $U \in \mathbf{U}(\mathbb{C}^2 \otimes \mathbb{C}^2)$.

2.2 Quantum information theory

In this section, we review fundamental formulations of quantum mechanics and quantum information theory.

2.2.1 Quantum mechanics

Postulate 1 A state of a physical system can be described by a vector in a *Hilbert space*.

A Hilbert space is a complex inner product space and is also a complete metric space with respect to the distance function induced by the inner product. An example of Hilbert space is \mathbb{C}^n with respect to the inner product function $(x, y) = \sum_{i=1}^n \bar{x}_i y_i$, where \bar{a} represents the complex conjugate of a . In this thesis, we only consider the cases with a finite d -dimensional Hilbert space denoted by \mathbb{C}^d for the reason quoted by Giulio Chiribella et al. [65] as follows.

”Another contribution of quantum information has been to shift the emphasis to finite dimensional systems, which allow for a simpler treatment but still possess all the remarkable quantum features. In a sense, the study of finite dimensional systems allows one to decouple the conceptual difficulties in our understanding of quantum theory from the technical difficulties of infinite dimensional systems.”

Consider a system A described by the Hilbert space \mathcal{H}_A . We denote a vector in the Hilbert space \mathcal{H}_A by $|\psi\rangle$. We often denote the state by

$$|\psi\rangle_{\mathcal{H}_A} \text{ or } |\psi\rangle_A \tag{2.1}$$

in order to specify the Hilbert space or the system that the state belongs to. We call a two-dimensional Hilbert space a *qubit*, which is analogous to a classical bit. Although the degree of freedom for a qubit is larger than that of a bit, the amount of encodable classical information in a qubit is as same as that to a bit [66].

Postulate 2 The Hilbert space of a composite physical system consisting of distinct physical systems is given by the tensor product of the Hilbert spaces of the component physical systems.

Consider two systems A and B with respective their Hilbert spaces \mathcal{H}_A and \mathcal{H}_B . If the system A is in state $|\psi\rangle_A$ and the system B in state $|\phi\rangle_B$, the state of total system is given by

$$|\psi\rangle_A \otimes |\phi\rangle_B. \tag{2.2}$$

We often use the abbreviated notation $|\psi\rangle_A|\phi\rangle_B$, $|\psi\phi\rangle_{AB}$ or $|\psi, \phi\rangle_{AB}$. If the state of a composite system can be described in the form of Eq.(2.2), the state is called a *product state* or a *separable state*. If for any $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$ we have

$$|\Psi\rangle_{AB} \neq |\psi\rangle_A|\phi\rangle_B, \quad (2.3)$$

then the state $|\Psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called an *entangled state*. For example, an entangled state,

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \quad (2.4)$$

is called an *EPR state* named after Einstein, Podolsky and Rosen [67], where $\{|0\rangle, |1\rangle\}$ is the computational basis.

Postulate 3 Any time evolution of a state of a closed quantum system is described by a *unitary operator* that corresponds to the time evolution operator of the Hamiltonian of the system.

The state $|\psi\rangle \in \mathcal{H}$ of the system at time t_1 is related to the state $|\psi'\rangle \in \mathcal{H}$ of the system at time t_2 by a unitary operator $U \in \mathbf{U}(\mathcal{H})$,

$$|\psi'\rangle = U|\psi\rangle. \quad (2.5)$$

When we control the time evolution of a quantum system that is described by a unitary operator U , we regard that a unitary operation U is performed or implemented.

Postulate 4 Quantum measurements on a system with Hilbert space \mathcal{H} are described by *Positive Operator-Valued Measure* (POVM), a set of positive semi-definite operators $\{M_m \in \mathbf{Pos}(\mathcal{H})\}_{m \in \Omega}$ satisfying the *completeness equation*,

$$\sum_{m \in \Omega} M_m = \mathbb{I}, \quad (2.6)$$

where m corresponds to an index of the possible measurement outcomes. When we measure a state $|\psi\rangle \in \mathcal{H}$ by $\{M_m\}_{m \in \Omega}$, we obtain outcome m with probability

$$p(m) = \langle \psi | M_m | \psi \rangle. \quad (2.7)$$

When we perform a quantum measurement described by a POVM whose elements are projection operators, i.e. $M_m^2 = M_m$ for all m , the measurement is said to be a *projective measurement* $\{M_m\}_{m \in \Omega}$.

If we do not have complete knowledge about a state of a quantum system but know a set of possible states $\{|\psi_i\rangle\}_i$ and their probabilities $\{p(i)\}_i$, or an *ensemble*

of states $\{p(i), |\psi_i\rangle\}_i$, such a state is described by using a *density operator* given by

$$\rho = \sum_i p(i) |\psi_i\rangle\langle\psi_i|. \quad (2.8)$$

A density operator is an operator on a Hilbert space that is non-negative and has trace equal to one. Ensembles of states and density operators are not in one-to-one correspondence. We cannot distinguish states representing different ensembles which are described by the same density operator. So the density operator determines the state of a physical system. The state is called to be *pure* if and only if the state can be represented by a vector in the Hilbert space, that is, the rank of the density operator is one, otherwise the state is said to be *mixed*. The state of a subsystem of a composite quantum system is provided by the *reduced density operator*. Suppose we have physical systems A and B , whose composite state is described by a density operator ρ_{AB} . The reduced density operator for system A is given by

$$\rho_A = \text{tr}_B[\rho_{AB}] := \sum_i \langle i|_B \rho_{AB} |i\rangle_B, \quad (2.9)$$

where tr_B is a map between operators known as the partial trace over system B , and $\{|i\rangle_B\}_i$ is an orthonormal basis of the Hilbert space of system B . Note that the trace operation does not depend on the orthonormal basis. The definition of the entangled state is generalized for mixed states as follows. If the state of a composite system ρ_{AB} is described by

$$\rho_{AB} = \sum_i p(i) \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad (2.10)$$

where $\rho_A^{(i)} \in \mathbf{D}(\mathcal{H}_A)$, $\rho_B^{(i)} \in \mathbf{D}(\mathcal{H}_B)$ and $p(i)$ is a probability distribution, the state is called a separable state. If not, the state is called an entangled state.

It is possible to reformulate the postulates of quantum mechanics in terms of density operators instead of state vectors.

Postulate 1' A state of a physical system can be completely described by a density operator $\rho \in \mathbf{D}(\mathcal{H})$.

Postulate 2' The state of the composite physical system is given by $\rho \in \mathbf{D}(\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n)$, where $\{\mathcal{H}_i\}_i$ are Hilbert spaces of the component physical systems.

Postulate 3' The time evolution of a closed quantum system is given by $U\rho U^\dagger$, where $U \in \mathbf{U}(\mathcal{H})$.

Postulate 4' Quantum measurements are described by a POVM $\{M_m \in \mathbf{Pos}(\mathcal{H})\}_{m \in \Omega}$. An outcome m is obtained with probability

$$p(m) = \text{tr}[M_m \rho]. \quad (2.11)$$

When we perform a quantum measurement on a subsystem \mathcal{H}_A of a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ described by a POVM $\{M_m \in \mathbf{Pos}(\mathcal{H}_A)\}_{m \in \Omega}$, the probability obtaining outcome m is given by

$$p(m) = \text{tr}[(M_m \otimes \mathbb{I}_B)\rho_{AB}], \quad (2.12)$$

and the state of the unmeasured system after the measurement is given by

$$\frac{1}{p(m)} \text{tr}_A[(M_m \otimes \mathbb{I}_B)\rho_{AB}]. \quad (2.13)$$

2.2.2 Schmidt decomposition

Suppose $|\psi\rangle_{AB}$ is a vector in a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. There exists a set of orthonormal vectors $\{|i\rangle_A \in \mathcal{H}_A\}_i$ and a set of orthonormal vectors $\{|i\rangle_B \in \mathcal{H}_B\}_i$ such that

$$|\psi\rangle_{AB} = \sum_i \lambda_i |i\rangle_A |i\rangle_B, \quad (2.14)$$

where $\{\lambda_i\}_i$ are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$, known as *Schmidt co-efficients*. The number of non-zero coefficients $|\{\lambda_i > 0\}|$ is called as the *Schmidt rank* and denoted by $\text{Sch}\#_B^A(|\psi\rangle_{AB}) = |\{\lambda_i > 0\}|$.

2.3 Quantum operations

A quantum operation is the most general physical process, consisting of unitary evolutions, measurements, discarding subsystems and attaching other subsystems, called *ancilla systems*. It represents any realizable physical process that a quantum system can undergo.

Mathematically, a quantum operation can be represented by a *quantum instrument*, which is described by a set of linear maps $\{\mathcal{M}_o : \mathbf{L}(\mathcal{H}_{in}) \rightarrow \mathbf{L}(\mathcal{H}_{out})\}_o$ that transforms a quantum input state $\rho \in \mathbf{D}(\mathcal{H}_{in})$ to a quantum output state given by

$$\frac{1}{p(o)} \mathcal{M}_o(\rho) \quad (2.15)$$

associated with a classical output o ($o = 1, 2, \dots, n$) with a probability distribution

$$p(o) = \text{tr}[\mathcal{M}_o(\rho)]. \quad (2.16)$$

If we discard the classical output, a quantum output state is given by

$$\sum_o \mathcal{M}_o(\rho). \quad (2.17)$$

Each element of instrument \mathcal{M}_o has to be a linear *completely positive* (CP) map and a sum of elements $\sum_o \mathcal{M}_o$ has to be a *trace preserving* (TP) map to describe quantum operations allowed in quantum mechanics. A quantum operation conditioned by a classical input i is denoted by $\{\mathcal{M}_{o|i}\}_o$, a quantum operation without classical output is denoted by $\mathcal{M}_{|i}$ and a quantum operation without classical input and output is denoted by \mathcal{M} . $\mathcal{M}_{|i}$ and \mathcal{M} are called deterministic quantum operations, which are described by linear CPTP maps. We define a set of linear CPTP maps from $\mathbf{L}(\mathcal{H}_{in})$ to $\mathbf{L}(\mathcal{H}_{out})$ as $\mathbf{C}(\mathcal{H}_{in} : \mathcal{H}_{out})$. Graphical representations of quantum operations are given in Fig 2.1.

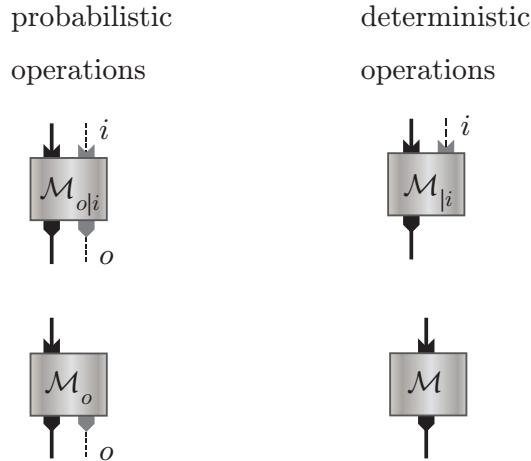


Figure 2.1: **Quantum operations.** Probabilistic operations have a classical output corresponding to an outcome of the measurement. Deterministic operations does not give any classical output.

There are several mathematical ways to represent the quantum instrument [68, 69, 70]. We introduce the Kraus representation and the Choi-Jamiolkowski (CJ) representation, which are mainly used in this thesis. We will show that any quantum instrument is physically realizable, i.e. it can be represented by a sequence of procedures consisting of attaching an ancilla system, applying a unitary time evolution and performing measurement.

Kraus representation

Any quantum instrument $\{\mathcal{M}_o : \mathbf{L}(\mathcal{H}_{in}) \rightarrow \mathbf{L}(\mathcal{H}_{out})\}_o$ can be represented by

$$\mathcal{M}_o(\rho) = \sum_k E_{k,o} \rho E_{k,o}^\dagger, \quad (2.18)$$

where $E_{k,o} \in \mathbf{L}(\mathcal{H}_{in} : \mathcal{H}_{out})$ satisfying $\sum_{k,o} E_{k,o}^\dagger E_{k,o} = \mathbb{I}_{in}$ are called *Kraus operators*. A deterministic quantum operation, a quantum instrument without classical output, $\{\mathcal{M} : \mathbf{L}(\mathcal{H}_{in}) \rightarrow \mathbf{L}(\mathcal{H}_{out})\}$ is a CPTP map,

$$\mathcal{M}(\rho) = \sum_k E_k \rho E_k^\dagger, \quad (2.19)$$

where $E_k \in \mathbf{L}(\mathcal{H}_{in} : \mathcal{H}_{out})$ satisfies $\sum_k E_k^\dagger E_k = \mathbb{I}_{in}$. We denote the set of all such CPTP maps by $\mathbf{C}(\mathcal{H}_{in} : \mathcal{H}_{out})$. If the quantum operation is deterministic and the number of Kraus operators is one, that is

$$\mathcal{M}(\rho) = E \rho E^\dagger, \quad (2.20)$$

where $E \in \mathbf{L}(\mathcal{H}_{in} : \mathcal{H}_{out})$ satisfies $E^\dagger E = \mathbb{I}_{in}$. Such E are called an *isometry operator*, and the set of all such isometry operators are denoted by $\mathbf{U}(\mathcal{H}_{in} : \mathcal{H}_{out})$. When $\dim(\mathcal{H}_{in}) = \dim(\mathcal{H}_{out})$, an isometry operator is equivalent to a unitary operator.

Choi-Jamiolkowski (CJ) representation

In Part III, we extensively use the CJ representation to represent quantum operations given by quantum instruments. For a map representing an element of a quantum instrument $\mathcal{M}_{o|i} : \mathbf{L}(\mathcal{H}_{in}) \rightarrow \mathbf{L}(\mathcal{H}_{out})$ where i is an index of the classical input and o is an index of the classical output, the corresponding CJ operator $M_{o|i} \in \mathbf{L}(\mathcal{H}_{in} \otimes \mathcal{H}_{out})$ is given by

$$M_{o|i} = \sum_{k,l} |k\rangle\langle l| \otimes \mathcal{M}_{o|i}(|k\rangle\langle l|), \quad (2.21)$$

where $\{|k\rangle\}_k$ is the computational basis on \mathcal{H}_{in} . The state of a quantum output for a quantum input ρ_{in} by a linear map $\mathcal{M}_{o|i}$ is obtained by using the CJ operator $M_{o|i}$ as

$$\mathcal{M}_{o|i}(\rho_{in}) = \text{tr}_{in}[M_{o|i}(\rho_{in}^T \otimes \mathbb{I}_{out})] \quad (2.22)$$

where \mathbb{I}_{out} is the identity operator on \mathcal{H}_{out} and ρ_{in}^T is the transposition of ρ_{in} with respect to the computational basis. Note that the output state does not depend on the choice of the computational basis. $\mathcal{M}_{o|i}$ is completely positive (CP) if and

only if $M_{o|i}$ is a positive semi-definite operator. $\sum_o \mathcal{M}_{o|i}$ is trace preserving (TP) if and only if $\text{tr}_{out}[\sum_o M_{o|i}] = \mathbb{I}_{in}$. The CJ representation is unique, i.e. a quantum instrument and a CJ operator are in one-to-one correspondence, while the Kraus representation is not unique.

Implementation of a quantum instrument

It is known that there exist physical implementations for any quantum instrument.

Proposition 1. *A quantum instrument $\{\mathcal{M}_o : \mathbf{L}(\mathcal{H}_{in}) \rightarrow \mathbf{L}(\mathcal{H}_{out})\}_o$ is physically implementable.*

Proof. We construct a sequence of procedures realizing a physical process represented by the quantum instrument. The sequence consists of attaching an ancilla system, applying unitary time evolution and performing measurement. Let $\{E_{k,o} \in \mathbf{L}(\mathcal{H}_{in} : \mathcal{H}_{out})\}_k$ be a set of Kraus operators of \mathcal{M}_o . First, we prepare an initial state $\rho = \sum_i p_i |x_i\rangle\langle x_i| \in \mathbf{D}(\mathcal{H}_{in})$ and an ancilla system $|0\rangle_R \in \mathcal{H}_R$. Next, we apply a unitary operator $U \in \mathbf{U}(\mathcal{H}_{in} \otimes \mathcal{H}_R)$ such that

$$U|\psi\rangle_{in}|0\rangle_R = \sum_{k,o} (E_{k,o}|\psi\rangle_{in})|k,o\rangle_M \quad (2.23)$$

for all $|\psi\rangle_{in} \in \mathcal{H}_{in}$, where $\{|k,o\rangle_M\}_{k,o}$ is a set of orthonormal vectors in \mathcal{H}_M . Note that the dimension of the ancilla system would be changed since the dimension of \mathcal{H}_{in} and that of \mathcal{H}_{out} are different in general. Thus, we denote the ancilla system after performing the unitary operator by \mathcal{H}_M , satisfying

$$\dim(\mathcal{H}_{in} \otimes \mathcal{H}_R) = \dim(\mathcal{H}_{out} \otimes \mathcal{H}_M). \quad (2.24)$$

We can always construct such a unitary operator U since for any $|\phi\rangle_{in}, |\psi\rangle_{in} \in \mathcal{H}_{in}$,

$$\langle \phi|_{in} \langle 0|_R U^\dagger U |\psi\rangle_{in} |0\rangle_R = \sum_{k,o} \langle \phi|_{in} E_{k,o}^\dagger E_{k,o} |\psi\rangle_{in} \quad (2.25)$$

$$= \langle \phi|\psi\rangle, \quad (2.26)$$

holds. Third, we perform a projective measurement $\{\sum_k |k,o\rangle_M \langle k,o|_M\}_o$ on system \mathcal{H}_M . A measurement outcome o is obtained with probability

$$\begin{aligned} p(o) &= \text{tr} \left[\left(\mathbb{I}_{out} \otimes \sum_k |k,o\rangle_M \langle k,o|_M \right) \sum_{a,b,c,d,i} p_i E_{a,b}|x_i\rangle_{in} \langle x_i|_{in} E_{c,d} \otimes |a,b\rangle_M \langle c,d|_M \right] \\ &= \text{tr} [\mathcal{M}_o(\rho)]. \end{aligned} \quad (2.27)$$

The state in the system \mathcal{H}_{out} after the measurement is given by

$$\frac{1}{p(o)} \text{tr}_M \left[(\mathbb{I}_{out} \otimes \sum_k |k, o\rangle_M \langle k, o|_M) \sum_{a,b,c,d,i} p_i E_{a,b}|x_i\rangle_{in} \langle x_i|_{in} E_{c,d} \otimes |a, b\rangle_M \langle c, d|_M \right] = \frac{1}{p(o)} \mathcal{M}_o(\rho). \quad (2.28)$$

□

2.4 Quantum computation models

Quantum computation is a process to apply a quantum operation on input state and obtain a classical outputs. There are several models to describe the process. We introduce the circuit model in this section and another model, measurement based quantum computation (MBQC) in Section 3.2.

2.4.1 Circuit model

The circuit model of quantum computation describes a quantum operation given by a unitary operation as a combination of *elementary quantum gates*, which corresponds to the elementary logic gates of classical electronic circuits in classical computation [75]. Each wire of a quantum circuit represents a qubit and a sequence of elementary quantum gates are performed on the qubits. In the first stage, we initialize qubits in a particular input state. In the second stage, we apply a unitary operation corresponding to the computation algorithm to the entire input. This differs from classical computation in that unitary ensures the computation is always reversible. In classical computation, irreversible gates such as the AND gate are used, whose inputs cannot be recovered from the output, meaning that some information about the initial state was lost. Another difference with classical computation is the impossibility of perfectly cloning or copying an unknown quantum state [76]. These facts make the construction of quantum algorithms different from that of classical algorithms. In final, output quantum states are measured. We use the circuit notation of quantum operations given in Table 2.1 in this thesis.

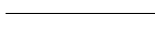



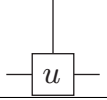
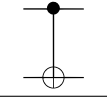
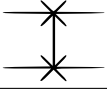
	A wire carrying a single qubit (time goes left to right)
	A wire carrying a single classical bit
	A projective measurement in the <i>computational basis</i> $\{ i\rangle\langle i \}_i$.
	A single unitary gate u .
	A controlled unitary gate $U = 0\rangle\langle 0 \otimes \mathbb{I} + 1\rangle\langle 1 \otimes u$.
	A CNOT gate $U^{CNOT} := 00\rangle\langle 00 + 01\rangle\langle 01 + 10\rangle\langle 11 + 11\rangle\langle 10 $.
	A SWAP operation $U^{SWAP} := 00\rangle\langle 00 + 01\rangle\langle 10 + 10\rangle\langle 01 + 11\rangle\langle 11 $.

Table 2.1: Notation of operations used in quantum circuits.

Single qubit operators are described by 2×2 unitary matrices in the computational basis, of which the Pauli operators

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.29)$$

are often used in this thesis. Any single qubit unitary operator u can be decomposed as

$$u = R_z(\alpha)R_y(\beta)R_z(\gamma), \quad (2.30)$$

where $R_z(\theta) = \exp(-i\frac{\theta}{2}Z)$ and $R_y(\theta) = \exp(-i\frac{\theta}{2}Y)$, which is called the Euler decomposition.

We also introduce the Hadamard gate and the phase gate as

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S := \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \quad (2.31)$$

Useful properties of single qubit operators are often used, such as

$$HXH = Z, \quad SXS^\dagger = Y, \quad (SH)Z(SH)^\dagger = Y. \quad (2.32)$$

For example, these properties are used to easily check,

$$(I \otimes H)U^{CNOT}(I \otimes H) = U^{CZ}, \quad (2.33)$$

where U^{CNOT} is the controlled NOT gate (controlled X gate) given by,

$$U^{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (2.34)$$

and U^{CZ} is the controlled Z gate given by,

$$U^{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (2.35)$$

The controlled NOT gate and the controlled Z gate are special cases of the *controlled unitary* operators. The two-qubit controlled unitary operator U is described by

$$U = |0\rangle\langle 0|_C \otimes \mathbb{I}_T + |1\rangle\langle 1|_C \otimes u_T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{0,0} & u_{0,1} \\ 0 & 0 & u_{1,0} & u_{1,1} \end{pmatrix}, \quad (2.36)$$

where $u = \begin{pmatrix} u_{0,0} & u_{0,1} \\ u_{1,0} & u_{1,1} \end{pmatrix}$ is a single qubit unitary operator. The first system \mathcal{H}_C is called a *controlled qubit* and the second system \mathcal{H}_T is called a *target qubit*. Properties of the controlled unitary operators are shown in Part II.

A unitary operation representing an algorithm in the circuit model can be decomposed into a set of smaller unitary ‘gates’ acting on subsets of qubits. A *universal gate set* is a set of unitary gates into which any unitary operation can be decomposed. There exists a variety of universal gate sets. For example, the two-qubit CNOT gate along with arbitrary single qubit unitary gates form a universal gate set.

2.5 Local Operations and Classical Communication (LOCC)

In this section, we introduce a class of joint quantum operations between distant parties where they cannot directly apply any joint quantum operations, but can transmit classical information to each other depending on the outcomes of local quantum operations on their respective subsystems. Such a class of joint quantum operations are referred to as *local operations and classical communication*, which is

abbreviated to LOCC. We also introduce two classes of joint quantum operations related to LOCC. At the end of this section, we review a more general class of operations implementable by LOCC assisted by pre-shared entanglement.

2.5.1 LOCC

LOCC is a set of deterministic joint quantum operations consisting of a sequence of local quantum operations and classical communication. Probabilistic quantum operations can be also applied in the sequence, however, to make the joint operation to be deterministic, we need to discard (sum up) all the measurement outcomes after all the operations in the sequence are completed. LOCC is widely used in quantum information science for describing practical experimental settings, where global quantum communication is much harder to implement than classical communication. For example, quantifying quantum entanglement [52, 53] and quantifying the globalness of unitary operations [71] are investigated in terms of LOCC. We first introduce the simplest class, bipartite one-way LOCC. Then we introduce a more general class, bipartite two-way LOCC, and present the most general class, multipartite two-way LOCC.

Bipartite one-way LOCC

We consider the scenario that Alice first performs a local operation represented by $\{\mathcal{A}_o\}_o$, then sends a classical output o to Bob and Bob performs a local operation represented by $\mathcal{B}|_o$ conditioned by the classical input o . Since we assume that Alice and Bob are acting on different quantum systems at different spacetime coordinates, the joint quantum operation is described by a tensor product of two local operations. By taking averages over o , we obtain a deterministic joint quantum operation given by

$$\mathcal{M} = \sum_o \mathcal{A}_o \otimes \mathcal{B}|_o. \quad (2.37)$$

One-way LOCC from Alice to Bob is the set of quantum operations in the form of Eq.(2.37). One-way LOCC from Bob to Alice can be defined in a similar way.

Bipartite two-way LOCC

A deterministic joint operation represented by local operations and more general two-way (finite-round) classical communication between two parties is defined by a sequence of Alice's local operations given by $\{\mathcal{A}_{o_N|i_N}^{(N)} \circ \dots \circ \mathcal{A}_{o_1}^{(1)}\}_{o_N, \dots, o_1}$ and another sequence of Bob's local operations given by $\{\mathcal{B}_{|i'_N}^{(N)} \circ \dots \circ \mathcal{B}_{o'_1|i'_1}^{(1)}\}_{o'_N, \dots, o'_1}$. Here \circ denotes a connection between two local operations linking a quantum output of a local operation and a quantum input of the next local operation. The indices i_k

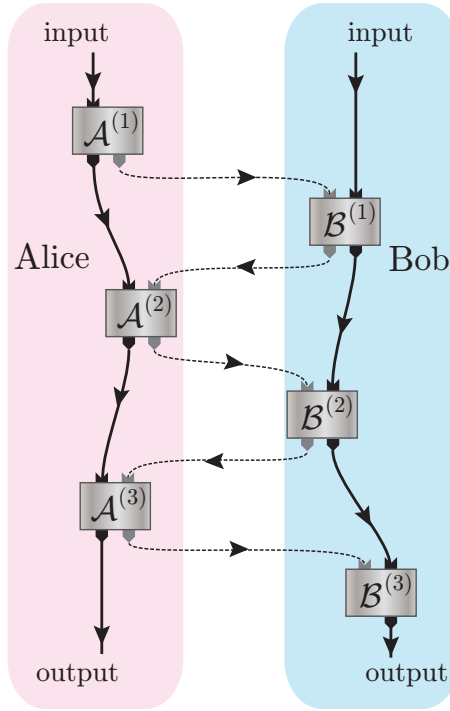


Figure 2.2: **A bipartite LOCC protocol.** Dotted arrows represent classical communication between local operations and solid arrows represent quantum communication between local operations. A box represents a local operation.

and i'_k are classical inputs of the k -th operations and o_k and o'_k are classical outputs of the k -th operations of Alice and Bob, respectively. We assume that Alice sends o_1 to Bob and Bob receives the classical message as i'_1 , i.e. $i'_1 = o_1$, and similarly, Bob sends o'_1 to Alice and so on. Thus, bipartite two-way LOCC between the two parties is defined by a set of joint quantum operations represented by

$$\mathcal{M} = \sum_{i_2, \dots, i_N, o_1, \dots, o_N} \mathcal{A}_{o_N | i_N}^{(N)} \circ \dots \circ \mathcal{A}_{o_1}^{(1)} \otimes \mathcal{B}_{|o_N}^{(N)} \circ \dots \circ \mathcal{B}_{i_2 | o_1}^{(1)}. \quad (2.38)$$

An example for $N = 3$ is shown in Fig.2.2. We refer to bipartite two-way LOCC as just bipartite LOCC.

Multipartite two-way LOCC

We consider a situation in which multiple (more than two) parties collectively perform local operations, depending on the outcomes of the previous operations. A set of such deterministic joint quantum operations is the most general LOCC,

called multipartite two-way LOCC. We denote multipartite two-way LOCC as $\mathbf{LOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N})$, where there are N parties and a sequence of local operations performed by the i -th party denoted by a quantum operation from $\mathbf{L}(\mathcal{H}_{I_i})$ to $\mathbf{L}(\mathcal{H}_{O_i})$. Since an element of LOCC is a deterministic quantum operation by definition, we obtain

$$\mathbf{LOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}) \subsetneq \mathbf{C}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{I_N} : \mathcal{H}_{O_1} \otimes \dots \otimes \mathcal{H}_{O_N}). \quad (2.39)$$

In this thesis, we refer to multipartite two-way LOCC as just LOCC. Note that local operations in LOCC are totally ordered.

2.5.2 Separable operation

We introduce a *separable operation*, which does not describe a physical process but a mathematically conceptual process [63]. In spite of its clear operational meaning, analysis of quantum information processing tasks under the restriction of LOCC is hard in general since the mathematical structure of LOCC is highly complicated [55]. The separable operation is known to be used to analyze nonlocal quantum tasks in place of LOCC [72, 73, 97] since it has a simpler mathematical structure than LOCC and the class of separable operations is a slightly larger class of deterministic quantum operations than LOCC. However, only limited number of examples of deterministic quantum operations that are separable operations but *not* included in LOCC are known so far [43, 44, 45, 64].

Definition 1. A CPTP map $\Phi \in \mathbf{C}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{I_N} : \mathcal{H}_{O_1} \otimes \dots \otimes \mathcal{H}_{O_N})$, is said to be a separable operation, if and only if there exists linear operators $\{E_k^{(1)} \in \mathbf{L}(\mathcal{H}_{I_1}, \mathcal{H}_{O_1})\}, \dots, \{E_k^{(N)} \in \mathbf{L}(\mathcal{H}_{I_N}, \mathcal{H}_{O_N})\}$ such that

$$\Phi(\rho) = \sum_k (E_k^{(1)} \otimes \dots \otimes E_k^{(N)}) \rho (E_k^{(1)} \otimes \dots \otimes E_k^{(N)})^\dagger \quad (2.40)$$

for all $\rho \in \mathbf{D}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{I_N})$. We refer to the set of separable operations as SEP and denote as $\mathbf{SEP}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N})$.

Following relations are obtained by definition of each class.

$$\mathbf{LOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}) \subsetneq \mathbf{SEP}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}), \quad (2.41)$$

$$\mathbf{SEP}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}) \subsetneq \mathbf{C}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{I_N} : \mathcal{H}_{O_1} \otimes \dots \otimes \mathcal{H}_{O_N}). \quad (2.42)$$

2.5.3 Stochastic LOCC

Stochastic LOCC (SLOCC) is a set of probabilistic joint quantum operations consisting of a sequence of local quantum operations and classical communication. It is not necessary to average over all the measurement outcomes in SLOCC in contrast to LOCC. Bipartite SLOCC is defined by a set of linear CP maps represented by

$$\mathcal{M} = \sum_{(i_1, \dots, i_N, o_1, \dots, o_N) \in \mathbb{M}} \mathcal{A}_{o_N | i_N}^{(N)} \circ \dots \circ \mathcal{A}_{o_1}^{(1)} \otimes \mathcal{B}_{|o_N}^{(N)} \circ \dots \circ \mathcal{B}_{i_2 | o_1}^{(1)}, \quad (2.43)$$

where \mathbb{M} is a subset of the set of all the measurement outcomes $\overline{\mathbb{M}}$. Note that an element of SLOCC is not necessary to be TP. For an input state ρ , the probability of obtaining a map in SLOCC \mathcal{M} is given by

$$\text{tr}[\mathcal{M}(\rho)], \quad (2.44)$$

and the final state after post-selection is given by

$$\frac{\mathcal{M}(\rho)}{\text{tr}[\mathcal{M}(\rho)]}. \quad (2.45)$$

We denote multipartite SLOCC as $\mathbf{SLOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N})$. By definition, SLOCC is strictly larger than LOCC, i.e.

$$\mathbf{LOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}) \subsetneq \mathbf{SLOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}). \quad (2.46)$$

In a practical experimental setting, it is not difficult to perform post-selection in a LOCC protocol, which gives a SLOCC protocol, and such a probabilistic operation has a stronger power than a deterministic operation, such as increasing entanglement, discriminating non-orthonormal states perfectly, and enhancing the computational power [74].

We can show that any TP elements of SLOCC are included in LOCC as follows.

Proof. Let $\{M_m \in \mathbf{Pos}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{O_N})\}_{m \in \mathbb{M}}$ be the CJ operator of an element of SLOCC, where \mathbb{M} is the set of all the measurement outcomes in a sequence of SLOCC. Then there exists a set of measurement outcomes $\overline{\mathbb{M}}$ such that $\mathbb{M} \subseteq \overline{\mathbb{M}}$ and an element of LOCC whose CJ operator is given by $\{M_m\}_{m \in \overline{\mathbb{M}}}$, i.e.

$$\text{tr}_{O_1, \dots, O_N} \left[\sum_{m \in \overline{\mathbb{M}}} M_m \right] = \mathbb{I}_{I_1, \dots, I_N}. \quad (2.47)$$

If the element of SLOCC is TP, then we obtain

$$\text{tr}_{O_1, \dots, O_N} \left[\sum_{m \in \mathbb{M}} M_m \right] = \mathbb{I}_{I_1, \dots, I_N}. \quad (2.48)$$

These two equations imply

$$\text{tr}_{O_1, \dots, O_N} \left[\sum_{m \in \overline{\mathbb{M}} \setminus \mathbb{M}} M_m \right] = 0 \quad (2.49)$$

and

$$\forall m \in \overline{\mathbb{M}} \setminus \mathbb{M}, \quad M_m = 0 \quad (2.50)$$

since M_m is a positive semi-definite operator. Therefore, the LOCC map $\{M_m\}_{m \in \overline{\mathbb{M}}}$ represents the same map as the SLOCC map $\{M_m\}_{m \in \mathbb{M}}$. \square

That is,

$$\begin{aligned} & \text{LOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}) = \\ & \text{SLOCC}(\mathcal{H}_{I_1}, \dots, \mathcal{H}_{I_N} : \mathcal{H}_{O_1}, \dots, \mathcal{H}_{O_N}) \cap \mathbf{C}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{I_N} : \mathcal{H}_{O_1} \otimes \dots \otimes \mathcal{H}_{O_N}). \end{aligned} \quad (2.51)$$

2.5.4 Entanglement assisted LOCC

When LOCC accompanies with pre-shared entanglement, called *entanglement assisted LOCC*, it can implement general global quantum operations acting on the systems of the multiple parties. We review two types of global quantum operations, *quantum teleportation* and a controlled unitary operation, which appear in this thesis.

Quantum teleportation

Entanglement shared between spacelike separated parties cannot be used for communication between parties and a finite amount of classical communication cannot be used for exact transmission of an arbitrary quantum state. However, if entanglement is accompanied by classical communication, exact transmission of an arbitrary quantum state can be achieved. Such a process is called *quantum teleportation* [36]. In a quantum teleportation protocol, there are two parties, a sender and a receiver. The sender has a quantum state to be transmitted and an entangled state is pre-shared between the sender and the receiver. First, the

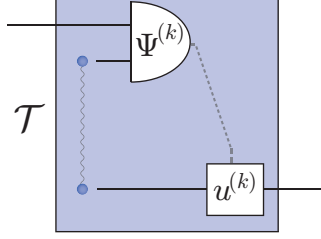


Figure 2.3: **A quantum circuit representation of the quantum teleportation protocol \mathcal{T} .** $\Psi^{(k)}$ represents the projective measurement $\{|\Psi^{(k)}\rangle\langle\Psi^{(k)}|\}_k$, $\{|\Psi^{(k)}\rangle\}_k = \{(u^{(k)} \otimes \mathbb{I})|\Phi^+\rangle\}$ is the Bell basis, $|\Phi^+\rangle$ is an EPR state and $\{u^{(k)}\}_k = \{I, Z, X, ZX\}$ is a set of operations to be applied conditional on the measurement outcome specified by k .

sender performs an appropriate measurement on her system. Second, she sends the measurement outcome to the receiver. Third, the receiver performs an appropriate unitary operation on his system corresponding to the measurement outcome. After all the procedures are done, the state of receiver's system is transformed into a quantum state that was initially possessed by the sender and the state of sender's system is transformed into a particular state corresponding to the measurement outcome not depending on the quantum state initially possessed by her.

We give a quantum circuit representation of the quantum teleportation protocol \mathcal{T} to transmit a one-qubit state by using an EPR state in Fig. 2.3.

Note that the quantum teleportation protocol is achieved by entanglement assisted bipartite one-way LOCC. Performing quantum teleportation in both directions, it is possible to implement any global quantum operations between spatially separated parties. Entanglement consumed in entanglement assisted LOCC is used for quantifying the globalness of a quantum operation [77, 78].

Controlled unitary operation

As we see, it is possible to implement any two-qubit unitary operations between two parties by bi-directional quantum teleportation using two EPR states and bipartite two-way LOCC. Only one EPR state is sufficient for implementing a two-qubit controlled unitary operation whereas one EPR state is not sufficient for implementing the SWAP operation. We give a quantum circuit representation of performing a two-qubit controlled unitary operation $U = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes u$ in Fig. 2.4.

One EPR state and 3-bits of classical communication are consumed in the protocol presented in Fig. 2.4. However, one EPR state and 2-bits of classical communication are shown to be sufficient for implementing a two-qubit controlled

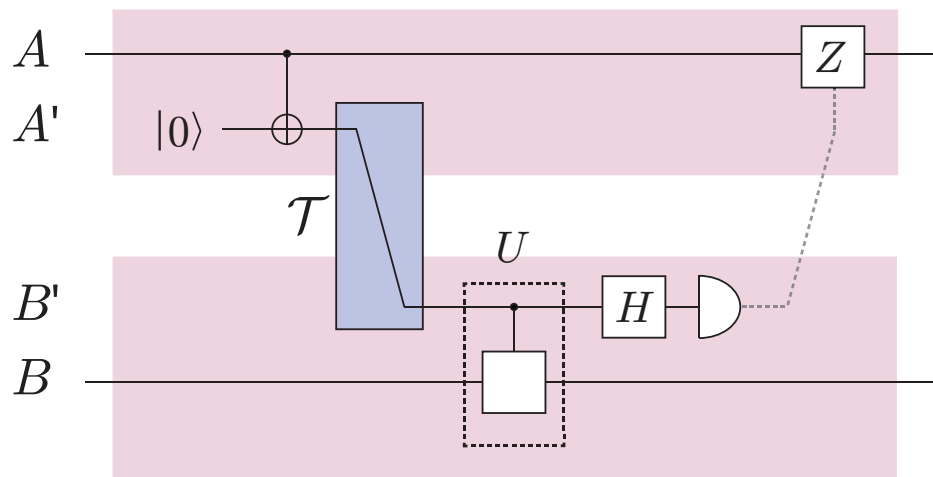


Figure 2.4: **A quantum circuit representation of the LOCC protocol implementing a two-qubit controlled unitary operation U .** Qubits in the first shaded region are possessed by the first party, those in the second shaded region are possessed by the second party. The protocol consists of introducing an ancillary qubits $\mathcal{H}_{A'}$ at the first party, teleporting the ancillary qubit state from the first party to the second party represented by qubit $\mathcal{H}_{B'}$, applying U on a controlled qubit $\mathcal{H}_{B'}$ and a target qubit \mathcal{H}_B at the second party, performing Hadamard operations and measurements in the computational basis on $\mathcal{H}_{B'}$ and finally applying conditional Z operations depending on the measurement outcome.

unitary operation [79]. The optimal amount of entanglement required for implementing a two-qubit controlled unitary operation is shown in [77, 78]. Note that one EPR state and 2-bits of classical communication are also sufficient for implementing a controlled unitary operation $U = |0\rangle\langle 0|_C \otimes \mathbb{I}_T + |1\rangle\langle 1|_C \otimes u_T$, where the dimension of the controlled system \mathcal{H}_C is 2 while the dimension of the target system \mathcal{H}_T can be higher than 2.

Part II

Quantum computation over quantum networks

Chapter 3

Preliminaries of Part II

In this part, we analyze the first question:

- How does the topology of a quantum network consisting of quantum channels affect the performance of quantum communication?

More specifically, we concentrate on how the performance of quantum communication (generally quantum computation) changes when the topology of a quantum network consisting of quantum channels is changed while the capacity of quantum channels is fixed. For simplicity, we consider quantum channels are noiseless and have 1-qubit capacity. We consider a one-shot scenario, i.e. we are allowed to use a given network only once, and concentrate on a *cluster network*, which is a certain class of the network consisting of intermediate nodes and the same number of senders and receivers. The cluster network is a subclass of k -pair network, which has been an actively studied network in both classical information theory [31] and quantum information theory [32, 33, 34]. We use the technique of *network coding* introduced in the following.

3.1 Network coding theory

In this section, we briefly review classical and quantum network coding theory, which is a basis of our analysis.

3.1.1 Classical network coding

In classical (network) information theory, *network coding*, which incorporates processing at each network node in addition to routing, provides efficient transmission protocols that can resolve the bottleneck problem [28]. Consider a communication task over the *butterfly network* and the *grail network* presented in Fig. 3.1 that

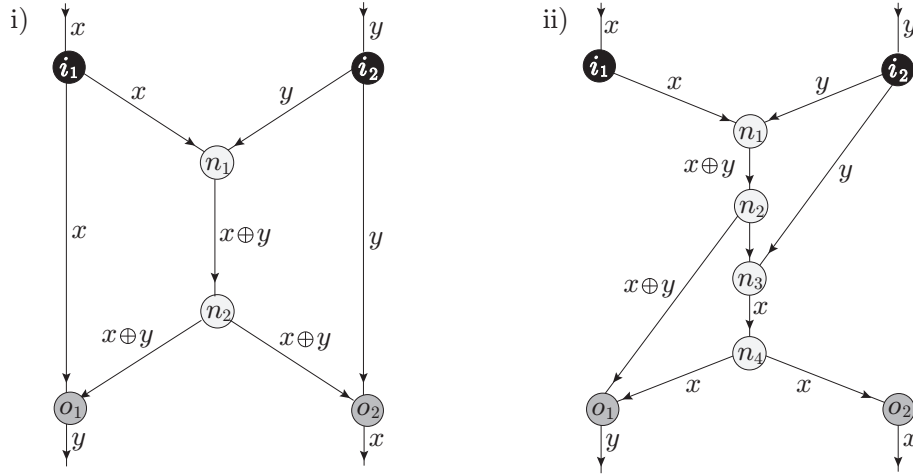


Figure 3.1: **Network coding for a classical communication task over i) the butterfly network and ii) the grail network.** Two bits of information $x, y \in \{0, 1\}$ are given at the input nodes i_1 and i_2 , respectively. $x \oplus y$ denotes addition of x and y modulus 2.

aims to transmit single bits x and y from i_1 to o_2 and i_2 to o_1 simultaneously via nodes n_1, n_2, n_3 and n_4 . The directed edges denote transmission channels with 1-bit capacity. One of the channels in each network exhibits the bottleneck without network coding shown in Fig. 3.1. Network coding has been already implemented in wireless network protocols and satellite communication protocols.

Such a communication task over a general two input-output network given by a graph G has been shown to be achievable if and only if G contains an essential substructure [80]. The butterfly network and the grail network are known to be two such essential substructures.

3.1.2 Quantum network coding

Quantum communication with *quantum network coding* has been studied by analogy to classical network coding [81, 82, 83, 32, 33, 34]. k -pair quantum communication over a network is a unicast communication task to faithfully transmit a k -qubit state given at distinct input nodes $\{i_1, i_2, \dots, i_k\}$ to distinct output nodes $\{o_1, o_2, \dots, o_k\}$ through a given network. Two examples of 2-pair quantum communication over a butterfly network and a grail network are shown in Fig. 3.2. The setting of network coding can be further classified into three cases based on how one treats classical communication, namely,

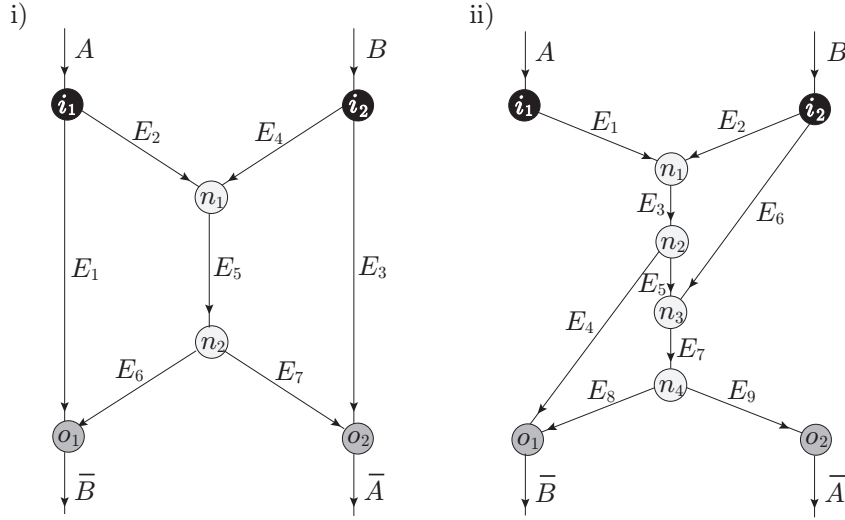


Figure 3.2: **The butterfly and the grail quantum network.** i) The butterfly network and ii) the grail network with the input nodes (i_1 and i_2), output nodes (o_1 and o_2) and the repeater nodes (n_1, n_2, n_3 and n_4). The directed edges $A, B, \bar{A}, \bar{B}, E_1, E_2, \dots, E_9$ represent quantum or classical channels. Quantum channels have 1-qubit capacity. Meanwhile there are some settings about classical channel capacity. Our task is to transmit a given two-qubit state $|\text{input}\rangle_{i_1, i_2}$ from i_1 to o_2 and from i_2 to o_1 simultaneously by using the channels and local quantum operations at each nodes.

1. The case where each channel can be used for either 1-bit classical communication or 1-qubit quantum communication [81, 82].
2. The case where each channel can be used for either 2-bit classical communication or 1-qubit quantum communication [83, 30].
3. The case where the channels only restrict the capacity of quantum communication, and classical communication is freely allowed between any two nodes [32, 33, 34].

In quantum network coding, perfect multicast communications are not allowed by the no-cloning theorem [76]. No-cloning theorem also makes it impossible to perform k -pair communication over the networks by using a simple extension of classical network coding. Indeed, in the setting where each edge can be used for either 1-bit classical communication or 1-qubit quantum communication, perfect quantum 2-pair communication over the butterfly network has been shown to be

impossible [81, 82]. However, it has been shown that in the setting where each edge can be used for either 2-bit classical communication or 1-qubit quantum communication, perfect quantum 2-pair communication over the butterfly network is possible, if and only if input nodes share two EPR pairs [83]. In the setting where each edge has 1-qubit channel capacity and classical communication is freely allowed between any nodes, however, it has been shown that there exists a quantum network coding protocol to achieve the 2-pair quantum communication over the butterfly and grail networks perfectly [32, 33, 34]. In this thesis, we focus on the third setting, where classical communication is freely allowed between any two nodes. This setting is justified in practical situations, where classical communication is easier to implement experimentally than quantum communication. Before proceeding to our research, we review the technique used in quantum network coding in the third setting and note two important points related to our research.

In [34], Kobayashi *et al.* have shown that if classical k -pair communication, which is a unicast communication task to faithfully transmit k -bit given at distinct input nodes to distinct output nodes simultaneously, is possible, quantum k -pair communication over the same network is possible in the quantum setting where free classical communication is allowed ¹. Their implementation protocol is composed of two stages. In the first stage, the encoding stage, a unitary operation $U_{encoding}$ described by a gate sequence consisting only of CNOT gates is performed to create a large entangled resource state over the qubits at all nodes of the graph. The CNOT gates correspond to the operation of copying and exclusive disjunction used for implementing $x \rightarrow x, x$ and $x, y \rightarrow x \oplus y$ in the classical setting of network coding. In the second stage, the disentangling stage, two kinds of disentangling operations are performed, denoted by maps Γ_{d2} and Γ_{d3} consisting of the Hadamard gate, measurements in the computational basis, and conditional Z operators depending on the measurement outcomes. Using the notation for quantum circuits presented in Table 2.1 and the notation for nodes and edges presented in Fig. 3.2, the gate sequence of $U_{encoding}$ for 2-pair communication over the butterfly network is presented in Fig. 3.3. Quantum circuits corresponding to Γ_{d2} and Γ_{d3} are shown in Figures 3.4 and 3.5, respectively.

¹Note that a network is a graph consisting nodes (vertices) and channels (edges) as we define later. Thus, if the graph is the same, we say the network is the same although the capacity of channels is different in the quantum setting and the classical setting.

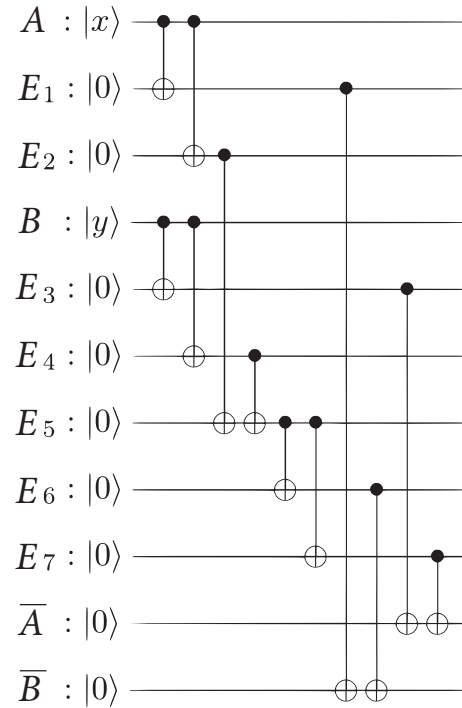


Figure 3.3: **The quantum circuit for $U_{encoding}$ in the encoding stage of the protocol presented by the Kobayashi *et al.* protocol for 2-pair communication over the butterfly network.** The indices of the Hilbert spaces of the qubits transmitted along the corresponding edges are also denoted by $A, B, \bar{A}, \bar{B}, E_1, \dots, E_7$. Operations on the qubits in the same node are considered local operations. An input state of the qubits A and B is given by $\sum_{x,y=0,1} \lambda_{x,y} |x\rangle_A |y\rangle_B$, where $\{|x\rangle_A\}$ and $\{|y\rangle_B\}$ denote the computational bases of qubit A and B , respectively, and $\sum_{x,y} |\lambda_{x,y}|^2 = 1$.

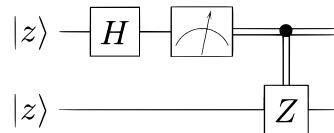


Figure 3.4: **A quantum circuit for the map Γ_{d2} .** It disentangles the first qubit of a two-qubit state $\sum_{z=0,1} \alpha_z |z\rangle_1 |z\rangle_2$ to obtain $\sum_z \alpha_z |z\rangle_2$ at the second qubit for all α_z satisfying $\sum_z |\alpha_z|^2 = 1$, where $\{|z\rangle\}$ is the computational basis.

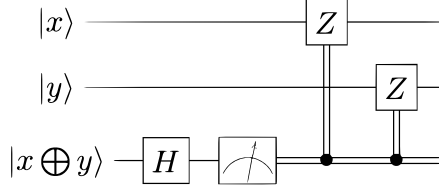


Figure 3.5: **A quantum circuit for the map Γ_{d3} .** It disentangles the third qubit from a three-qubit state $\sum_{x,y=0,1} \lambda_{x,y} |x\rangle_1 |y\rangle_2 |x \oplus y\rangle_3$ to obtain $\sum_{x,y} \lambda_{x,y} |x\rangle_1 |y\rangle_2$ on the first two qubits for all $\lambda_{x,y}$ satisfying $\sum_{x,y} |\lambda_{x,y}|^2 = 1$, where $\{|x\rangle\}$ and $\{|y\rangle\}$ denote the computational basis.

We give an overview of the Kobayashi et al. protocol for 2-pair communication over the butterfly network. We write the initial state of two qubits A and B given at the input nodes i_1 and i_2 , respectively, by

$$|input(\lambda)\rangle_{AB}^{i_1 i_2} = \sum_{x,y=0,1} \lambda_{x,y} |x\rangle_A^{i_1} |y\rangle_B^{i_2} \quad (3.1)$$

where λ specifies a set of coefficients $\lambda = \{\lambda_{x,y}\}_{x,y=0,1}$ satisfying $\sum_{x,y} |\lambda_{x,y}|^2 = 1$, superscripts i_1 and i_2 specify the nodes where qubits belong, and $\{|x\rangle\}$ and $\{|y\rangle\}$ are the computational basis. All the other qubits E_1, \dots, E_7, \bar{A} and \bar{B} are in the fixed state $|0\rangle$. In general, the initial state given by $|input(\lambda)\rangle$ represents an entangled state of qubits A and B . If necessary, the input state can be restricted to a product state by imposing $\lambda_{x,y} = \mu_x \nu_y$ for $x, y = 0, 1$ satisfying $\sum_x |\mu_x|^2 = 1$ and $\sum_y |\nu_y|^2 = 1$.

By performing $U_{encoding}$ in the encoding stage, the initial state is transformed to an entangled state of 11 qubits, $A, B, E_1, \dots, E_7, \bar{A}$ and \bar{B} , given by

$$\sum_{x,y=0,1} \lambda_{x,y} |x\rangle_A^{i_1} |x\rangle_{E_1}^{o_1} |x\rangle_{E_2}^{n_1} |y\rangle_B^{i_2} |y\rangle_{E_3}^{o_2} |y\rangle_{E_4}^{n_1} |x \oplus y\rangle_{E_5}^{n_2} |x \oplus y\rangle_{E_6}^{o_1} |x \oplus y\rangle_{E_7}^{o_2} |x\rangle_{\bar{A}}^{o_2} |y\rangle_{\bar{B}}^{o_1}. \quad (3.2)$$

In the disentangling stage, the disentangling operation Γ_{d2} on qubits A and E_1 is performed to disentangle the qubit A . The resulting state is given by

$$\sum_{x,y=0,1} \lambda_{x,y} |x\rangle_{E_1}^{o_1} |x\rangle_{E_2}^{n_1} |y\rangle_B^{i_2} |y\rangle_{E_3}^{o_2} |y\rangle_{E_4}^{n_1} |x \oplus y\rangle_{E_5}^{n_2} |x \oplus y\rangle_{E_6}^{o_1} |x \oplus y\rangle_{E_7}^{o_2} |x\rangle_{\bar{A}}^{o_2} |y\rangle_{\bar{B}}^{o_1}. \quad (3.3)$$

This disentangling operation can be performed when both of the two qubits A and E_1 are at the node i_1 , but it can be also performed after the qubit E_1 is transmitted from i_1 to o_1 using the edge E_1 . In this case, 1-bit classical communication is required from the node i_1 to the node o_1 to perform the conditional Z operation

on the qubit E_1 . Similarly, the disentangling operation Γ_{d2} is performed on the pairs of qubits $\{B, E_3\}$, $\{E_2, E_1\}$, $\{E_4, E_3\}$ and $\{E_5, E_6\}$ to disentangle qubits B , E_2 , E_4 , and E_5 . Then another disentangling operation Γ_{d3} is performed on the sets of qubits $\{E_1, \bar{B}, E_6\}$ and $\{\bar{A}, E_3, E_7\}$ to disentangle the qubits E_6 and E_7 . Then we obtain a state of four qubits E_3, \bar{A} at the node o_2 and E_1, \bar{B} at the node o_1 given by

$$|\phi(\lambda)\rangle^{o_2 o_1} = \sum_{x,y=0,1} \lambda_{x,y} |x\rangle_{E_1}^{o_1} |y\rangle_{E_3}^{o_2} |x\rangle_{\bar{A}}^{o_2} |y\rangle_{\bar{B}}^{o_1}. \quad (3.4)$$

At last, the disentangling operation Γ_{d2} is performed on the pairs $\{E_1, \bar{A}\}$ and $\{E_3, \bar{B}\}$ to disentangle E_1 and E_3 . Then we obtain the output state

$$|output(\lambda)\rangle^{o_2 o_1} = \sum_{x,y=0,1} \lambda_{x,y} |x\rangle_{\bar{A}}^{o_2} |y\rangle_{\bar{B}}^{o_1}. \quad (3.5)$$

Thus, we achieve $|output(\lambda)\rangle_{\bar{A}\bar{B}} = |input(\lambda)\rangle_{A,B}$. Note that 7-bits of classical communication is required in the disentangling stage.

At the end of this section, we note two important points of quantum network coding with free classical communication which is related to our research.

- Applying CNOT gates instead of the operation of copying and exclusive disjunction used for implementing $x \rightarrow x, x$ and $x, y \rightarrow x \oplus y$ in the classical setting of network coding enables to perform quantum communication. However, it is possible to perform a more general controlled unitary operations instead of CNOT by using quantum network, which is a key idea for implementing a unitary operation over a quantum network.
- In [34], they have shown that if classical k -pair communication is possible, then quantum k -pair communication is possible. However, we do not know the converse. Particularly, we do not know whether a quantum communication is possible or not over the *square network* presented in Fig. 3.6, where a classical communication is impossible.

3.2 Measurement Based Quantum Computation (MBQC)

Quantum computation over quantum networks is related to a model of quantum computation, *measurement based quantum computation* (MBQC). MBQC was first proposed in 2001 by Raussendorf and Briegel in a much acclaimed paper [35]. They showed that a particular highly entangled multi-qubit state called a *cluster*

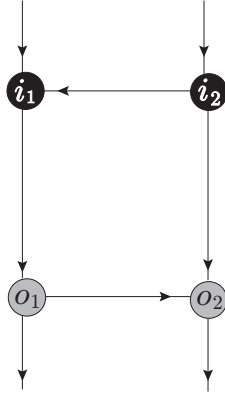


Figure 3.6: **The square network with the input nodes (i_1 and i_2) and output nodes (o_1 and o_2).** We focus on the setting where quantum channels described by directed edges have 1-qubit capacity and classical communication is freely allowed. The task is to transmit a given two-qubit state $|\text{input}\rangle_{i_1, i_2}$ from i_1 to o_2 and from i_2 to o_1 simultaneously. It has been an open problem whether the task is achievable or not. We show that the task is impossible by using a tool we develop in this Part.

state combined with single qubit measurements and classical communication are sufficient for performing universal quantum computation. In the first stage, a cluster state is prepared by initializing all qubits in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ state and then applying controlled Z gates between pairs of neighboring qubits on a square lattice, more generally, one can prepare graph states similarly for neighbors corresponding to the edges of graph. A definition of a graph state $|\phi\rangle$ is given as follows. Note that the order in the product has no bearing on the definition since all the controlled Z gates are commutative.

Definition 2. For a given graph $G = \{\mathcal{V}, \mathcal{E}\}$, the graph state $|\phi\rangle \in \mathbb{C}^{2^{|\mathcal{V}|}}$ is a $|\mathcal{V}|$ -qubit state such that

$$|\phi\rangle = \prod_{(u,v) \in \mathcal{E}} U_{u,v}^{CZ} \left(\otimes_{i=1}^{|\mathcal{V}|} |+\rangle_i \right), \quad (3.6)$$

where $U_{u,v}^{CZ}$ is the controlled Z gate acting only on the u -th qubit and the v -th qubit.

In the second stage, we perform a projective measurement $\{|+\alpha\rangle\langle+\alpha|, |-\alpha\rangle\langle-\alpha|\}$, where

$$|\pm\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle), \quad (3.7)$$

on all single qubits in a certain sequence, sending the classical outcome bits to the measurement in the next step. The entanglement between measured and unmeasured qubits ensures that the quantum state of the remaining qubits is transformed according to the algorithm given by the initial state and the measurement pattern. The final qubits to be measured define the output of the computation.

Since we use only local measurements, all of the entanglement that we need for the computation must be prepared in the first stage. This model highlights the role of entanglement in quantum computation.

3.3 Classifications of unitary operators

In this section, we first review *controlled unitary operation*, since it plays a central role in quantum computation over a quantum network. In order to characterize the class of implementable unitary operations over a quantum network, we introduce two ways to classify unitary operators, the Kraus-Cirac decomposition and the operator Schmidt decomposition. Note that the operator Schmidt decomposition is applicable to unitary operators on any non-prime dimensional Hilbert space while the Kraus-Cirac decomposition is applicable only to two-qubit unitary operators.

3.3.1 Controlled unitary operation

A fully controlled unitary operator $U \in \mathbf{U}(\mathcal{H}_c \otimes \mathcal{H}_t)$ is a unitary operator that acts on a control system \mathcal{H}_c and a target system \mathcal{H}_t such that

$$U = \sum_{i=1}^{\mathcal{C}} |i\rangle\langle i|_c \otimes u^{(i)}, \quad (3.8)$$

where $\{|i\rangle_c\}_i$ is an orthonormal basis of \mathcal{H}_c and $u^{(i)} \in \mathbf{U}(\mathcal{H}_t)$ is a unitary operator. U^{CNOT} and U^{CZ} are special cases of two-qubit controlled unitary operators. A controlled unitary operator is similar to a classical switch where the gate acting on the target system changes depending on the state of the control system. The i -th unitary operator $u^{(i)}$ of the set $\{u^{(i)}\}$ is performed on the target system when the state of the control system is prepared to be $|i\rangle_c$. However, unlike the classical switch, we can prepare the state of the control system to be any superposition of states, which creates entanglement between the control system and the target system.

Any two-qubit controlled unitary operators U defined by

$$U := |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes u \quad (3.9)$$

where $u \in \mathbf{U}(\mathbb{C}^2)$, is locally unitarily equivalent to a two-qubit controlled phase operator $U^{(\theta)}$. $U^{(\theta)}$ can be written by

$$U^{(\theta)} := |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|.$$

That is, for all two-qubit controlled unitary operators U , there exists $u_1, u_2, u_3, u_4 \in \mathbf{U}(\mathbb{C}^2)$ and $\theta \in \mathbb{R}$ such that $U = (u_3 \otimes u_4)U^{(\theta)}(u_1 \otimes u_2)$. We give a proof of this statement in the following.

Proof. $u_1, u_2, u_3, u_4 \in \mathbf{U}(\mathbb{C}^2)$ and θ are given by the following.

1. Diagonalize u , and obtain $u = e^{i\alpha}(|\psi\rangle\langle\psi| + e^{i\beta}|\psi'\rangle\langle\psi'|)$, where $\{e^{i\alpha}, e^{i(\alpha+\beta)}\}$ are the eigenvalues of u and $\{|\psi\rangle, |\psi'\rangle\}$ the eigenvectors.
2. Set $u_1 = \mathbb{I}, u_2 = |0\rangle\langle\psi| + |1\rangle\langle\psi'|$, $u_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}, u_4 = |\psi\rangle\langle 0| + |\psi'\rangle\langle 1|$ and $\theta = \beta$.

□

We summarize the property of the local unitary equivalence of two-qubit controlled unitary operators in Fig. 3.7. The set of two-qubit unitary operations that is locally unitarily equivalent to a controlled phase operator is denoted by \mathbf{U}_c .

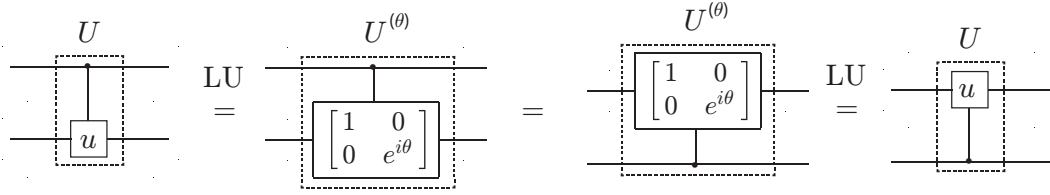


Figure 3.7: **Quantum circuits representing the property of local unitary equivalence of a two-qubit controlled unitary operator and a controlled phase operator.** $\stackrel{\text{LU}}{=}$ represents local unitary equivalence. Note that the controlled qubit and the target qubit can be flipped in a local unitary equivalence class.

3.3.2 Kraus-Cirac decomposition

A general two-qubit unitary operator $U \in \mathbf{U}(\mathcal{H}_{\mathcal{I}_Q} : \mathcal{H}_{\mathcal{O}_Q})$ where $\mathcal{H}_{\mathcal{I}_Q} = \mathcal{H}_{\mathcal{O}_Q} = \mathbb{C}^2 \otimes \mathbb{C}^2$ can be decomposed into a canonical form called the Kraus-Cirac decomposition introduced in [84, 85, 86] given by

$$U = (u \otimes u')e^{i(xX \otimes X + yY \otimes Y + zZ \otimes Z)}(w \otimes w'). \quad (3.10)$$

where u, u', w and w' are single qubit unitary operators and X, Y and Z are the Pauli operators on \mathbb{C}^2 and $x, y, z \in \mathbb{R}$. Since u, u', w and w' represent local unitary equivalence, we focus on analyzing implementability of the two-qubit global unitary part

$$U_{global}(x, y, z) := e^{i(xX \otimes X + yY \otimes Y + zZ \otimes Z)} \quad (3.11)$$

In Eq. (3.11), the parameters x, y, z in $0 \leq x < \pi/2$ (or $0 \leq x \leq \pi/4$ if $z = 0$), $0 \leq y \leq \min\{x, \pi/2 - x\}$ and $0 \leq z \leq y$ cover all two-qubit global unitary operators up to the local unitarily equivalence (the Weyl chamber [85]). We define the Kraus-Cirac number of a two-qubit unitary operator U as the number of non-zero parameters x, y, z in $U_{global}(x, y, z)$ and denote by $KC\#(U)$. $KC\#(U)$ characterizes nonlocal properties (globalness) of U [87].

3.3.3 Operator Schmidt decomposition

The operator Schmidt decomposition can be applied to any unitary operation acting on a finite (non-prime number) dimensional Hilbert space. The set of linear operators $\mathbf{L}(\mathcal{H}_A)$ forms a Hilbert space with respect to the inner product $(M, N) = \frac{1}{\dim(\mathcal{H}_A)} \text{tr}(M^\dagger N)$. Thus we can apply the Schmidt decomposition to operators, such that for any linear operator $M \in \mathbf{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$, there exists a set of orthonormal operators $\{P_i \in \mathbf{L}(\mathcal{H}_A)\}_i$ and $\{Q_i \in \mathbf{L}(\mathcal{H}_B)\}_i$ satisfying

$$M = \sum_i \lambda_i P_i \otimes Q_i, \quad (3.12)$$

where $\{\lambda_i\}$ are non-negative real numbers known as the *operator Schmidt coefficients* [91]. The number of non-zero coefficients $|\{\lambda_i > 0\}|$ is known as the *operator Schmidt rank*. We denote the operator Schmidt rank of a linear operator M by $\text{Op}\#_B^A(M)$.

Elements of two-qubit unitary operators $\mathbf{U}(\mathcal{H}_A \otimes \mathcal{H}_B)$ can be classified by the Kraus-Cirac number and the operator Schmidt rank as follows. We summarize the classifications in Table 3.1.

- U with $KC\#(U) = 0$ is a product of local unitary operators and satisfies $\text{Op}\#_B^A(U) = 1$.
- U with $KC\#(U) = 1$ is locally unitarily equivalent to a controlled unitary operator and satisfies $\text{Op}\#_B^A(U) = 2$.
- U with $KC\#(U) = 2$ is locally unitarily equivalent to a special class of

two-qubit unitary operators called a matchgate U^{match} defined by

$$U^{match} = \begin{pmatrix} u_{0,0}^{(1)} & 0 & 0 & u_{0,1}^{(1)} \\ 0 & u_{0,0}^{(2)} & u_{0,1}^{(2)} & 0 \\ 0 & u_{1,0}^{(2)} & u_{1,1}^{(2)} & 0 \\ u_{1,0}^{(1)} & 0 & 0 & u_{1,1}^{(1)} \end{pmatrix}, \quad (3.13)$$

where $u^{(i)} = \begin{pmatrix} u_{0,0}^{(i)} & u_{0,1}^{(i)} \\ u_{1,0}^{(i)} & u_{1,1}^{(i)} \end{pmatrix}$ is a single-qubit unitary operator whose determinant is equal to 1. A sequence of the matchgates acting only on the nearest neighbor of one-dimensionally aligned qubits corresponds to a physical model of noninteracting fermions [89] and is efficiently simulatable on a classical computer [88, 90]. U^{match} satisfies $\text{Op}\#_B^A(U) = 4$.

- The rest of two-qubit unitary operators including the SWAP operator have $\text{KC}\#(U) = 3$ and satisfy $\text{Op}\#_B^A(U) = 4$.

$\text{KC}\#(U)$	$\text{Op}\#_B^A(U)$	class
0	1	LU
1	2	LU C-phase
2	4	LU matchgate
3	4	$SU(4)$

Table 3.1: Classification of two-qubit unitary operators $U(\mathcal{H}_A \otimes \mathcal{H}_B)$ by the Kraus-Cirac number and the operator Schmidt rank. We refer the class with Kraus-Cirac number 0 as local unitary operators. The class with Kraus-Cirac number 1 is locally unitarily equivalent to controlled phase gates. The class with Kraus-Cirac number 2 is locally unitarily equivalent to matchgates.

Chapter 4

Computation over the cluster network

In k -pair quantum communication, the output state $|\text{output}\rangle_{o_1 \dots o_k}$ at the output nodes can be regarded as a state obtained by performing a k -qubit unitary operation U on the input state $|\text{input}\rangle_{i_1 \dots i_k}$ given at the input nodes

$$|\text{output}\rangle_{o_1 \dots o_k} = U |\text{input}\rangle_{i_1 \dots i_k}, \quad (4.1)$$

where U is a permutation operator¹. We do not need to restrict the k -qubit unitary operator U in Eq.(4.1) to be a permutation operator, it can be a general unitary operator. This leads to the idea of quantum computation over a quantum network, which aims to perform a unitary operation on a state given at distinct input nodes and to faithfully transmit the resulting state to the distinct output nodes efficiently over the network at the same time [29, 30]. By computing and communicating simultaneously, quantum computation over the network may reduce communication resources in DQC. Since communication can be naturally regarded as a special class of computation, investigating the capability of quantum computation gives us a new insight of quantum network coding, which originally aims at just quantum communication.

We investigate implementability of a unitary operation over a *cluster network*, which is a special class of networks with k input nodes and k output nodes, which we call k -pair network, as a first step to analyze more general network. The cluster network contains the grail network as its special case and relates to the butterfly network. We focus on the setting where classical communication is freely allowed between any two nodes. We present which class of unitary operators is

¹A k -qubit permutation operator U is defined by $U = \sum_{i_1, \dots, i_k} |i_{\sigma(1)}, \dots, i_{\sigma(k)}\rangle \langle i_1, \dots, i_k|$, where σ represents a permutation. An example of a two-qubit permutation operator is a SWAP operator U^{SWAP} , defined in Table 2.1.

implementable over cluster networks in this setting by investigating transformations of cluster networks into quantum circuits. The transformation method of cluster networks provides constructions of quantum network coding to implement any two-qubit unitary operations over the grail and butterfly networks, which are fundamental primitive networks for classical network coding. We also analyze probabilistic implementation of N -qubit unitary operations over the cluster network to understand the properties of quantum network coding for quantum computation when the requirement of deterministic implementations are relaxed but that of exact implementations are kept.

We denote the Hilbert space of a set of qubits specified by a set \mathcal{Q} by $\mathcal{H}_{\mathcal{Q}}$ and the Hilbert space corresponding to a qubit Q_k specified by an index k by $\mathcal{H}_{Q_k} = \mathbb{C}^2$. In our setting where quantum communications are restricted but classical communications are unrestricted, quantum communication of a qubit state between two nodes is replaced by teleportation between two nodes. Since any direction of classical communications is allowed, quantum communication of a single qubit state can be achieved by sharing a maximally entangled two-qubit state between the nodes and the direction of quantum communication is not limited. Thus what we can do over a given network in principle is equivalent to perform *local operations* (at each nodes) *and classical communication* (LOCC) assisted by the *resource state* that consists of a set of maximally entangled two-qubit states (the EPR states) $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ shared between the nodes connected by edges.

We investigate which unitary operations are implementable by LOCC assisted by the resource state for a given network where nodes are represented by a two-dimensional lattice. We consider that a node represented by $v_{i,j}$ is on the coordinate of the two-dimensional lattice (i, j) and edges connect nearest neighbor nodes. We call these networks *cluster networks*. In Discussion of this part, we examine implementability of a unitary operation over *generalized cluster network*, where nodes are represented by a two-dimensional lattice and edges connect nearest neighbor horizontal nodes but edges can connect any pair of vertical nodes. We first give a formal definition of a cluster network.

Definition 3. A network $G = \{\mathcal{V}, \mathcal{E}, \mathcal{I}, \mathcal{O}\}$ is a (k, N) -cluster network if and only if,

$$\begin{aligned}
 \mathcal{V} &= \{v_{i,j}; 1 \leq i \leq k, 1 \leq j \leq N\} \\
 \mathcal{I} &= \{v_{i,1}; 1 \leq i \leq k\} \\
 \mathcal{O} &= \{v_{i,N}; 1 \leq i \leq k\} \\
 \mathcal{E} &= \mathcal{S} \cup \mathcal{K}
 \end{aligned} \tag{4.2}$$

where

$$\begin{aligned}\mathcal{S} &= \{(v_{i,j}, v_{i+1,j}); 1 \leq i \leq k-1, 1 \leq j \leq N\}, \\ \mathcal{K} &= \{(v_{i,j}, v_{i,j+1}); 1 \leq i \leq k, 1 \leq j \leq N-1\},\end{aligned}\quad (4.3)$$

$k \geq 1$ and $N \geq 1$. \mathcal{V} represents the set of all nodes, \mathcal{I} and \mathcal{O} represent k input nodes and k output nodes, respectively. \mathcal{E} represents the set of all edges and \mathcal{S} and \mathcal{K} represent the sets of vertical and horizontal edges, respectively.

Next we define the resource state corresponding to the (k, N) -cluster network. We introduce qubits $S_{i,j}^1$ at node $v_{i,j}$ and $S_{i+1,j}^2$ at node $v_{i+1,j}$ to represent an EPR pair corresponding to an edge $(v_{i,j}, v_{i+1,j}) \in \mathcal{S}$. Similarly, we introduce qubits specified by $K_{i,j}^1$ at node $v_{i,j}$ and $K_{i,j+1}^2$ at node $v_{i,j+1}$ to represent an EPR pair corresponding to an edge $(v_{i,j}, v_{i,j+1}) \in \mathcal{K}$. We denote the set of all qubits in the resource state by $\mathcal{R} = \{S_{i,j}^1, S_{i+1,j}^2 | 1 \leq i \leq k-1, 1 \leq j \leq N\} \cup \{K_{i,j}^1, K_{i,j+1}^2 | 1 \leq i \leq k, 1 \leq j \leq N-1\}$. The resource state $|\Phi\rangle_{\mathcal{R}}$ corresponding to a cluster network is defined by the following.

Definition 4. For a given (k, N) -cluster network, the resource state $|\Phi\rangle_{\mathcal{R}} \in \mathcal{H}_{\mathcal{R}}$ is defined by

$$\begin{aligned}|\Phi\rangle_{\mathcal{R}} &= \otimes_{i=1}^{k-1} \otimes_{j=1}^N |\Phi^+\rangle_{S_{i,j}^1, S_{i+1,j}^2} \\ &\quad \otimes_{i=1}^k \otimes_{j=1}^{N-1} |\Phi^+\rangle_{K_{i,j}^1, K_{i,j+1}^2}.\end{aligned}\quad (4.4)$$

For example, the $(3, 3)$ -cluster network and the corresponding resource state are shown in Fig. 4.1. Note that the resource state for a cluster network represented by Eq. (4.4) is different from the cluster states used in MBQC, defined by Eq.(3.6). While we can convert the resource state for a cluster network into a cluster state by performing a projective measurement on all qubits at each node, a cluster state cannot be converted to the resource state for the corresponding cluster network by LOCC.

Finally we define implementability of a unitary operation over a k -pair network. In addition to resource qubits \mathcal{R} , We introduce input qubits I_i at the input node $v_{i,1} \in \mathcal{I}$, output qubits O_i at the output node $v_{i,N} \in \mathcal{O}$, a set of input qubits $\mathcal{I}_Q = \{I_i | 1 \leq i \leq k\}$ and a set of output qubits $\mathcal{O}_Q = \{O_i | 1 \leq i \leq k\}$ for a (k, N) -cluster network. Note that each input and output node has only one input or output qubit since we concentrate on implementability of a unitary operation, and the state of output qubits is initially set to be in $|0\rangle \in \mathcal{H}_{\mathcal{O}_Q}$.

Definition 5. For a (k, N) -cluster network specified by $G = \{\mathcal{V}, \mathcal{E}, \mathcal{I}, \mathcal{O}\}$, a unitary operation $U \in \mathbf{U}(\mathcal{H}_{\mathcal{I}_Q} : \mathcal{H}_{\mathcal{O}_Q})$ is deterministically implementable over the

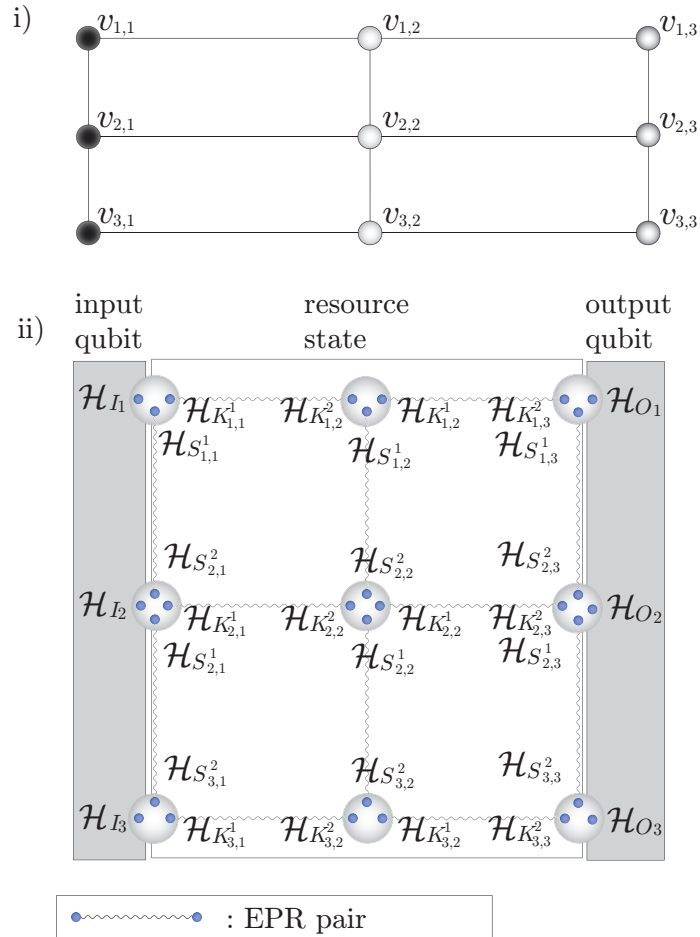


Figure 4.1: **An example of a cluster network.** i) The $(3,3)$ -cluster network with the input nodes $\mathcal{I} = \{v_{1,1}, v_{2,1}, v_{3,1}\}$, output nodes $\mathcal{O} = \{v_{1,3}, v_{2,3}, v_{3,3}\}$ and 3 repeater nodes $\{v_{1,2}, v_{2,2}, v_{3,2}\}$, and ii) the corresponding resource state. Note that the resource states of the cluster networks are different from the cluster states used in MBQC [35].

network if and only if there exists a LOCC map Γ such that for any pure state $|\psi\rangle \in \mathcal{H}_{\mathcal{I}_Q}$,

$$\Gamma(|\psi\rangle\langle\psi| \otimes |\Phi\rangle\langle\Phi|_{\mathcal{R}}) = U|\psi\rangle\langle\psi|U^\dagger, \quad (4.5)$$

where LOCC map Γ consists of local operations on each node and classical communications and $\mathbf{U}(\mathcal{H}_{\mathcal{I}_Q} : \mathcal{H}_{\mathcal{O}_Q})$ is the set of unitary operations from $\mathcal{H}_{\mathcal{I}_Q}$ to $\mathcal{H}_{\mathcal{O}_Q}$.

Note that the main difference between this network computation model for implementing a unitary operation over a cluster network and standard MBQC is that any operations inside each node are allowed including adding arbitrary ancilla states in this model whereas only certain projective measurements on the cluster state in each node are allowed in MBQC. Thus the full set of implementable unitary operations over a (k, N) -cluster network is larger than a set of operations implementable by MBQC using the corresponding cluster states converted from the resource state for the (k, N) -cluster network by LOCC. In Chapter 5, of this part, we investigate a difference between MBQC and computation over the butterfly network and discuss a potential contribution of our result toward MBQC.

4.1 Possible computation

We propose a method to convert a (k, N) -cluster network into quantum circuits representing a class of unitary operators implementable by LOCC assisted by the resource state corresponding to a given cluster network. By using the converted circuit, it is easier to construct a network coding protocol since a set of implementable unitary operators are represented by a set of parameters of the converted circuit instead of a complicated LOCC protocol. The class of implementable unitary operators represented by the converted circuit is a subset of that over the cluster network in general since the conversion method does not guarantee to give all possible constructions. However, in some cases, the constructions given by the conversion methods cover all possible implementable unitary operations as will be shown in the next section.

We define a set of vertically aligned nodes $\mathcal{V}_j^v := \{v_{i,j}\}_{i=1}^k$ and a set of vertically aligned edges $\mathcal{S}_j := \{(v_{i,j}, v_{i+1,j})\}_{i=1}^{k-1}$ where $1 \leq j \leq N$. We also define a set of horizontally aligned nodes $\mathcal{V}_i^h := \{v_{i,j}\}_{j=1}^N$ and a set of horizontally aligned edges $\mathcal{K}_i := \{(v_{i,j}, v_{i,j+1})\}_{j=1}^{N-1}$ where $1 \leq i \leq k$. We consider that the EPR pairs given for a set of vertically aligned edges \mathcal{S}_j are used for implementing global unitary operations between nodes whereas each EPR pair given for a set of horizontal aligned edges \mathcal{K}_i is used for teleporting a qubit state from node $v_{i,j}$ to node $v_{i,j+1}$.

We investigate which kinds of global operations are implementable between the nodes in \mathcal{V}_j^v if only one EPR pair is given for each edge and LOCC between the

nodes is allowed. In this case, a two-qubit controlled unitary operation

$$C_{l;n}(\{u_n^{(a)}\}_{a=0,1}) := \sum_{a=0}^1 |a\rangle\langle a|_l \otimes u_n^{(a)}, \quad (4.6)$$

where l represents the vertical coordinate of the node $v_{l,j}$ of a control qubit and n represents the vertical coordinate of the node $v_{n,j}$ of a target qubit, and $u_n^{(a)}$ ($a = 0, 1$) are single qubit unitary operations on the target qubit, can be performed by using the method to implement a controlled unitary operation using a EPR pair proposed by [79]. If $n \neq l \pm 1$, all EPR pairs represented by edges between l and n are consumed to implement the two-qubit control unitary. When we do not specify the single qubit unitary operations $\{u_n^{(a)}\}$ on the target qubit we denote a two-qubit controlled unitary operation simply by $C_{l;n}$.

In addition to the two-qubit control unitary operations, we can perform three-qubit fully controlled unitary operations defined by

$$C_{l,m;n}(\{u_n^{(ab)}\}_{a,b=0,1}) := \sum_{a=0}^1 \sum_{b=0}^1 |ab\rangle\langle ab|_{lm} \otimes u_n^{(ab)}, \quad (4.7)$$

where l and m represent the vertical coordinates of the nodes $v_{l,j}$ and $v_{m,j}$ of two control qubits, respectively, and n represents the vertical coordinates of the node $v_{n,j}$ of a target qubit, and $u_n^{(ab)}$ ($a, b = 0, 1$) represents single qubit operations on the target qubit. (See Appendix A.1 for details of the LOCC protocol implementing three-qubit fully controlled unitary operations.) Note that the indices l , n and m should be taken such that $l < n < m$ or $m < n < l$. Similarly to the case of a two-qubit controlled unitary operation, we denote a three-qubit fully controlled unitary operation by $C_{l,m;n}$ when we do not specify the target single qubit operations. On the other hand, any four-qubit fully controlled unitary, where three of the four qubits are control qubits and the rest of the qubit is a target qubit, is not implementable on qubits that are all in different nodes of \mathcal{V}_j^v in a (k, N) -cluster network, if a single EPR pair is given for each edge in \mathcal{S}_j . Obviously any single qubit unitary operations can be implemented on any qubit.

We present a protocol to convert a given (k, N) -cluster network into quantum circuits. First (step 1 to step 3), we construct quantum circuits of unitary operations that are implementable on qubits in a set of vertically aligned nodes \mathcal{V}_j^v by LOCC assisted by the EPR pairs given for a set of vertically aligned edges \mathcal{S}_j for a certain j . Then (step 4), we repeat the procedure given by the first part (step 1 to step 3) for different j of $1 \leq j \leq N$.

The conversion protocol:

1. Draw k horizontal wire segments where each of the wire segments corresponds to a set of qubits at vertically aligned nodes \mathcal{V}_j^v .

2. Symbols representing two-qubit controlled unitary operations $C_{l;n}$ or three-qubit fully controlled unitary operations $C_{l,m;n}$ are added on the horizontal wire segments according to the following rules.
 - To represent $C_{l;n}$, draw a black dot representing a control qubit on the l -th wire, draw a vertical segment from the dot to the n -th wire segment and draw a box representing a target unitary operation on the n -th wire segment at the end of the vertical segment. Write index l at the side of the vertical segment between the horizontal wire segments. An example is shown in Fig. 4.2 i).
 - To represent $C_{l,m;n}$, draw two black dots representing control qubits on the l -th and m -th wire segments, draw vertical segments from each dot to the n -th wire and draw a box representing an arbitrary target unitary operation on the n -th wire segment at the end of the vertical segment. Write indices l and m at the sides of the vertical segment between the horizontal wire segments. An example is shown in Fig. 4.2 ii)
 - Multiple gates of $C_{l;n}$ or $C_{l,m;n}$ can be added as long as there are only one type of index appearing between the horizontal wire segments and no target unitary operation represented by a box is inserted between two black dots on a horizontal wire segment. An example of possible circuits generated in this protocol is shown in Fig. 4.2 iii). We also give an example of circuits that do not follow the rule in Fig. 4.2 iv).
3. Arbitrary single qubit unitary operations represented by boxes are inserted between before and after the sequence of $C_{l;n}$ and $C_{l,m;n}$ (but not during the sequence) obtained by step 2.
4. Repeat step 1 to step 3 for each $1 \leq j \leq N$ and connect all the i -th horizontal wire segments.

In Appendix A.2, we show that a unitary operation represented by the quantum circuit obtained by step 1 to step 3 of the conversion protocol is implementable in a set of vertically aligned nodes \mathcal{V}_j^y , namely, it is implementable by LOCC assisted by $(k-1)$ EPR pairs corresponding to a set of vertically aligned edges \mathcal{S}_j . As examples, quantum circuits converted from the $(2,3)$ -cluster and $(3,2)$ -cluster networks are shown in Fig. 4.3.

Our conversion method generates infinitely many quantum circuits in general. However for special cluster networks, standard forms of quantum circuits can be obtained. In Appendix A.3, we show that any converted circuit obtained from a $(2,3)$ -cluster network can be simulated by the circuit presented in Fig. 4.3 i), and any converted circuit obtained from a $(3,2)$ -cluster network can be simulated by the circuit presented in Fig.4.3 ii).

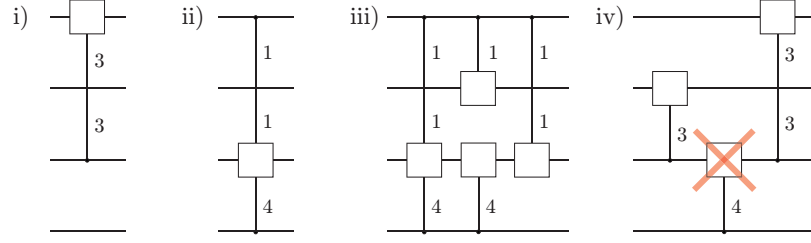


Figure 4.2: i) A symbol representing $C_{3;1}$. ii) A symbol representing $C_{1,4;3}$. iii) An example of circuits generated in step 2 of the conversion protocol. The index in the upper region is 1, that of index in the middle region is 1 and that of index in the lower region is 4. iv) This conversion is forbidden since there is a target unitary operation inserted between two black dots representing controlled qubits.

4.2 Upper bound of computation

In this section, we derive the condition for k -qubit unitary operations to be implementable over a given cluster network. We show that our conversion method presented in the previous section gives all implementable unitary operations over the (k, N) -cluster network for $k = 2, 3$.

Theorem 1. *If i) a k -qubit unitary operation U is deterministically implementable over the (k, N) -cluster network ($k \geq 2, N \geq 1$), then ii) the matrix representation of U in terms of the computational basis U^M can be decomposed into*

$$U^M = V_1^M V_2^M \dots V_N^M, \quad (4.8)$$

where each V_i^M is a 2^k by 2^k unitary matrix such that

$$\begin{aligned} V_i^M = & \sum_{a_1=0}^1 \sum_{a_2=0}^1 \dots \sum_{a_{k-1}=0}^1 E_{1,i}^{(a_1)} \otimes E_{2,i}^{(a_1, a_2)} \otimes E_{3,i}^{(a_2, a_3)} \\ & \otimes \dots \otimes E_{k-1,i}^{(a_{k-2}, a_{k-1})} \otimes E_{k,i}^{(a_{k-1})}, \end{aligned} \quad (4.9)$$

where $E_{i,j}^{(m,n)}$ and $E_{i,j}^{(m)}$ are 2 by 2 complex matrices.

To prove Theorem 1, we use Lemma 4 represented in Appendix A.4 about a class of bipartite *separable maps* that preserves entanglement. A bipartite separable map Γ_{sep} is a completely positive and trace preserving (CPTP) map as follows:

$$\Gamma_{sep}(\rho_{AB}) = \sum_k (A_k \otimes B_k) \rho_{AB} (A_k \otimes B_k)^\dagger, \quad (4.10)$$

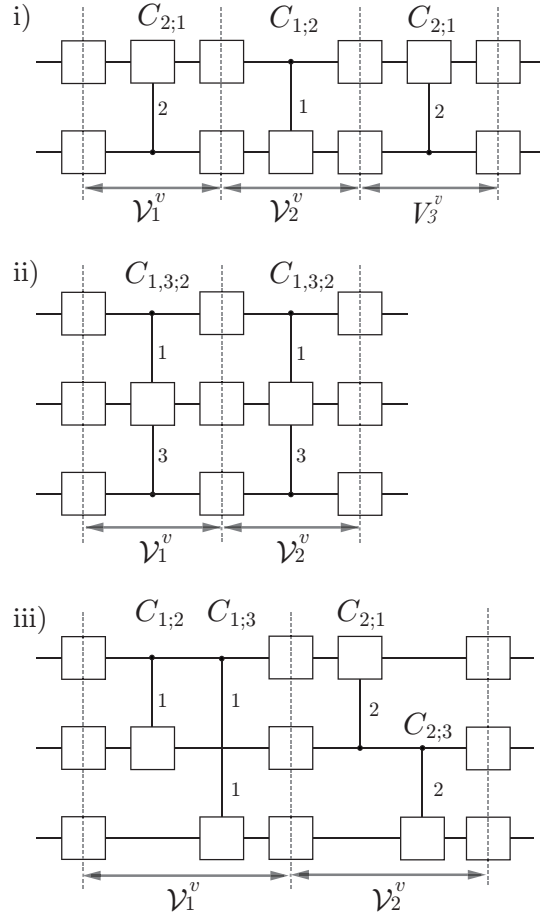


Figure 4.3: i) A converted quantum circuit from the (2,3)-cluster network. It is obtained by connecting three segments of circuits generated in step 1 to step 3 of the protocol corresponding to \mathcal{V}_1^v , \mathcal{V}_2^v and \mathcal{V}_3^v . It consists of two-qubit controlled unitary operations defined by $C_{l;n} = |0\rangle\langle 0|_l \otimes u_n^{(0)} + |1\rangle\langle 1|_l \otimes u_n^{(1)}$, where l denotes the wire segment of the control qubit and $u_n^{(i)}$ are arbitrary single qubit unitary operations on the n -th qubit, and arbitrary single qubit unitary operations are represented by boxes. ii) A converted quantum circuit from the (3,2)-cluster network. It consists of three-qubit fully controlled unitary operations defined by $C_{l,m;n} = |00\rangle\langle 00|_{l,m} \otimes u_n^{(00)} + |01\rangle\langle 01|_{l,m} \otimes u_n^{(01)} + |10\rangle\langle 10|_{l,m} \otimes u_n^{(10)} + |11\rangle\langle 11|_{l,m} \otimes u_n^{(11)}$, where l, m denotes the wire segments of the control qubits and $u_n^{(ij)}$ are arbitrary single qubit unitary operations on the n -th qubit. iii) Another converted quantum circuit obtainable from the (3,2)-cluster network.

where $\sum_k (A_k \otimes B_k)^\dagger (A_k \otimes B_k) = \mathbb{I}_A \otimes \mathbb{I}_B$. Since quantum network coding is equivalent to performing LOCC assisted by the resource state in our setting, we have to analyze multipartite LOCC. However, the analysis of multipartite LOCC is extremely difficult. Thus, we analyze multipartite separable maps, which are much easier to analyze than LOCC due to their simple structure. Note that a set of separable maps is exactly larger than that of LOCC [43, 44, 45, 64].

Proof of Theorem 1. Denote by $\mathcal{H}_{\mathcal{I}_Q} = \otimes_{i=1}^k \mathcal{H}_{I_i}$ and $\mathcal{H}_{\mathcal{O}_Q} = \otimes_{i=1}^k \mathcal{H}_{O_i}$ the Hilbert spaces of k input qubits and k output qubits, respectively. By introducing another ancillary Hilbert space $\mathcal{H}_{I'_i}$ at the input nodes $v_{i,1}$, denote the Hilbert space of k qubits by $\mathcal{H}_{\mathcal{I}'_Q} = \otimes_{i=1}^k \mathcal{H}_{I'_i}$. A joint state of k copies of the EPR pairs in $\mathcal{H}_{\mathcal{I}_Q} \otimes \mathcal{H}_{\mathcal{I}'_Q}$ is denoted by

$$|\mathbb{I}\rangle := \frac{1}{\sqrt{D}} \sum_i |i\rangle_{\mathcal{I}_Q} |i\rangle_{\mathcal{I}'_Q} = \otimes_{i=1}^k |\Phi^+\rangle_{I_i, I'_i}$$

where $D = \dim(\mathcal{H}_{\mathcal{I}_Q}) = 2^k$. If $U \in \mathbf{U}(\mathcal{H}_{\mathcal{I}_Q} : \mathcal{H}_{\mathcal{O}_Q})$ is deterministically implementable over a (k, N) -cluster network for $k \geq 2$ and $N \geq 1$, and we consider applying U on $|\mathbb{I}\rangle$. That is, there exists a LOCC map Γ such that

$$\frac{1}{D} \sum_{i,j} \Gamma(|i\rangle\langle j|_{\mathcal{I}_Q} \otimes |\Phi\rangle\langle\Phi|_{\mathcal{R}} \otimes |i\rangle\langle j|_{\mathcal{I}'_Q}) = |U\rangle\langle U|, \quad (4.11)$$

where $|\Phi\rangle_{\mathcal{R}}$ is the resource state of the (k, N) -cluster network and $|U\rangle$ is defined by

$$|U\rangle := (U \otimes \mathbb{I})|\mathbb{I}\rangle \in \mathcal{H}_{\mathcal{O}_Q} \otimes \mathcal{H}_{\mathcal{I}'_Q}. \quad (4.12)$$

By defining a map represented by the left hand side of Eq. (4.11) as $\Gamma'(|\Phi\rangle\langle\Phi|_{\mathcal{R}}) := \frac{1}{D} \sum_{i,j} \Gamma(|i\rangle\langle j|_{\mathcal{I}_Q} \otimes |\Phi\rangle\langle\Phi|_{\mathcal{R}} \otimes |i\rangle\langle j|_{\mathcal{I}'_Q})$, where Γ' is also a LOCC map if we assume two qubits belonging to \mathcal{H}_{I_i} and $\mathcal{H}_{I'_i}$ are in the same input node for all i . Since any LOCC maps are separable maps, there exists a separable map Γ'_{sep} satisfying

$$\Gamma'_{sep}(|\Phi\rangle\langle\Phi|_{\mathcal{R}}) = |U\rangle\langle U|, \quad (4.13)$$

if U is deterministically implementable over a (k, N) -cluster network. Since Γ'_{sep} is a map from a pure state to a pure state, the action of Γ'_{sep} represented by Eq.(4.13) can be equivalently given by the existence of a set of linear operators (the Kraus operators) $\{A_{i,j}^m\}_m$ for each node $v_{i,j}$ and a probability distribution $\{p_m\}$ such that

$$\forall m; \otimes_{i=1}^k \otimes_{j=1}^N A_{i,j}^m |\Phi\rangle_{\mathcal{R}} = \sqrt{p_m} |U\rangle, \quad (4.14)$$

$$\sum_m \otimes_{i=1}^k \otimes_{j=1}^N (A_{i,j}^{m\dagger} A_{i,j}^m) = \mathbb{I}, \quad (4.15)$$

where

$$\begin{aligned}
A_{i,1}^m &\in \mathbf{L}(\mathcal{H}_{v_{i,1}} : \mathcal{H}_{I'_i}) \\
&\quad (1 \leq i \leq k), \\
A_{i,j}^m &\in \mathbf{L}(\mathcal{H}_{v_{i,j}} : \mathbb{C}) \\
&\quad (1 \leq i \leq k, 2 \leq j \leq N-1), \\
A_{i,N}^m &\in \mathbf{L}(\mathcal{H}_{v_{i,N}} : \mathcal{H}_{O_i}) \\
&\quad (1 \leq i \leq k),
\end{aligned} \tag{4.16}$$

and $\mathcal{H}_{v_{i,j}}$ is the Hilbert space of qubits of the resource state at node $v_{i,j}$ defined by

$$\begin{aligned}
\mathcal{H}_{v_{i,j}} &= \mathcal{H}_{S_{i,j}} \otimes \mathcal{H}_{K_{i,j}} \\
\mathcal{H}_{S_{i,j}} &= \begin{cases} \mathcal{H}_{S_{1,j}^1} & (i=1) \\ \mathcal{H}_{S_{i,j}^1} \otimes \mathcal{H}_{S_{i,j}^2} & (2 \leq i \leq k-1) \\ \mathcal{H}_{S_{k,j}^2} & (i=k) \end{cases} \\
\mathcal{H}_{K_{i,j}} &= \begin{cases} \mathcal{H}_{K_{i,1}^1} & (j=1) \\ \mathcal{H}_{K_{i,j}^1} \otimes \mathcal{H}_{K_{i,j}^2} & (2 \leq j \leq N-1) \\ \mathcal{H}_{K_{i,N}^2} & (j=N) \end{cases}
\end{aligned} \tag{4.17}$$

First, letting $E_m = \otimes_{i=1}^k A_{i,1}^m$, $F_m = \otimes_{i=1}^k \otimes_{j=2}^N A_{i,j}^m$ and applying Lemma 4 presented in Appendix A.4, we obtain for all $\{m | p_m \neq 0\}$,

$$\exists \alpha_{1,m} > 0, \exists V_{1,m}^M \in \mathbf{U}(\mathbb{C}^D); E_m^M = \alpha_{1,m} V_{1,m}^M, \tag{4.20}$$

where $\mathbf{U}(\mathbb{C}^D)$ is the set of D by D unitary matrices and E_m^M is a D by D matrix satisfying

$$(E_m^M)_{a,b} = \langle a | \mathcal{I}'_Q (\otimes_{i=1}^k A_{i,1}^m) | A_b \rangle_{S_{*,1}^*, K_{*,1}^1}$$

and

$$|A_b\rangle_{S_{*,1}^*, K_{*,1}^1} = \otimes_{i=1}^{k-1} |\Phi^+\rangle_{S_{i,1}^1, S_{i+1,1}^2} \otimes |b\rangle_{K_{1,1}^1, \dots, K_{k,1}^1}.$$

Let

$$A_{1,1}^m = \sum_{a_1=0}^1 \langle a_1 |_{S_{1,1}^1} \otimes E_{1,1}^{(a_1),m} \tag{4.21}$$

$$\begin{aligned}
A_{i,1}^m &= \sum_{a_1=0}^1 \sum_{a_2=0}^1 \langle a_1 |_{S_{i,1}^1} \langle a_2 |_{S_{i,1}^2} \otimes E_{i,1}^{(a_1, a_2),m} \\
&\quad (2 \leq i \leq k-1)
\end{aligned} \tag{4.22}$$

$$A_{k,1}^m = \sum_{a_1=0}^1 \langle a_1 |_{S_{k,1}^2} \otimes E_{k,1}^{(a_1),m} \tag{4.23}$$

where $E_{1,1}^{(a_1),m} \in \mathbf{L}(\mathcal{H}_{K_{1,1}^1} : \mathcal{H}_{I'_1})$, $E_{i,1}^{(a_1,a_2),m} \in \mathbf{L}(\mathcal{H}_{K_{i,1}^1} : \mathcal{H}_{I'_i})$ and $E_{k,1}^{(a_1),m} \in \mathbf{L}(\mathcal{H}_{K_{k,1}^1} : \mathcal{H}_{I'_k})$. Thus, $V_{1,m}^M$ can be decomposed into

$$V_{1,m}^M = \sum_{a_1, \dots, a_{k-1}=0}^1 E_{1,1}^{(a_1),m} \otimes E_{2,1}^{(a_1,a_2),m} \otimes \dots \otimes E_{k-1,1}^{(a_{k-2},a_{k-1}),m} \otimes E_{k,1}^{(a_{k-1}),m}. \quad (4.24)$$

Note that we identify a linear operation and its matrix representation in the computational basis, e.g., $E_{1,1}^{(a_1),m}$ is a 2 by 2 complex matrix.

Next, letting $E_m = \otimes_{i=1}^k \otimes_{j=1}^2 A_{i,j}^m$, $F_m = \otimes_{i=1}^k \otimes_{j=3}^N A_{i,j}^m$ and using Lemma 4 represented in Appendix A.4, we obtain for all $\{m | p_m \neq 0\}$,

$$\exists \alpha_{2,m} > 0, \exists V_{2,m}^M \in \mathbf{U}(\mathbb{C}^D); E_m^M = \alpha_{2,m} V_{2,m}^M, \quad (4.25)$$

where E_m^M is a $D \times D$ matrix such that

$$(E_m^M)_{a,b} = \langle a |_{\mathcal{I}'_Q} (\otimes_{i=1}^k \otimes_{j=1}^2 A_{i,j}^m) | A_b \rangle_{S_{*,1}^*, S_{*,2}^*, K_{*,1}^1, K_{*,2}^*}$$

and

$$\begin{aligned} |A_b \rangle_{S_{*,1}^*, S_{*,2}^*, K_{*,1}^1, K_{*,2}^*} &= \otimes_{i=1}^{k-1} |\Phi^+\rangle_{S_{i,1}^1, S_{i+1,1}^2} \\ &\otimes_{i=1}^{k-1} |\Phi^+\rangle_{S_{i,2}^1, S_{i+1,2}^2} \otimes_{i=1}^k |\Phi^+\rangle_{K_{i,1}^1, K_{i,2}^2} \\ &\otimes |b \rangle_{K_{1,2}^1, \dots, K_{k,2}^1}. \end{aligned}$$

Let

$$A_{1,2}^m = \sum_{a_1=0}^1 \langle a_1 |_{S_{1,2}^1} \otimes E_{1,2}^{(a_1),m} \quad (4.26)$$

$$A_{i,2}^m = \sum_{a_1=0}^1 \sum_{a_2=0}^1 \langle a_1 |_{S_{i,2}^1} \langle a_2 |_{S_{i,2}^2} \otimes E_{i,2}^{(a_1,a_2),m} \quad (2 \leq i \leq k-1) \quad (4.27)$$

$$A_{k,2}^m = \sum_{a_1=0}^1 \langle a_1 |_{S_{k,2}^2} \otimes E_{k,2}^{(a_1),m}, \quad (4.28)$$

where $E_{1,2}^{(a_1),m} \in \mathbf{L}(\mathcal{H}_{K_{1,2}^1} \otimes \mathcal{H}_{K_{1,2}^2} : \mathbb{C})$, $E_{i,2}^{(a_1,a_2),m} \in \mathbf{L}(\mathcal{H}_{K_{i,2}^1} \otimes \mathcal{H}_{K_{i,2}^2} : \mathbb{C})$ and $E_{k,2}^{(a_1),m} \in \mathbf{L}(\mathcal{H}_{K_{k,2}^1} \otimes \mathcal{H}_{K_{k,2}^2} : \mathbb{C})$. By a straightforward calculation, $V_{2,m}^M$ are shown to be decomposed into

$$V_{2,m}^M = V_{1,m}^M \sum_{a_1, \dots, a_{k-1}=0}^1 E_{1,2}'^{(a_1),m} \otimes E_{2,2}'^{(a_1,a_2),m} \otimes \dots \otimes E_{k-1,2}'^{(a_{k-2},a_{k-1}),m} \otimes E_{k,2}'^{(a_{k-1}),m}, \quad (4.29)$$

where $E_{1,2}^{(a_1),m}$, $E_{i,2}^{(a_1,a_2),m}$, and $E_{k,2}^{(a_1),m}$ are 2×2 complex matrices.

Iterating this procedure, we obtain for all $\{m | p_m \neq 0\}$,

$$\exists \alpha > 0, \exists W^M \in \mathbf{U}(\mathbb{C}^D); E_m^M = \alpha W^M, F_m^M = \frac{\sqrt{p_m}}{\alpha} \overline{W^M}, \quad (4.30)$$

where W^M and $\overline{W^M}$ can be decomposed into

$$W^M = V_1^M V_2^M \cdots V_{N-1}^M \quad (4.31)$$

$$\overline{W^M} = U^{M\dagger} V_N^M, \quad (4.32)$$

and $V_i^M = \sum_{a_1, \dots, a_{k-1}=0}^1 E_{1,i}^{(a_1)} \otimes E_{2,i}^{(a_1,a_2)} \otimes \cdots \otimes E_{k-1,i}^{(a_{k-2},a_{k-1})} \otimes E_{k,i}^{(a_{k-1})} \in \mathbf{U}(\mathbb{C}^D)$. U^M can be decomposed into the form of Eq.(4.8) since $\overline{V_i^M}$ and $V_i^{M\dagger}$ can be decomposed into the form of Eq.(4.9).

□

In the case of the $(2, N)$ -cluster networks, which we call N -bridge *ladder networks*, V_i is locally unitarily equivalent to the two-qubit controlled unitary operation since its operator Schmidt rank is 2 [91]. Thus, statements i) and ii) in Theorem 1 are equivalent since a sequence of N two-qubit controlled unitary operations is implementable by the converted circuit presented in Fig. 4.3 i). Then we obtain the following theorem for the ladder networks.

Theorem 2. *A unitary operation U is deterministically implementable over the N -bridge ladder network if and only if $\text{KC}\#(U) \leq N$, where $\text{KC}\#(U)$ is the Kraus-Cirac number of a two-qubit unitary operator U , which is the number of non-zero parameters x, y, z in Eq. (3.11) characterizing the global part of U .*

This theorem is proven by using the following lemma relating the Kraus-Cirac number of a two-qubit unitary operation and the decomposition of the unitary operation into controlled unitary operations shown in [87].

Lemma 1. *Consider a set of two-qubit unitary operators \mathbf{U}_c that is locally unitarily equivalent to a controlled unitary operator. The decomposition of a two-qubit unitary operator U into a shortest sequence of two-qubit unitary operators in \mathbf{U}_c depends on the Kraus-Cirac number $\text{KC}\#(U)$ of U as*

$$\begin{aligned} \{U \in SU(4) | \text{KC}\#(U) \leq 1\} &= \{U | U \in \mathbf{U}_c\} \\ \{U \in SU(4) | \text{KC}\#(U) \leq 2\} &= \{UV | U, V \in \mathbf{U}_c\} \\ \{U \in SU(4) | \text{KC}\#(U) \leq 3\} &= \{UVW | U, V, W \in \mathbf{U}_c\}. \end{aligned}$$

Proof of Theorem 2. Since $\text{KC}\#(U)$ is less than or equal to N if and only if U can be decomposed into N two-qubit controlled unitary operations as shown in Lemma 1, and N two-qubit controlled unitary operations are deterministically implementable over N -bridge ladder network, Theorem 3 is straightforwardly shown. \square

We also show that statements i) and ii) are equivalent in the case of the $(3, N)$ -cluster networks in Appendix A.5.

4.3 Butterfly, grail and square networks

For classical network coding, it has been shown that there exists a network coding protocol over a 2-pair network, which has two input nodes and two output nodes, if and only if the network has at least one of the butterfly, grail and identity substructures [80]. Thus any classical network coding protocol over a 2-pair network can be reduced into a combination of protocols over the butterfly, grail or identity networks, and these networks are fundamental primitive networks for classical network coding. As a first step to investigate implementability of quantum computation over general 2-pair quantum networks, we investigate implementability of two-qubit unitary operations over the butterfly and grail networks in this section by using the method converting a (k, N) -cluster network into quantum networks introduced in Section 4.1.

By constructing a protocol for implementing $U_{\text{global}}(x, y, z)$ defined in Eq.(3.11) for arbitrary x, y, z , we obtain the following theorem.

Theorem 3. *Any two-qubit unitary operation is deterministically implementable over the butterfly network.*

Proof. For implementability of $U_{\text{global}}(x, y, z)$ over the butterfly network represented by the left hand side of Fig. 4.4, we consider a $(3, 2)$ -cluster network represented by the right hand side of Fig. 4.4 by assigning the nodes $\{i_1, n_1, i_2, o_1, n_2, o_2\}$ of the butterfly network to the nodes $\{v_{1,1}, v_{2,1}, v_{3,1}, v_{1,2}, v_{2,2}, v_{3,2}\}$ of the $(3, 2)$ -cluster network, respectively. In this assignment, the correspondence of the edges of the butterfly network and the horizontal and vertical sets of edges $\mathcal{K}_1, \mathcal{S}_1, \mathcal{S}_2$ of the $(3, 2)$ -cluster network is given by

$$\begin{aligned} \{E_1, E_5, E_3\} &\leftrightarrow \mathcal{K}_1, \\ \{E_2, E_4\} &\leftrightarrow \mathcal{S}_1, \\ \{E_6, E_7\}, &\leftrightarrow \mathcal{S}_2. \end{aligned} \tag{4.33}$$

Thus any two-qubit unitary operation is deterministically implementable over the butterfly network if any $U_{\text{global}}(x, y, z)$ in the form of Eq. (3.11) is deterministically

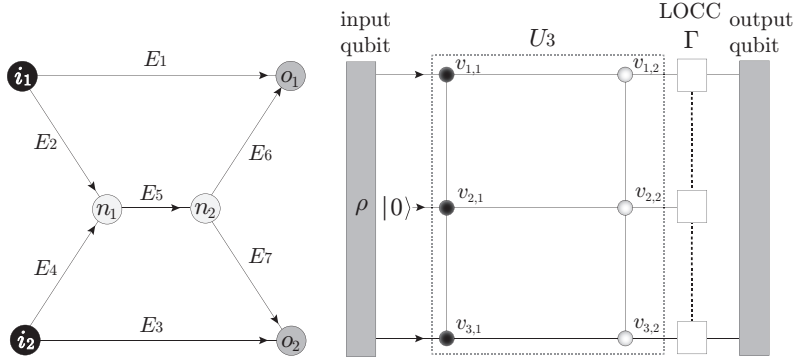


Figure 4.4: The nodes i_1, i_2, o_1, o_2, n_1 and n_2 of the butterfly network correspond to the nodes $v_{1,1}, v_{3,1}, v_{1,2}, v_{3,2}, v_{2,1}$ and $v_{2,2}$ of a $(3, 2)$ -cluster network each other. The *two-qubit* unitary operation $U_{global}(x, y, z) = e^{i(xX \otimes X + yY \otimes Y + zZ \otimes Z)}$ is implementable over a $(3, 2)$ -cluster network by fixing an input state at the node $v_{2,1}$ at $|0\rangle$, performing an appropriate *three-qubit* unitary operation U_3 and performing an appropriate LOCC map Γ consisting of a measurement on the qubit at the output node $v_{2,2}$ and the conditional operations on the other output nodes $v_{1,2}$ and $v_{3,2}$ depending on the measurement outcome.

implementable over the $(3, 2)$ -cluster network where input states are given at nodes $v_{1,1}$ and $v_{3,1}$ and output states are obtained at nodes $v_{1,2}$ and $v_{3,2}$, since the topology of the butterfly network is the same as that of the $(3, 2)$ -cluster network.

We construct a protocol implementing two-qubit unitary $U_{global}(x, y, z)$ by setting a fixed input state at node $v_{2,1}$ and arbitrary two-qubit input state at nodes $v_{1,1}$ and $v_{3,1}$ as a three-qubit input state at input nodes $\mathcal{I} = \{v_{1,1}, v_{2,1}, v_{3,1}\}$, and implementing a three-qubit unitary operation denoted by U_3 over the $(3, 2)$ -cluster network followed by an LOCC map denoted by Γ performed at output nodes $\mathcal{O} = \{v_{1,2}, v_{2,2}, v_{3,2}\}$. Recall that a unitary operation of represented by the quantum circuit shown in Fig. 4.3 ii) is implementable over the $(3, 2)$ -cluster network. That is, two three-qubit fully controlled unitary operations $C_{1,3;2}$ are implementable, one at nodes \mathcal{I} and another at nodes \mathcal{O} . The following protocol shows that by choosing appropriate parameters for one of the three-qubit fully controlled unitary operations and one of single-qubit local unitary operations in U_3 , we can implement $U_{global}(x, y, z)$ with arbitrary x, y, z .

The protocol for implementing $U_{global}(x, y, z)$:

1. An arbitrary two-qubit input state ρ is given for qubits at input nodes $v_{1,1}$ and $v_{3,1}$ and a fixed input state $|0\rangle$ is prepared for the qubit at node $v_{2,1}$.
2. Implement U_3 of which the quantum circuit representation is given by the

left shaded part of Fig.4.5 over the (3, 2)-cluster network.

- (a) All single-qubit unitary operations appearing in the circuit representation of U_3 are trivially performed at each node.
- (b) The first fully controlled unitary operation implemented at input nodes \mathcal{I} using the EPR pairs represented by vertical edges \mathcal{S}_1 is given by $C_{1,3;2}(\{u_n^{(ab)}\}_{a,b=0,1})$ where $u_n^{(00)} = u_n^{(11)} = \mathbb{I}$ and $u_n^{(01)} = u_n^{(10)} = Z$.
- (c) To transmit a qubit state from input nodes $v_{i,1}$ to output node $v_{i,2}$ for $i = 1, 2, 3$, quantum teleportation is performed for each i by using the EPR pair represented by a horizontal edge in \mathcal{K}_1 .
- (d) The second fully controlled unitary operation implemented at output nodes \mathcal{O} contains parameters y and z and is given by $C'_{1,3;2}(\{w_n^{(ab)}\}_{a,b=0,1})$ where

$$\begin{aligned} w_n^{(00)} &= w_n^{(11)} = e^{i(z-y)}|0\rangle\langle 0| - ie^{i(z+y)}|1\rangle\langle 1|, \\ w_n^{(01)} &= w_n^{(10)} = e^{-i(z-y)}|0\rangle\langle 0| - ie^{-i(z+y)}|1\rangle\langle 1|. \end{aligned}$$

- (e) After implementing $C'_{1,3;2}(\{w_n^{(ab)}\}_{a,b=0,1})$, a single-qubit unitary operation parameterized by x given by

$$u(x) = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{ix} & -ie^{-ix} \\ e^{ix} & ie^{-ix} \end{pmatrix} \quad (4.34)$$

is performed at node $v_{2,2} \in \mathcal{O}$.

3. Perform an LOCC map Γ at output nodes \mathcal{O} of which the quantum circuit representation is given by the right shaded part of Fig.4.5. The map Γ consists of the following three steps.
 - (a) Perform a projective measurement on the qubit at node $v_{2,2}$ in the computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$.
 - (b) Classically communicate the measurement outcome $k \in \{0, 1\}$ from node $v_{2,2}$ to $v_{1,2}$ and also to $v_{3,2}$.
 - (c) If $k = 1$, perform a conditional operation X on output qubits at nodes $v_{1,2}$ and $v_{3,2}$, otherwise do nothing.

This protocol maps any input state ρ given at input nodes $v_{1,1}$ and $v_{3,1}$ to

$$U_{global}(x, y, z)\rho U_{global}^\dagger(x, y, z) = \Gamma(U_3(\rho \otimes |0\rangle\langle 0|)U_3^\dagger) \quad (4.35)$$

at output nodes $v_{1,2}$ and $v_{3,2}$ where $|0\rangle$ represents the fixed input state at node $v_{2,1}$. See Appendix A.6 for details of calculations. It is straightforward to translate the

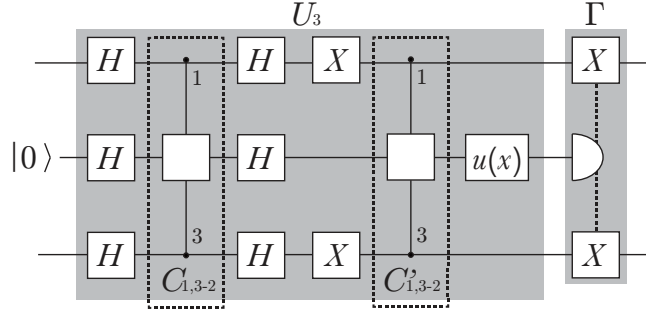


Figure 4.5: A quantum circuit representation of a three-qubit unitary operation U_3 (the left shaded part) and an LOCC map Γ (the right shaded part) used in a protocol for implementing a two-qubit unitary operation $U_{global}(x, y, z) = e^{i(xX \otimes X + yY \otimes Y + zZ \otimes Z)}$ on the first and third qubits. The input state of the second qubit is fixed in $|0\rangle$. The single qubit unitary operations represented by boxes are given by $H = (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)/\sqrt{2}$, $u(x) = H(e^{ix}|0\rangle\langle 0| - ie^{-ix}|1\rangle\langle 1|)$ and $X = |0\rangle\langle 1| + |1\rangle\langle 0|$. The target single-qubit unitary operations of the first three-qubit fully controlled unitary operation $C_{1,3,2}(\{u_n^{(ab)}\}_{a,b=0,1})$ are given by $u_n^{(00)} = u_n^{(11)} = \mathbb{I}$ and $u_n^{(01)} = u_n^{(10)} = Z$. The target single-qubit unitary operations of the second three-qubit fully controlled unitary operation $C'_{1,3,2}(\{w_n^{(ab)}\}_{a,b=0,1})$ are given by $w_n^{(00)} = w_n^{(11)} = e^{i(z-y)}|0\rangle\langle 0| - ie^{i(z+y)}|1\rangle\langle 1|$ and $w_n^{(01)} = w_n^{(10)} = e^{-i(z-y)}|0\rangle\langle 0| - ie^{-i(z+y)}|1\rangle\langle 1|$. The half circle symbol represents a projective measurement in the computational basis $\{|k\rangle\langle k|\}_{k=0,1}$. The single qubit operations (boxes) connected to the measurement symbol by dotted lines represent conditional unitary operations performed only if the measurement result is $k = 1$ and do nothing (or perform \mathbb{I}) if $k = 0$.

protocol over the $(3, 2)$ -cluster network to a protocol to implement $U_{global}(x, y, z)$ over the butterfly network by using the correspondence of vertices and edges. Thus, $U_{global}(x, y, z)$ is deterministically implementable over the butterfly network. \square

For implementability of $U_{global}(x, y, z)$ over the grail network, we consider a $(2, 3)$ -cluster network by assigning the nodes $\{n_1, n_2, o_1, i_2, n_3, n_4\}$ of the grail network to the nodes $\{v_{1,1}, v_{1,2}, v_{1,3}, v_{2,1}, v_{2,2}, v_{2,3}\}$ of the $(2, 3)$ -cluster network, respectively (Fig. 4.6). The $(2, 3)$ -cluster network can be converted to a quantum circuit containing three controlled NOT gates and arbitrary single unitary operations that are inserted between the controlled NOT gates. It is shown that any two-qubit unitary operations $U_{global}(x, y, z)$ can be decomposed into three controlled NOT gates and single unitary operations inserted between the controlled NOT gates [92]. Thus any two-qubit controlled unitary operation is deterministi-

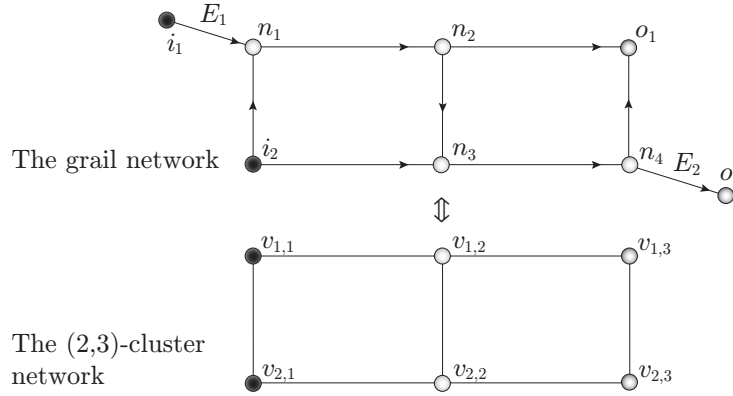


Figure 4.6: The nodes n_1 , n_2 , o_1 , i_2 , n_3 and n_4 of the grail network correspond to the nodes $v_{1,1}$, $v_{1,2}$, $v_{1,3}$, $v_{2,1}$, $v_{2,2}$ and $v_{2,3}$ of a (2, 3)-cluster network, respectively. The set of all unitary operations implementable over the (2, 3)-cluster network is also implementable over the grail network, since we can use the edges E_1 and E_2 for just teleporting qubits and the rest of the network forms the (2, 3)-cluster network, with which any two-qubit unitary operation is implementable.

cally implementable over the grail network.

4.4 Probabilistic computation

In this section, we investigate the probabilistic implementation of unitary operations. There is no classical network coding protocol to send single bits from $v_{1,1}$ to $v_{2,2}$ and from $v_{2,1}$ to $v_{1,2}$ over a (2, 2)-cluster network since there is no butterfly, grail or identity substructure. This task corresponds to implementing a SWAP operator in quantum network coding. It is interesting to know whether there exists a task that is not achievable by classical network coding but a corresponding task is achievable in a quantum setting or not. We give a negative result in this section. Using Theorem 2, we see that a SWAP operator is not deterministically implementable over a (2, 2)-cluster network, which is a 2-bridge ladder network, since the Kraus-Cirac number of the SWAP operator is 3. Furthermore, we show that the SWAP operator is not implementable even *probabilistically* in this section.

Theorem 4. *A k -qubit unitary operation U is probabilistically implementable over the (k, N) -cluster network ($k \geq 2$, $N \geq 1$) if and only if the matrix representation of U in terms of the computational basis U^M can be decomposed into*

$$U^M = F_1^M F_2^M \cdots F_N^M, \quad (4.36)$$

where each F_i^M is a 2^k by 2^k complex matrix that can be decomposed in the same way as Eq. (4.9)

Proof. Similar to the case of deterministic implementation, we consider applying $U \in \mathbf{U}(\mathcal{H}_{\mathcal{I}_Q} : \mathcal{H}_{\mathcal{O}_Q})$ on a part of k maximally entangled states $|\mathbb{I}\rangle \in \mathcal{H}_{\mathcal{I}_Q} \otimes \mathcal{H}_{\mathcal{I}_Q}$. Then U is probabilistically implementable over the (k, N) -cluster network ($k \geq 2, N \geq 1$) if and only if there exists a stochastic LOCC (SLOCC) map Γ'' and non-zero probability $p > 0$ such that

$$\Gamma''(|\Phi\rangle\langle\Phi|_{\mathcal{R}}) = p|U\rangle\langle U|, \quad (4.37)$$

where $|\Phi\rangle_{\mathcal{R}}$ is the resource state of the (k, N) -cluster network and $|U\rangle \in \mathcal{H}_{\mathcal{O}_Q} \otimes \mathcal{H}_{\mathcal{I}_Q}$ is defined by Eq. (4.12). Eq. (4.37) is equivalent to the statement that there exists a set of linear operators $\{A_{i,j}\}$ and non-zero probability $p > 0$ such that

$$\otimes_{i=1}^k \otimes_{j=1}^N A_{i,j} |\Phi\rangle_{\mathcal{R}} = \sqrt{p}|U\rangle. \quad (4.38)$$

The conditions of $\{A_{i,j}\}$ given by Eq. (4.38) is similar to the conditions of Kraus operators $\{A_{i,j}^m\}_m$ given by Eq. (4.14) presented in the proof of Theorem 1. The index m is dropped in Eq. (4.38) since the map we consider is SLOCC instead of LOCC considered in Theorem 1. By taking the correspondence between $A_{i,j}$ and $A_{i,j}^m$, we obtain a decomposition of the form presented in Eq. (4.36). \square

Lemma 2. *A SWAP operation $U^{SWAP} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$ is not implementable over the 2-bridge ladder network with non-zero probability.*

Proof. By using Theorem 4, the SWAP operation is probabilistically implementable over the $(2, 2)$ -cluster network (2-bridge ladder network) if and only if there exists a linear operation $P, Q \in \mathbf{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ and $E_{i,j}^{(k)} \in \mathbf{L}(\mathcal{H}_i)$ such that

$$U^{SWAP} = PQ, \quad (4.39)$$

$$P = E_{1,1}^{(0)} \otimes E_{2,1}^{(0)} + E_{1,1}^{(1)} \otimes E_{2,1}^{(1)} \quad (4.40)$$

$$Q = E_{1,2}^{(0)} \otimes E_{2,2}^{(0)} + E_{1,2}^{(1)} \otimes E_{2,2}^{(1)}, \quad (4.41)$$

where $\mathcal{H}_i = \mathbb{C}^2$. For any linear operations M , there exists the operator Schmidt decomposition, and we can define the *operator Schmidt rank* $\text{Op}\#_1^2(M)$, which is the number of non-zero coefficients of the operator Schmidt decomposition. Since P and Q can be decomposed into Eq.(4.40) and Eq.(4.41), we can derive

$$\text{Op}\#_1^2(P) \leq 2, \quad (4.42)$$

$$\text{Op}\#_1^2(Q) \leq 2. \quad (4.43)$$

Since $\text{Op}\#_1^2(U^{SWAP}) = 4$, $\text{Op}\#_1^2(P) = \text{Op}\#_1^2(Q) = 2$. In [93], it is shown that if $\text{Op}\#_1^2(P) = 2$ and P is invertible, $\text{Op}\#_1^2(P^{-1}) = 2$. Thus, the SWAP operation is probabilistically implementable if and only if there exists linear operations $P, Q \in \mathbf{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that

$$Q = U^{SWAP}P, \quad (4.44)$$

$$\text{Op}\#_1^2(P) = 2, \text{ rank}(P) = 4 \quad (4.45)$$

$$\text{Op}\#_1^2(Q) = 2, \text{ rank}(Q) = 4. \quad (4.46)$$

In general, we can regard P as a matrix representation of a four qubit pure state $|\Phi\rangle_{1,2,3,4}$;

$$P = \sum_{i=1}^4 \langle i|_{1,2} |\Phi\rangle_{1,2,3,4} \langle i|_{1,2}. \quad (4.47)$$

Then, the following correspondences are obtained,

$$\text{rank}(P) = 4 \Leftrightarrow \text{Sch}\#_{1,2}^{3,4}(|\Phi\rangle) = 4, \quad (4.48)$$

$$\text{Op}\#_1^2(P) = 2 \Leftrightarrow \text{Sch}\#_{1,3}^{2,4}(|\Phi\rangle) = 2, \quad (4.49)$$

$$\text{Op}\#_1^2(U^{SWAP}P) = 2 \Leftrightarrow \text{Sch}\#_{1,4}^{2,3}(|\Phi\rangle) = 2, \quad (4.50)$$

where $\text{Sch}\#_{1,2}^{3,4}(|\Phi\rangle)$ is a Schmidt number in terms of a partition between qubit 1, 2 and qubit 3, 4. We show that there is no four qubit state simultaneously satisfying Eqs. (4.48), (4.49), and (4.50) in Appendix A.7. \square

Note that we have shown that U can be decomposed into a particular form represented by Eq.(4.8) *if* U is deterministically implementable in Theorem 1 and that U can be decomposed into a particular form represented by Eq.(4.36) *if and only if* U is probabilistically implementable in Theorem 4. And each factor F_i^M in Eq.(4.36) can be a non-unitary complex matrix while each factor V_i^M in Eq.(4.8) must be a unitary matrix. Whether there exists a difference between implementable unitary operations in the deterministic implementation and in the probabilistic implementation or not is an open problem.

Chapter 5

Summary and Discussions of Part II

5.1 Summary

We have investigated implementability of k -qubit unitary operations over the (k, N) -cluster networks where inputs and outputs of quantum computation are given in all separated nodes and quantum communication between nodes is restricted to sending just one-qubit while classical communication is freely allowed. We consider a one-shot scenario where we can use a given cluster network only once and exact implementation without error is required. We have presented a method to obtain quantum circuit representations of unitary operations implementable over a given cluster network. For the (k, N) -cluster networks with $k = 2, 3$, we have shown that our method provides all implementable unitary operations over the cluster network. As a first step to find the fundamental primitive networks of network coding for quantum settings, we have shown that both of the butterfly and grail networks are sufficient resources for implementing arbitrary two-qubit unitary operations, meanwhile the $(2, 2)$ -cluster network is not sufficient to implement arbitrary two-qubit unitary operations even probabilistically.

5.2 Discussions

- **Asymptotic implementability of unitary operations over the cluster networks**

In addition to the one-shot scenario, which we have focused on in this part, an *asymptotic scenario* is often considered in information science. For example, a capacity of a channel is usually given by the optimal transmission rate via the channel when asymptotically many uses of the channel is allowed. In

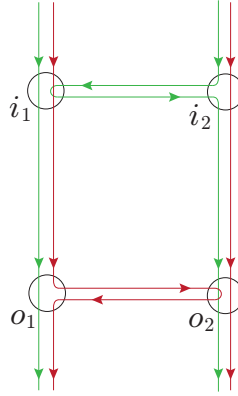


Figure 5.1: **Quantum computation with double uses of the square network.** In this case, any two-qubit unitary operations are implementable over the square network. The green paths and the red paths represent the first pair of qubits and the second pair of qubits, respectively. By performing a given two-qubit unitary operation at nodes i_1 on the first pair of qubits and o_2 on the second pair of qubits, any two-qubit unitary operation can be applied for two sets of initial states.

a similar way, implementable unitary operations with asymptotically many uses of a given cluster network can be considered. However, there is a remarkable gap between the one-shot and a multiple-shot scenario including the asymptotic scenario. For example, the set of unitary operations implementable over the square network $((2, 2)$ -cluster network) is the set of the unitary operators whose Kraus-Cirac number is smaller than or equal to 2 in the one-shot scenario. Meanwhile, it is easy to verify that arbitrary two-qubit unitary operations are implementable over the square network if the network can be used twice. The network coding scheme for this case is presented in Fig. 5.1. That is, the SWAP operation, corresponding to quantum communication from i_1 and i_2 to o_2 and o_1 respectively, is always implementable with double uses of the square network.

- **Implementability over a generalized cluster network.**

Our results can be applied to a *generalized cluster network* defined as follows.

Definition 6. A network $G = \{\mathcal{V}, \mathcal{E}, \mathcal{I}, \mathcal{O}\}$ is a *generalized cluster network*

if and only if for some $k \geq 1$ and $N \geq 1$,

$$\begin{aligned}\mathcal{V} &= \{v_{i,j}; 1 \leq i \leq k, 1 \leq j \leq N\} \\ \mathcal{I} &= \{v_{i,1}; 1 \leq i \leq k\} \\ \mathcal{O} &= \{v_{i,N}; 1 \leq i \leq k\} \\ \mathcal{E} &= \mathcal{S}_{sub} \cup \mathcal{K}\end{aligned}\tag{5.1}$$

where

$$\begin{aligned}\mathcal{S}_{sub} &\subseteq \mathcal{S}_{comp}, \\ \mathcal{S}_{comp} &= \{(v_{m,j}, v_{n,j}); 1 \leq m < n \leq k, 1 \leq j \leq N\}, \\ \mathcal{K} &= \{(v_{i,j}, v_{i,j+1}); 1 \leq i \leq k, 1 \leq j \leq N-1\}.\end{aligned}\tag{5.2}$$

In this case, if there exists a loop of vertical edges $\mathcal{L} \subseteq \mathcal{S}_{sub}$ such that for some j , L and $\{i_m\}_{m=1}^L$,

$$\mathcal{L} = \{e_1 = (v_{i_1,j}, v_{i_2,j}), e_2 = (v_{i_2,j}, v_{i_3,j}), \dots, e_L = (v_{i_L,j}, v_{i_1,j}) | e_m \neq e_n \text{ if } m \neq n\},\tag{5.3}$$

we can perform a cyclic permutation that transmits a qubit state from $v_{i_1,j}$ to $v_{i_2,j}$, from $v_{i_2,j}$ to $v_{i_3,j}$ and so on (by consuming EPR states corresponding to the looped vertical edges for teleportation) in addition to performing controlled unitary operations presented in Section 4.1. Thus, quantum computation over a generalized cluster network with a loop of vertical edges has more capability than that without a loop. Note that the implementable unitary operations over a generalized cluster network are still restricted by Theorem 1 and 4.

- **Quantum computation and MBQC over the butterfly network.**

In MBQC, a graph that has a *generalized flow* (gflow) is extensively studied since a unitary operation is always implementable over a graph state corresponding to such a graph irrespective of the angle α of each projective measurement defined in Eq.(3.7) with appropriate measurement corrections [94, 95].

Definition 7. (g, \prec) is a gflow of a graph (G, I, O) , where $g : O^c \rightarrow 2^{I^c}$ and \prec is a strict partial order over V , if and only if

- if $j \in g(i)$ then $i \prec j$
- if $j \in \text{Odd}(g(i))$ then $j = i$ or $i \prec j$
- $i \in \text{Odd}(g(i))$,

where $X^c = V \setminus X$, $Odd(K) = \{u \in V, |N_G(u) \cup K| = 1 \pmod{2}\}$ and $N_G(u)$ is the set of vertices neighboring u .

In [96], it was shown that a graph has a gflow if and only if the graph has a *focused gflow* defined as follows.

Definition 8. (g, \prec) is a focused gflow of a graph (G, I, O) , where $g : O^c \rightarrow 2^{I^c}$ and \prec is a strict partial order over V , if and only if

- if $j \in g(i)$ then $i \prec j$
- for all $u \in O^c$, $Odd(g(u)) \cap O^c = \{u\}$.

The butterfly network does not have a focused gflow as shown below while any two-qubit unitary operations are implementable over the butterfly network in our scenario.

Proposition 2. *The butterfly network does not have a focused gflow.*

Proof. The butterfly network consists of $I = \{i_1, i_2\}$, $O = \{o_1, o_2\}$, $V = \{n_1, n_2\} \cup I \cup O$ as presented in Fig. 3.2. $g(n_1)$ does not include n_1 since \prec is a strict partial order. If $g(n_1)$ includes o_1 or o_2 , $i_1 \in Odd(g(n_1))$ or $i_2 \in Odd(g(n_1))$. This contradicts the condition of the focused gflow. Thus, $g(n_1) = \{n_2\}$, i.e. $n_1 \prec n_2$. On the other hand, $\{n_1, o_1\} \subseteq g(n_2)$ or $n_1 \notin g(n_2) \wedge o_1 \notin g(n_2)$ since $i_1 \notin Odd(g(n_2))$. Similarly, $\{n_1, o_2\} \subseteq g(n_2)$ or $n_1 \notin g(n_2) \wedge o_2 \notin g(n_2)$ since $i_2 \notin Odd(g(n_2))$. Thus, $g(n_2) = \{n_1, o_1, o_2\}$ since $n_2 \in Odd(g(n_2))$. This is a contradiction to $n_1 \prec n_2$. \square

This implies that if we restrict the angle of a set of projective measurements in MBQC over the butterfly network, we can implement two-qubit unitary operations. It is unknown how to characterize an implementable unitary operations over a given network in MBQC where the angle of each projective measurement can be restricted. Our results give an upper bound of such an implementable unitary operations over the cluster network.

Part III

Role of entanglement and causal relation in DQC

Note that in this part, we mainly consider a bipartite scenario. Thus, we abbreviate bipartite (one-way or two-way) LOCC and bipartite SEP as LOCC and SEP, respectively. An extension to a multipartite scenario is given in discussions of this part.

Chapter 6

Resources for state discrimination

State discrimination is a task to discriminate states chosen from a given set of states $\{|\psi_i\rangle\}_i$ by performing a measurement. If the set contains non-orthogonal states, it is trivially impossible to discriminate them perfectly. However, even if the set contains only orthogonal states, it can be impossible to discriminate them perfectly when the state is shared between two parties and the measurement they can perform is somewhat restricted to be local. State discrimination under the restriction of operations to be local is called local state discrimination. Local state discrimination can be used for characterizing the non-locality of the set of states. It is shown that any two orthogonal pure states can be distinguished by using LOCC followed by local measurements [42] even if the states are maximally entangled states. However, several sets of orthogonal product states cannot be distinguished by using LOCC followed by local measurements [43, 45, 44]. Since any sets of orthogonal product states can be distinguished by using operations in SEP followed by local measurements, such results demonstrate the gap between LOCC and SEP. We give an example of local state discrimination tasks that cannot be achieved by LOCC but be achieved by SEP as follows.

Example: In [43], Bennett et al. have shown that a set of product states of two three-dimensional systems shared between Alice and Bob defined by

$$\begin{aligned} |\psi_{1(2)}\rangle_{AB} &= |0\rangle_A |0 \pm 1\rangle_B, & |\psi_{3(4)}\rangle_{AB} &= |0 \pm 1\rangle_A |2\rangle_B \\ |\psi_{5(6)}\rangle_{AB} &= |2\rangle_A |1 \pm 2\rangle_B, & |\psi_{7(8)}\rangle_{AB} &= |1 \pm 2\rangle_A |0\rangle_B, & |\psi_9\rangle_{AB} &= |1\rangle_A |1\rangle_B, \end{aligned} \tag{6.1}$$

where $\{|j\rangle\}_{j=0}^2$ is the computational basis of a three-level system, $|a \pm b\rangle := (|a\rangle \pm |b\rangle)/\sqrt{2}$, indices A and B represents Alice's share of the state and Bob's share of the state respectively, is not deterministically and perfectly distinguishable by any protocol described by a map belonging to LOCC followed by local measurements.

In this chapter, we focus on a set of orthonormal basis states and analyze the amount of entanglement required for discriminating the states by using one-way

LOCC and two-way LOCC. We assume classical communication of one-way LOCC is from Alice to Bob. Note that in both one-way LOCC and two-way LOCC, the discrimination task is achievable for any set of orthonormal basis states if sufficient amount of entanglement is shared between Alice and Bob since Alice can teleport her share of the state to Bob and then Bob can perform joint measurement to distinguish the state on the received state and his share of the state. As a result, we show that the amount of entanglement required for two-way LOCC is less than the lower bound for one-way LOCC in terms of a certain entanglement measure called the Schmidt rank. That is, entanglement and classical communication required for local state discrimination by using one-way LOCC can be substituted by less entanglement and more rounds of classical communication corresponding to two-way LOCC. We consider an orthonormal basis on a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$, and entanglement resource $|\Phi\rangle$ on the ancilla system $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ in this chapter. We assume that Alice and Bob hold system represented by Hilbert spaces $\mathcal{H}_{AA'} := \mathcal{H}_A \otimes \mathcal{H}_{A'}$ and $\mathcal{H}_{BB'} := \mathcal{H}_B \otimes \mathcal{H}_{B'}$, respectively.

6.1 Entanglement resource for one-way LOCC

In this section, we focus on characterizing the amount of entanglement resource to discriminate a state from a set of orthonormal basis states by one-way LOCC in terms of the Schmidt rank. Note that we do not assume the orthonormal basis as a product basis; thus, all the results in this section are valid for the cases of all possibly entangled orthonormal basis. Although we assume that one-way LOCC means one-way LOCC starting from Alice ($\mathcal{H}_{AA'}$) to Bob ($\mathcal{H}_{BB'}$) in this subsection, all the results can be easily extend to one-way LOCC from Bob to Alice.

For an orthonormal basis $\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$, we define $r_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right)$ as the minimum of the Schmidt rank of a state $|\Phi\rangle_{A'B'} \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ such that a set $\{|\psi_j\rangle_{AB} \otimes |\Phi\rangle_{A'B'}\}_{j=1}^{d_A d_B} \subset \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ can be perfectly discriminated by one-way LOCC, namely,

$$r_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right) := \min_{|\Phi\rangle} \left\{ \text{Sch}\#_{B'}^{A'}(|\Phi\rangle) \mid \exists \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}, \text{ s.t. } |\Phi\rangle \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}, \right. \\ \left. \text{and } \{|\psi_j\rangle_{AB} \otimes |\Phi\rangle_{A'B'}\}_{j=1}^{d_A d_B} \text{ is one-way LOCC distinguishable} \right\}, \quad (6.2)$$

where $\text{Sch}\#_{B'}^{A'}(|\Phi\rangle)$ is the Schmidt rank of $|\Phi\rangle$. Thus, $r_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right)$ is the optimal entanglement resource to discriminate $\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B}$ by one-way LOCC in terms of the Schmidt rank.

Our main result in this section is stated as the following theorem which completely characterizes $r_{\min} \left(\{ |\psi_j\rangle_{AB} \}_{j=1}^{d_A d_B} \right)$ and a proof is shown in Appendix B.1.

Theorem 5. *For any orthonormal basis $\{ |\psi_j\rangle_{AB} \}_{j=1}^{d_A d_B} \subset \mathcal{H}_A \otimes \mathcal{H}_B$,*

$$r_{\min} \left(\{ |\psi_j\rangle_{AB} \}_{j=1}^{d_A d_B} \right) = d_{\min} \left(\{ |\psi_j\rangle_{AB} \}_{j=1}^{d_A d_B} \right),$$

where $d_{\min} \left(\{ |\psi_j\rangle_{AB} \}_{j=1}^{d_A d_B} \right)$ is defined by

$$d_{\min} \left(\{ |\psi_j\rangle_{AB} \}_{j=1}^{d_A d_B} \right) := \min_{\mathcal{H}_A = \bigoplus_k \mathcal{M}_k} \max_k \left\{ \dim \mathcal{M}_k \mid \forall j, \exists k, \text{ s.t. } |\psi_j\rangle_{AB} \in \mathcal{M}_k \otimes \mathcal{H}_B \right\}.$$

6.2 Entanglement resource for two-way LOCC

In this section, we focus on the case of orthogonal product bases and study the amount of entanglement necessary to discriminate one of the basis states by LOCC. In particular as an example, we consider the basis given by the nine states defined by Eq. (6.1) and their generalization. We study the entanglement resource necessary to discriminate a state from the nine states by LOCC.

For the nine states $\{ |\psi_j\rangle_{AB} \}_{j=1}^9$ defined by Eq. (6.1), we can easily see that there is no non-trivial subspace $\mathcal{M} \subset \mathcal{H}_A$ satisfying for all j , either $|\psi_j\rangle \in \mathcal{M} \otimes \mathcal{H}_B$ or $|\psi_j\rangle \in \mathcal{M}^\perp \otimes \mathcal{H}_B$, where \mathcal{M}^\perp is the orthogonal complement of \mathcal{M} . Thus, from Theorem 5, the optimal entanglement resource $|\Phi\rangle$ necessary to discriminate the nine states by one-way LOCC satisfies $\text{Sch}\#_{B'}^{A'}(|\Phi\rangle) = 3$. On the other hand, we construct a two-way LOCC protocol by which the nine states can be discriminated by consuming an entanglement resource with $\text{Sch}\#_{B'}^{A'}(|\Phi\rangle) = 2$. The protocol can be described as follows: First, we extend the dimension of \mathcal{H}_B from 3 to d by adding additional states $|i\rangle_B$ for $3 \leq i \leq d$. Then, apply a global unitary V_d given by

$$V_d := |0\rangle\langle 0|_A \otimes (|3\rangle\langle 1| + |1\rangle\langle 3| + |0\rangle\langle 0| + |2\rangle\langle 2| + |4\rangle\langle 4| + \cdots + |d\rangle\langle d|)_B + (|1\rangle\langle 1| + |2\rangle\langle 2|)_A \otimes I_B. \quad (6.3)$$

As a result, the nine states $\{ |\psi_j\rangle_{AB} \}_{j=1}^9$ are transformed into

$$\begin{aligned} \{ |\psi'_{1(2)}\rangle_{AB} = |0\rangle_A |0 \pm 3\rangle_B, \quad |\psi'_{3(4)}\rangle_{AB} = |0 \pm 1\rangle_A |2\rangle_B, \\ |\psi'_{5(6)}\rangle_{AB} = |2\rangle_A |1 \pm 2\rangle_B, \quad |\psi'_{7(8)}\rangle_{AB} = |1 \pm 2\rangle_A |0\rangle_B, \quad |\psi'_9\rangle_{AB} = |1\rangle_A |1\rangle_B \}. \end{aligned} \quad (6.4)$$

These states are distinguishable by LOCC. We use a graphical representation of the states in Fig. 6.1 in order to show a LOCC protocol given in Fig. 6.2. Note that we show how the protocol works when $|\psi'_9\rangle = |1\rangle_A |1\rangle_B$ is given. When another state is given, the flow of the protocol will be changed since Alice and Bob can change measurements depending on their past measurement outcomes.

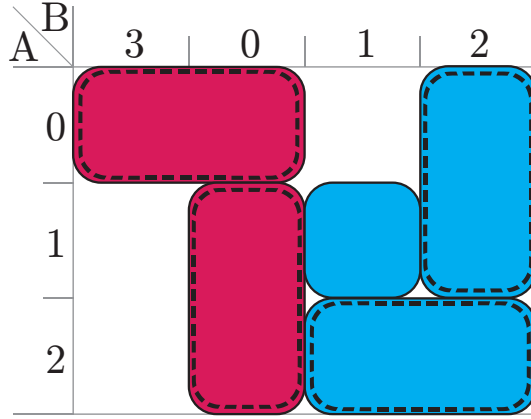
A \ B	3	0	1	2
0	$ 0\rangle_A 0 \pm 3\rangle_B$			$ 0 \pm 1\rangle_A 2\rangle_B$
1		$ 1 \pm 2\rangle_A 0\rangle_B$	$ 1\rangle_A 1\rangle_B$	
2			$ 2\rangle_A 1 \pm 2\rangle_B$	

Figure 6.1: **A graphical representation of states.** After applying V_d , the nine states are transformed into the states represented in this figure.

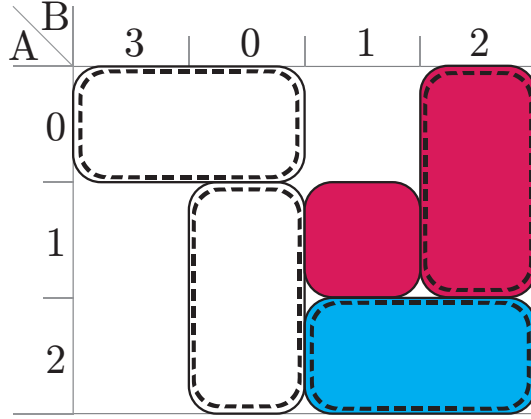
V_d can be implemented with an EPR state since the operator Schmidt rank of V_d is 2 [98].

The above discussion can be generalized to a general orthogonal product basis

$$\text{i) } \{K_{b_1=0}^{(B)} = |0\rangle\langle 0|_B + |3\rangle\langle 3|_B, K_{b_1=1}^{(B)} = |1\rangle\langle 1|_B + |2\rangle\langle 2|_B\}_{b_1=0,1}$$



$$\text{ii) } \{K_{a_1=0}^{(A)} = |0\rangle\langle 0|_A + |1\rangle\langle 1|_A, K_{a_1=1}^{(A)} = |2\rangle\langle 2|_A\}_{a_1=0,1}$$



$$\text{iii) } \{K_{b_2=0}^{(B)} = |1\rangle\langle 1|_B, K_{b_2=1}^{(B)} = |2\rangle\langle 2|_B, K_{b_2=2}^{(B)} = |0\rangle\langle 0|_B + |3\rangle\langle 3|_B\}_{b_2=0,1,2}$$

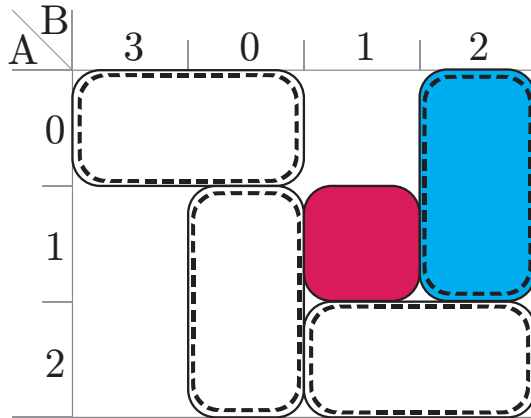


Figure 6.2: **A LOCC protocol for discrimination.** We see how the protocol works when $|\psi'_9\rangle = |1\rangle_A |1\rangle_B$ is given. i) First, Bob performs a measurement of which Kraus operators are given by $\{K_{b_1=0}^{(B)} = |0\rangle\langle 0|_B + |3\rangle\langle 3|_B, K_{b_1=1}^{(B)} = |1\rangle\langle 1|_B + |2\rangle\langle 2|_B\}_{b_1=0,1}$ and obtains a measurement outcome $b_1 = 1$. ii) Second, Alice performs a measurement of which Kraus operators are given by $\{K_{a_1=0}^{(A)} = |0\rangle\langle 0|_A + |1\rangle\langle 1|_A, K_{a_1=1}^{(A)} = |2\rangle\langle 2|_A\}_{a_1=0,1}$ and obtains a measurement outcome $a_1 = 0$. iii) Third, Bob performs a measurement of which Kraus operators are given by $\{K_{b_2=0}^{(B)} = |1\rangle\langle 1|_B, K_{b_2=1}^{(B)} = |2\rangle\langle 2|_B, K_{b_2=2}^{(B)} = |0\rangle\langle 0|_B + |3\rangle\langle 3|_B\}_{b_2=0,1,2}$, obtains a measurement outcome $b_2 = 0$ and they know $|\psi'_9\rangle$ is given.

$\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B}$ defined by

$$\begin{aligned}
|\psi_{1(2)}\rangle &= \frac{1}{\sqrt{2}}|1\rangle \otimes (|1\rangle \pm |2\rangle), \\
|\psi_{3(4)}\rangle &= \frac{1}{\sqrt{2}}(|d_A - 1\rangle \pm |d_A\rangle) \otimes |1\rangle, \\
|\psi_{m_1+5}\rangle &= \sum_{k=2}^{d_A-2} e^{i\frac{2\pi}{d_A-3}m_1\cdot(k-2)}|k\rangle \otimes |1\rangle, \\
|\psi_{d_A+m_2+2}\rangle &= \sum_{k=2}^{d_A-1} e^{i\frac{2\pi}{d_A-2}m_2\cdot(k-2)}|k\rangle \otimes |2\rangle, \\
|\psi_{2d_A+m_3}\rangle &= |d_A\rangle \otimes \sum_{k=2}^{d_B} e^{i\frac{2\pi}{d_B-1}m_3\cdot(k-2)}|k\rangle, \\
|\psi_{2d_A+d_B-1+(d_A-1)m_5+m_4}\rangle &= \sum_{k=1}^{d_A-1} e^{i\frac{2\pi}{d_A-1}m_4\cdot(k-1)}|k\rangle \otimes |m_5 + 3\rangle \quad (6.5)
\end{aligned}$$

where m_i for $i = 1, 2, 3, 4, 5$ satisfies $0 \leq m_1 \leq d_A - 4$, $0 \leq m_2 \leq d_A - 3$, $0 \leq m_3 \leq d_B - 2$, $0 \leq m_4 \leq d_A - 2$, and $0 \leq m_5 \leq d_B - 3$. A graphical representation of the orthogonal product basis is given in Fig. 6.3. We consider local state discrimination of $\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B}$. Theorem 5 guarantees that in order to discriminate a state from this basis states by one-way LOCC starting from Alice to Bob an entanglement resource with the Schmidt rank d_A is necessary. Similarly, to discriminate a state from the same basis states by one-way LOCC starting from Bob to Alice an entanglement resources with the Schmidt rank d_B is necessary. On the other hand, by means of the similar discussion as the nine states, it is enough to use an entanglement resource with the Schmidt rank 2 in case of two-way LOCC. Therefore, in the limit of large d_A , there is infinite gap between one-way LOCC and two-way LOCC in terms of entanglement resource in terms of the Schmidt rank to distinguish the orthogonal product basis defined by Eq. (6.5).

Chapter 7

Resources for SEP

In this chapter, we show that a causal relation between the classical outputs and classical inputs of the local operations without predefined partial order, which we call “classical communication” without predefined causal order (CC^*), characterizing a special class of deterministic quantum operations, separable operations. In Section 7.1, we extend LOCC into a joint quantum operation between two parties implemented without using shared entanglement but with local operations connected by CC^* . We name a new class of deterministic joint quantum operations obtained by this extension but still within quantum mechanics by $LOCC^*$. We show that $LOCC^*$ with CC^* respecting partial order reduces LOCC. In Section 7.2, we show that $LOCC^*$ can be represented by the ∞ -shaped loop in Fig. 7.1 and is equivalent to SEP [63], which has been introduced for mathematical simplicity to analyze nonlocal quantum tasks in place of LOCC. In Section 7.3, by considering the correspondence between $LOCC^*$ and a probabilistic version of LOCC called stochastic LOCC (SLOCC), we analyze the power of CC^* in terms of enhancing the success probability of probabilistic operations in SLOCC. In Section 7.4, we also investigate the relationship between $LOCC^*$ and the quantum process formalism for joint quantum operations without partial order developed in [58]. In Section 7.5, by using our framework, we give an example of the quantum operation which is an element of SEP but not an element of LOCC, i.e., to perform such an operation within special relativistic spacetime, entanglement and classical communication are necessary.

7.1 $LOCC^*$

We consider a deterministic joint quantum operation (a CPTP map) taking only quantum input and output denoted by \mathcal{M} implemented by two parties, Alice and Bob, who are connected only by classical communication. We set Alice performs

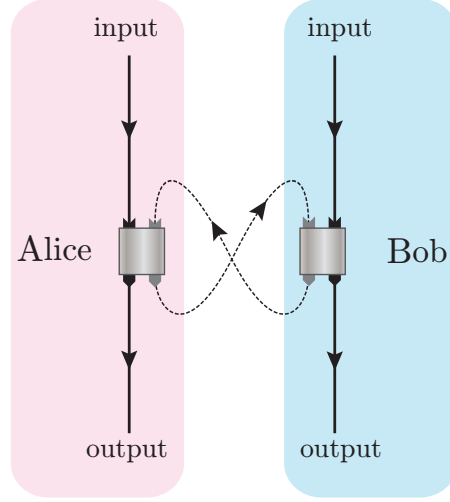


Figure 7.1: **A deterministic joint quantum operation consisting of local operations connected by the ∞ -shaped loop.** Any element of LOCC* can be represented by this joint quantum operation and vice versa as shown in Results.

the first operation. As a simplest case, we consider to link a classical output o of Alice's local operation represented by $\{\mathcal{A}_o\}_o$ and a classical input i of Bob's local operation represented by \mathcal{B}_i . Since Alice and Bob are acting on different quantum systems at different spacetime coordinates, the joint quantum operation is described by a tensor product of two local operations. Ability of classical communication indicates that the spacetime coordinate of Alice's local operation and that of Bob's local operation are timelike separated, and Bob's coordinate is in the future cone of Alice's coordinate. Linking the classical output of Alice o and the classical input of Bob i means that they are perfectly correlated, namely $i = o$ for all o . By taking averages over o and i , we obtain a deterministic joint quantum operation given by

$$\mathcal{M} = \sum_{o,i} \delta_{i,o} \mathcal{A}_o \otimes \mathcal{B}_i = \sum_o \mathcal{A}_o \otimes \mathcal{B}_o, \quad (7.1)$$

where $\delta_{o,i}$ denotes the Kronecker delta. This is the simplest case of LOCC called one-way LOCC.

A deterministic joint operation represented by more general finite-round LOCC between two parties is defined by connecting a sequence of Alice's local operations given by $\{\mathcal{A}_{o_N|i_N}^{(N)} \circ \cdots \circ \mathcal{A}_{o_1}^{(1)}\}_{o_N, \dots, o_1}$ and another sequence of Bob's local operations given by $\{\mathcal{B}_{o'_N|i'_N}^{(N)} \circ \cdots \circ \mathcal{B}_{o'_1|i'_1}^{(1)}\}_{o'_N, \dots, o'_1}$. Here \circ denotes a connection between two local operations at timelike separated coordinates linking a quantum output of a

local operation and a quantum input of the next local operation of the *same* party and introduces a total order for each party's local operations. The indices i_k and i'_k are classical inputs of the k -th operations and o_k and o'_k are classical outputs of the k -th operations of Alice and Bob, respectively. In LOCC, not only local operations within the parties are totally ordered, but also the spacetime coordinates of all local operations of Alice and Bob are totally ordered alternately. Then o_1 of Alice's local operation and i'_1 of Bob's local operation are linked by classical communication and setting $i'_1 = o_1$, and similarly, o'_1 of Bob's local operation and i_2 of Alice's local operation are linked by setting $i_2 = o'_1$ and so on. Thus, finite-round LOCC between the two parties is defined by a set of the joint quantum operation represented by

$$\mathcal{M} = \sum_{i_1, \dots, i'_N, o_1, \dots, o'_N} \delta_{o_N, i'_N} \cdots \delta_{o_1, i'_1} \mathcal{A}_{o_N | i_N}^{(N)} \circ \cdots \circ \mathcal{A}_{o_1 | i_1}^{(1)} \otimes \mathcal{B}_{o'_N | i'_N}^{(N)} \circ \cdots \circ \mathcal{B}_{o'_1 | i'_1}^{(1)} \quad (7.2)$$

$$= \sum_{i_1, \dots, i_N, o_1, \dots, o_N, o'_N} \mathcal{A}_{o_N | i_N}^{(N)} \circ \cdots \circ \mathcal{A}_{o_1 | i_1}^{(1)} \otimes \mathcal{B}_{o'_N | o_N}^{(N)} \circ \cdots \circ \mathcal{B}_{i_2 | o_1}^{(1)} \quad (7.3)$$

where we define $\mathcal{A}_{o_1}^{(1)} := \sum_{i_1} \mathcal{A}_{o_1 | i_1}^{(1)}$. An example for $N = 3$ is shown in Fig.2.2.

Now we develop a framework to investigate local operations and classical communication between the parties without the assumption of the existence of predefined ordering of the spacetime coordinates. That is, we keep the local spacetime coordinates and the totally ordered structure of local operations within each party but do not assign the *global* spacetime coordinate across the parties, and allow connecting any classical inputs and outputs of local operations between different parties as long as the resulting deterministic joint quantum operation is in quantum mechanics. This relaxation allows a generalization of classical communication to a conditional probability distribution $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ linking the classical outputs and the classical inputs of local operations. The corresponding joint quantum operation is represented by

$$\mathcal{M} = \sum_{i_1, \dots, i'_N, o_1, \dots, o'_N} p(i_1, \dots, i'_N | o_1, \dots, o'_N) \mathcal{A}_{o_N | i_N}^{(N)} \circ \cdots \circ \mathcal{A}_{o_1 | i_1}^{(1)} \otimes \mathcal{B}_{o'_N | i'_N}^{(N)} \circ \cdots \circ \mathcal{B}_{o'_1 | i'_1}^{(1)}. \quad (7.4)$$

This generalization does not guarantee the joint quantum operation represented by Eq.(7.4) to be TP whereas its CP property is preserved. Since we investigate deterministic joint quantum operations, we require $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ to keep the form of Eq.(7.4) to represent a CPTP maps. We call a set of CPTP maps in the form of Eq.(7.4) with $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ as LOCC*.

For one-way LOCC, such a generalization corresponds to replacing the delta function $\delta_{o,i}$ in Eq.(7.1) by a conditional probability distribution $p(i|o)$. This is equivalent to replacing a perfect classical channel by a general noisy classical channel. However, it is not the case for multiple-round LOCC. A deterministic joint quantum operation is LOCC if and only if it can be decomposed in the form of Eq.(7.4) with $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ respecting *causal order* of the classical inputs and outputs of local operations imposed by special relativistic no-signaling conditions. $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ respecting causal order can be regarded as classical communication respecting causal order. The definition of the causal order of $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ and relationship between LOCC and causal order are given in Appendix B.2.

It is easy to check that without loss of generality, any CPTP map in LOCC* can be implemented by just one local operation performed by each party connected by a conditional probability distribution, since by letting $o_A := (o_1, \dots, o_N)$, $i_A := (i_1, \dots, i_N)$, $o_B := (o'_1, \dots, o'_N)$ and $i_B := (i'_1, \dots, i'_N)$, we can regard the sequence of Alice's local operations $\{\mathcal{A}_{o_N|i_N}^{(N)} \circ \dots \circ \mathcal{A}_{o_1|i_1}^{(1)}\}_{o_N, \dots, o_1}$ as one quantum instrument $\{\mathcal{A}_{o_A|i_A}\}_{o_A}$ conditioned by the classical input i_A , the same with Bob's local operations and $p(i_A, i_B | o_A, o_B)$ is still a conditional probability distribution. Thus LOCC* is simply defined by a set of deterministic joint quantum operations (= CPTP maps) \mathcal{M} given in the form of

$$\mathcal{M} = \sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) \mathcal{A}_{o_A|i_A} \otimes \mathcal{B}_{o_B|i_B}, \quad (7.5)$$

where $p(i_A, i_B | o_A, o_B)$ is a conditional probability distribution satisfying

$$p(i_A, i_B | o_A, o_B) \geq 0 \quad \text{and} \quad \sum_{i_A, i_B} p(i_A, i_B | o_A, o_B) = 1, \quad (7.6)$$

where $\{\mathcal{A}_{o_A|i_A}\}_{o_A}$ is Alice's local operation with a classical input i_A and a classical output o_A , and $\{\mathcal{B}_{o_B|i_B}\}_{o_B}$ is Bob's local operation with a classical input i_B and a classical output o_B . We call $p(i_A, i_B | o_A, o_B)$ in Eq. (7.5) linking the classical outputs and classical inputs as CC*, "*classical communication*" *without predefined causal order*, with respect to local operations $\{\{\mathcal{A}_{o_A|i_A}\}_{o_A}, \{\mathcal{B}_{o_B|i_B}\}_{o_B}\}$. Note that we can also "collapse" the sequential local operations in multi-round LOCC to represent a joint quantum operation in the form of Eq. (7.5). However in this case if we regard the combined operations $\{\mathcal{A}_{o_A|i_A}\}_{o_A}$ and $\{\mathcal{B}_{o_B|i_B}\}_{o_B}$ as operations localized in the spacetime of LOCC, the corresponding $p(i_A, i_B | o_A, o_B)$ cannot be interpreted as classical communication respecting causal order.

Further, we show that LOCC* can be always represented by a ∞ -shaped loop shown in Fig.7.1. It is easy to see that if $p(i_A, i_B | o_A, o_B) = \delta_{i_A, o_B} \delta_{i_B, o_A}$, LOCC*

		b		
		1	2	3
i) $K_{a b}^{(A)}$:	a			
	1	$ 1\rangle_{A'}\langle 0 _A$	$ 2\rangle_{A'}\langle 0 _A$	$ 3\rangle_{A'}\langle 0+1 _A$
	2	$ 8\rangle_{A'}\langle 1-2 _A$	$ 9\rangle_{A'}\langle 1 _A$	$ 4\rangle_{A'}\langle 0-1 _A$
	3	$ 7\rangle_{A'}\langle 1+2 _A$	$ 6\rangle_{A'}\langle 2 _A$	$ 5\rangle_{A'}\langle 2 _A$

		b		
		1	2	3
ii) $K_{b a}^{(B)}$:	a			
	1	$ 1\rangle_{B'}\langle 0+1 _B$	$ 2\rangle_{B'}\langle 0-1 _B$	$ 3\rangle_{B'}\langle 2 _B$
	2	$ 8\rangle_{B'}\langle 0 _B$	$ 9\rangle_{B'}\langle 1 _B$	$ 4\rangle_{B'}\langle 2 _B$
	3	$ 7\rangle_{B'}\langle 0 _B$	$ 6\rangle_{B'}\langle 1-2 _B$	$ 5\rangle_{B'}\langle 1+2 _B$

Table 7.1: Tables of the Kraus operators $K_{a|b}^{(A)}$ of Alice's local operations $\{\mathcal{A}_{a|b}\}_a$ in i) and $K_{b|a}^{(B)}$ of Bob's local operation $\{\mathcal{B}_{b|a}\}_b$ in ii). In the Kraus operator representation, the deterministic joint quantum operation $\mathcal{M} = \sum_{a,b} \mathcal{A}_{a|b} \otimes \mathcal{B}_{b|a}$ transforms any quantum input ρ_{AB} on systems A and B into a quantum output on systems A' and B' as $\rho'_{A'B'} = \mathcal{M}(\rho_{AB}) = \sum_{a,b} K_{a|b}^{(A)} \otimes K_{b|a}^{(B)} \rho_{AB} (K_{a|b}^{(A)} \otimes K_{b|a}^{(B)})^\dagger$ where $\sum_a (K_{a|b}^{(A)})^\dagger K_{a|b}^{(A)} = \mathbb{I}_A$ for any b and $\sum_b (K_{b|a}^{(B)})^\dagger K_{b|a}^{(B)} = \mathbb{I}_B$ for a with identity operators \mathbb{I}_A and \mathbb{I}_B on system A and B , respectively.

defined by Eq.(7.5) reduces to

$$\mathcal{M} = \sum_{a,b} \mathcal{A}_{a|b} \otimes \mathcal{B}_{b|a}. \quad (7.7)$$

In Appendix B.4, we show the converse, all elements of LOCC* can be decomposed into this form, is also true. From this form of LOCC*, it is possible to interpret that CC* in LOCC* can be *looped*, namely, Alice's classical input is Bob's classical output and Bob's classical input is Alice's classical output.

7.2 LOCC* and SEP

We show that LOCC* provides a new characterization of a set of deterministic joint quantum operations corresponding to SEP by proving that LOCC* is equivalent to SEP. We start with investigating inclusion relations between LOCC and LOCC*. It is easy to verify that LOCC is a subset of LOCC* by definition of LOCC*. We show that LOCC* is strictly larger than LOCC by constructing the following example based on the nine-state discrimination [43].

We show that the the nine-state *can* be deterministically and perfectly distinguishable by a map in LOCC* followed by local measurements by presenting constructions of Alice's local operation $\{\mathcal{A}_{a|b}\}_a$ and Bob's local operation $\{\mathcal{B}_{b|a}\}_b$ in the form of Eq.(7.7). The constructions of $\{\mathcal{A}_{a|b}\}_a$ and $\{\mathcal{B}_{b|a}\}_b$ in the Kraus operator representations are given in Table 7.1 i) and ii), respectively. It is easy to check that for any $|\psi_k\rangle \in \{|\psi_i\rangle\}_{i=1}^9$, the corresponding \mathcal{M} in LOCC* with the constructions of the local operations transforms

$$|\psi_k\rangle\langle\psi_k| \rightarrow \sum_{a,b} \mathcal{A}_{a|b} \otimes \mathcal{B}_{b|a} (|\psi_k\rangle\langle\psi_k|) = |k\rangle_{A'}\langle k| \otimes |k\rangle_{B'}\langle k| \quad (7.8)$$

where indices A' and B' denote nine-dimensional output systems for Alice and Bob. Once Alice and Bob obtain the output state $|k\rangle_{A'}\langle k| \otimes |k\rangle_{B'}\langle k|$, they can find out the classical output k by individually performing projective measurements in the basis given by $\{|j\rangle\}_{j=1}^9$. Note that the nine states can be probabilistically distinguished without error by a stochastic LOCC (SLOCC) protocol, which indicates LOCC* is closely related to SLOCC as it will be shown later.

We can further show that LOCC* is equivalent to a well known class of CPTP maps called *separable map* (SEP) as summarized in Fig. 7.2. SEP is a set of maps representing deterministic joint quantum operations \mathcal{M} that can be written by

$$\mathcal{M} = \sum_k \mathcal{E}_k^A \otimes \mathcal{E}_k^B, \quad (7.9)$$

where all the elements of local operations without classical inputs \mathcal{E}_k^A and \mathcal{E}_k^B are completely positive. The set of nine states can be deterministically and perfectly distinguished by using a map in SEP of which Kraus operator representation is given by $\{|k\rangle_{A'} \otimes |k\rangle_{B'} \langle\psi_k|_{AB}\}$ followed by local projective measurements in the basis given by $\{|k\rangle\}_{k=1}^9$. SEP is equivalent to a set of CPTP maps that cannot transform any separable states into entangled states [52, 53]. Therefore, SEP does not have a power to create entanglement between two parties if the quantum input is not entangled. This can be interpreted as a characterization of operational effects of SEP since the characterization is based on the effect of SEP. The class SEP includes the class LOCC [55]. Due to the mathematical simplicity of its structure, the class SEP is often used for proving a quantum task to be not implementable by LOCC protocols by showing that the task is not implementable even by using a stronger class of operations, SEP. However, the gap between LOCC and SEP has not been clear.

It is easy to see that LOCC* is a subset of SEP from the form of Eq.(7.5), since $\mathcal{A}_{o_A|i_A}$ and $\mathcal{B}_{o_B|i_B}$ are also completely positive and $p(i_A, i_B|o_A, o_B)$ is not negative, so we can always transform a map in LOCC* into the form of (7.9). To prove that SEP is a subset of LOCC*, we use the fact that an element of SEP is implementable

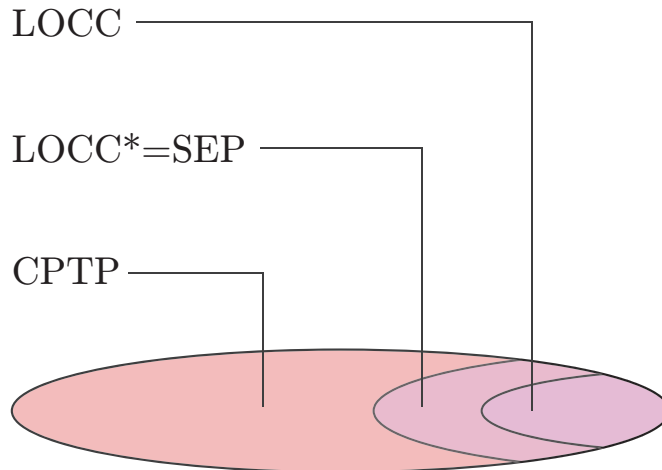


Figure 7.2: The inclusion relation between the classes of deterministic joint quantum operations CPTP, SEP, LOCC*, and LOCC. LOCC* is equivalent to the set of separable maps (SEP). LOCC is strictly smaller than SEP. LOCC* is strictly smaller than the set of CPTP.

by SLOCC with a *constant* success probability [55]. In Appendix B.5, we show that it is possible to reduce the failure probability to be zero in a LOCC* protocol and there always exists a map in LOCC* corresponding to a map in SEP. Note that the LOCC* map obtained by Appendix B.5 is different from the simpler LOCC* map given in Table 7.1 in the case of nine-state discrimination. LOCC* gives a new characterization of SEP in terms of operational resources in the sense that SEP can be interpreted as a set of operations consisting local operations and CC*. Note that in LOCC*, two assumptions of local operations, (a) they are partially ordered and (b) the choice of a local operation does not depend on resources connecting the local operation, are relaxed and the local operations are connected by CC*.

So far, we have considered the implementation of a deterministic joint quantum operation when no entanglement is shared across the parties. Now we consider the effect of entanglement shared between the parties. Since any deterministic joint quantum operations can be implementable by entanglement assisted LOCC, LOCC* can be implementable by entanglement assisted (standard) classical communication respecting causal order. The results shown in this part suggest that entanglement assisted LOCC implementing SEP can be simulated by LOCC*, where no entanglement is needed.

7.3 LOCC* and local post selection

In this part, we present the relationship between LOCC* and SLOCC. SLOCC is a set of (linear) CP maps consisting of local operations and standard classical communication. In contrast to LOCC, SLOCC contains the CP maps representing the cases where particular measurement outcomes are post-selected. Since we use a linear map to represent SLOCC, a SLOCC element is not TP but trace decreasing (TD) in general. We define a class of linear CP maps called SLOCC* that can be simulated by SLOCC. That is, SLOCC* is the set of linear CP maps from two input systems X and Y to two output system A and B such that

$$\mathcal{M} = c\Gamma, \quad (7.10)$$

where Γ is an element of SLOCC and a positive constant $c > 0$. Note that SLOCC* contains not only TD maps but also trace increasing maps. It is easy to see that LOCC* (or SEP) is a subset of SLOCC* since any element of LOCC* (or SEP) is implementable by SLOCC with a constant success probability independent of inputs. In the following, we show that a superset of LOCC* where the TP condition is removed from LOCC* is equivalent to SLOCC*. That is, SLOCC* is equivalent to the set of linear CP maps that can be decomposed into the form of Eq. (7.5). By definition, SLOCC* is equivalent to the set of linear CP maps that can be decomposed into the form of Eq. (7.9), where k corresponds to a measurement outcome. Without loss of generality, we can restrict \mathcal{E}_k^A and \mathcal{E}_k^B in Eq. (7.9) to be CPTD maps since for all linear CP maps \mathcal{E}_k^A , there exists natural number M such that $\frac{1}{M}\mathcal{E}_k^A$ is a CPTD map and \mathcal{M} given by Eq. (7.9) can be represented by $\sum_{i=1}^M \sum_k \tilde{\mathcal{E}}_{i,k}^A \otimes \tilde{\mathcal{E}}_{i,k}^B$, where $\tilde{\mathcal{E}}_{i,k}^A = \frac{1}{M}\mathcal{E}_k^A$ and $\tilde{\mathcal{E}}_{i,k}^B = \mathcal{E}_k^B$. By applying the same technique described in Appendix B.5, any element of SLOCC* can be decomposed into the form of Eq. (7.7). Thus, any SLOCC* element can be decomposed into Eq. (7.5). We summarize the inclusion relation of sets of linear CP maps as shown in Fig. 7.3.

Any linear CP maps that can be decomposed into the form of Eq. (7.5) is simulatable by LOCC with post-selection (SLOCC), and vice versa. A connection between post-selection and the causal structure of the spacetime has been discussed in the context of the probabilistic closed time-like curve (p-CTC) in [100, 101, 102]. Our result indicates the connection between post-selection and CC* without causal order. In the standard spacetime, a map in SEP but not in LOCC is implementable by LOCC assisted by entanglement. Thus we can regard that entanglement accompanied with classical communication is used only for enhancing the success probability of a task achievable without entanglement $p < 1$ to $p = 1$ for implementing a map in SEP (=LOCC*, but not in LOCC). In this sense, CC* without causal order can be understood as alternative characterizations of a

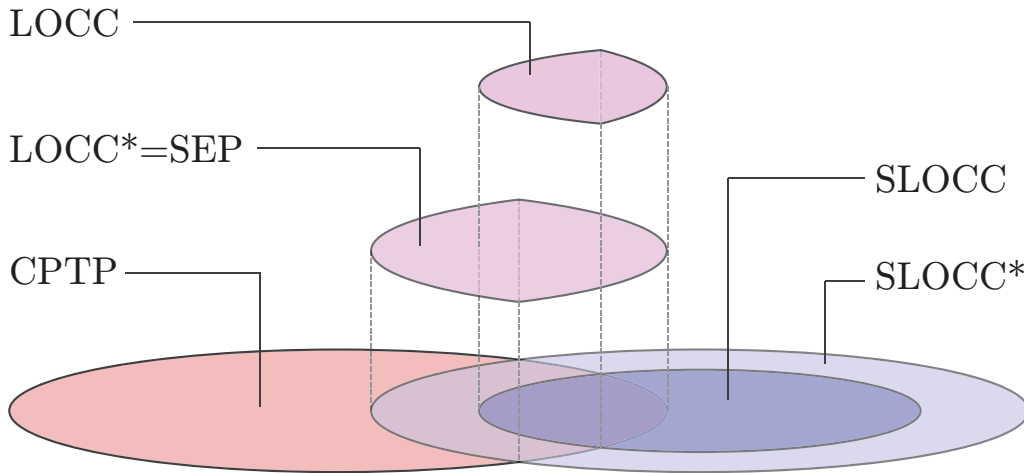


Figure 7.3: Class of linear CP maps. The intersection of SLOCC and the set of CPTP maps (TP SLOCC elements) is LOCC since any TP SLOCC element can be implemented by a LOCC protocol. The intersection of SLOCC* and the set of CPTP maps (TP SLOCC* elements) is LOCC*.

power of entanglement for enhancing success probability by effectively changing the partial ordering properties of the spacetime.

7.4 LOCC* and quantum processes

We discuss correspondences between our formalism of LOCC* and other formalisms of quantum operations without the assumptions of the partial order of local operations, *higher order formalisms* developed by [58, 60]. In the higher order formalism, effects of quantum communication linking local operations of two parties are described as a map that transforms local operations into a deterministic joint quantum operation. The map, called a *quantum process*, is a higher order map (supermap) transforming a quantum operation to another quantum operation, whereas a (normal) map transforms a quantum state to another quantum state. In [58], the requirements for a quantum process to be consistent with quantum mechanics but without predefined causal order of local operations have been derived. They have shown that there exists quantum processes not implementable by *quantum* communication linking partially ordered local operations. Such requirements for a quantum process to be consistent with quantum mechanics can be interpreted as a new kind of causality, which is different from the special relativistic causality but based only on quantum mechanics. The quantum process shows a new possibility to speed up quantum computers [103] and implementations

of the quantum process are discussed for several settings [105, 104].

A crucial difference between the higher order formalisms and our formalism of LOCC* is that the local operations are linked by quantum communication in the higher order formalisms, but we only allow classical communication between the parties. To compare the two formalisms, we consider a special type of quantum processes where quantum communication between the parties are restricted to transmitting a probabilistic mixture of “classical” states, namely, a set of fixed mutually orthogonal states. Such a process is called a *classical* quantum process (CQP). In [58], it is shown that a deterministic joint operation described by local operations linked by a classical quantum process does not exhibit the new causality as a (fully) quantum process does. In Appendix B.6, we show that the deterministic joint operations in this case reduce to a probabilistic mixture of two types of operations in one-way LOCC from Alice to Bob and from Bob to Alice. We denote a set of such deterministic joint quantum operations as LOCQP for comparing to LOCC*.

Since LOCQP is a set of probabilistic mixtures of one-way LOCC, LOCC* is a larger set than LOCQP. Therefore, CC* used in implementing non-LOCC quantum operations cannot be a classical quantum process linking two local operations. The gap between LOCC* and LOCQP originates from the conditions on local operations imposed for restricting CC* and a classical quantum process. CC* in LOCC* is only required to guarantee the joint quantum operation to be deterministic for *some* choices of local operations, whereas a classical quantum process in LOCQP is required to guarantee the joint quantum operation to be deterministic for *arbitrary* choices of local operations. Hence CC* is less restricted than a classical quantum process. Considering that CC* is simulated by entanglement assisted classical communication, we can conclude that entanglement provides a power to waver restrictions on classical communication linking local operations originated from both the causality in special relativity and the restriction for classical quantum processes when it is accompanied by classical communication.

7.5 LOCQP and SEP

In bipartite cases, we have shown that LOCQP is equivalent to a set of probabilistic mixtures of one-way LOCC since the classical quantum process is just a probabilistic mixtures of classical communication. A quantum process is called *causally separable* if the quantum process represents a probability mixtures of normal communication channels, otherwise, it is called *causally non-separable*. There exists a classical quantum process W that is causally non-separable in *tripartite* cases as shown in Appendix B.8. This implies that tripartite LOCQP not only contains a simple probability mixture of one-way LOCC but also possibly contains

an element of a larger set such as two-way LOCC and even non-LOCC separable operations. In this section, we give an example of the tripartite non-LOCC separable operations consisting of local operations linked by tripartite LOCQP. Very few classes of non-LOCC separable operations are known [43, 44, 45, 64] and the gap between SEP and LOCC has not been clarified so far. LOCQP can be used for a new tool to generate operations in non-LOCC SEP.

In Appendix B.8, we show that CC^* defined by

$$\begin{aligned}
p(x, y, z|a, b, c) = \frac{1}{2} \text{ if } (x, y, z, a, b, c) = & (0, 0, 0, 0, 0, 0) \\
& = (0, 0, 0, 1, 1, 1) \\
& = (0, 0, 1, 0, 1, 0) \\
& = (0, 0, 1, 1, 0, 1) \\
& = (0, 1, 0, 0, 1, 1) \\
& = (0, 1, 0, 1, 0, 0) \\
& = (0, 1, 1, 0, 0, 1) \\
& = (0, 1, 1, 1, 1, 0) \\
& = (1, 0, 0, 0, 0, 1) \\
& = (1, 0, 0, 1, 1, 0) \\
& = (1, 0, 1, 0, 1, 1) \\
& = (1, 0, 1, 1, 0, 0) \\
& = (1, 1, 0, 0, 1, 0) \\
& = (1, 1, 0, 1, 0, 1) \\
& = (1, 1, 1, 0, 0, 0) \\
& = (1, 1, 1, 1, 1, 1). \tag{7.11}
\end{aligned}$$

corresponds to a causally non-separable classical quantum process. A joint map Γ obtained by using this CC^* is given by

$$\Gamma = \sum_{x,y,z,a,b,c} p(x, y, z|a, b, c) A_{a|x} \otimes B_{b|y} \otimes C_{c|z}, \tag{7.12}$$

where we use the CJ representations of local operations for Alice, Bob and Charlie, for example, and $\{A_{a|x}\}_a$ is the CJ representation of a local quantum operation of Alice in $\mathbf{C}(\mathcal{H}_1 : \mathcal{H}_2)$. We can prove that Γ is a separable map that is not in a finite round LOCC with

$$A_{a|x} = H^x |a\rangle \langle a|_1 H^x \otimes |xa\rangle \langle xa|_2 \tag{7.13}$$

$$B_{b|y} = H^y |b\rangle \langle b|_3 H^y \otimes |yb\rangle \langle yb|_4 \tag{7.14}$$

$$C_{c|z} = H^z |c\rangle \langle c|_5 H^z \otimes |zc\rangle \langle zc|_6. \tag{7.15}$$

We denote $|000\rangle, |101\rangle, |+10\rangle, |-11\rangle, |100\rangle, |001\rangle, |-10\rangle, |+11\rangle$ as $|\mathbf{0}\rangle, |\mathbf{1}\rangle, |\mathbf{2}\rangle, |\mathbf{3}\rangle, |\mathbf{4}\rangle, |\mathbf{5}\rangle, |\mathbf{6}\rangle, |\mathbf{7}\rangle$ and $|x\rangle\langle x|$ as $[x]$. Then the joint map Γ is written as

$$\begin{aligned} \Gamma = & \frac{1}{2}([000] + [111] + [012] + [103] + [031] + [120] + [023] + [132] \\ & + [201] + [310] + [213] + [302] + [230] + [321] + [222] + [333]) \end{aligned} \quad (7.16)$$

We show the existence of a LOCC protocol implies a contradiction. First, we show the following lemma about a condition of LOCC operators.

Lemma 3. *If there exist non-zero positive semidefinite operators $A_i \in Pos^*(\mathcal{H}_1 \otimes \mathcal{H}_2)$, $B_i \in Pos^*(\mathcal{H}_3 \otimes \mathcal{H}_4)$ and $C_i \in Pos^*(\mathcal{H}_5 \otimes \mathcal{H}_6)$ such that*

$$\sum_i A_i \otimes B_i \otimes C_i = \Gamma, \quad (7.17)$$

where $Pos^*(\mathcal{H})$ is a set of positive operators with at least one non-zero diagonal element, then

$$\begin{aligned} \forall i, (A_i, B_i, C_i) \in \{ & (\alpha[\mathbf{0}], \beta[\mathbf{0}], \gamma[\mathbf{0}]), \\ & (\alpha[\mathbf{1}], \beta[\mathbf{2}], \gamma[\mathbf{0}]), \\ & (\alpha[\mathbf{2}], \beta[\mathbf{3}], \gamma[\mathbf{0}]), \\ & (\alpha[\mathbf{3}], \beta[\mathbf{1}], \gamma[\mathbf{0}]), \\ & (\alpha[\mathbf{0}], \beta[\mathbf{3}], \gamma[\mathbf{1}]), \\ & (\alpha[\mathbf{1}], \beta[\mathbf{1}], \gamma[\mathbf{1}]), \\ & (\alpha[\mathbf{2}], \beta[\mathbf{0}], \gamma[\mathbf{1}]), \\ & (\alpha[\mathbf{3}], \beta[\mathbf{2}], \gamma[\mathbf{1}]), \\ & (\alpha[\mathbf{0}], \beta[\mathbf{1}], \gamma[\mathbf{2}]), \\ & (\alpha[\mathbf{1}], \beta[\mathbf{3}], \gamma[\mathbf{2}]), \\ & (\alpha[\mathbf{2}], \beta[\mathbf{2}], \gamma[\mathbf{2}]), \\ & (\alpha[\mathbf{3}], \beta[\mathbf{0}], \gamma[\mathbf{2}]), \\ & (\alpha[\mathbf{0}], \beta[\mathbf{2}], \gamma[\mathbf{3}]), \\ & (\alpha[\mathbf{1}], \beta[\mathbf{0}], \gamma[\mathbf{3}]), \\ & (\alpha[\mathbf{2}], \beta[\mathbf{1}], \gamma[\mathbf{3}]), \\ & (\alpha[\mathbf{3}], \beta[\mathbf{3}], \gamma[\mathbf{3}]) \mid \alpha, \beta, \gamma > 0\}. \end{aligned} \quad (7.18)$$

Proof.

$$\langle \mathbf{00} |_{AB} \Gamma | \mathbf{00} \rangle_{AB} = \sum_i \langle \mathbf{0} | A_i | \mathbf{0} \rangle \langle \mathbf{0} | B_i | \mathbf{0} \rangle C_i = \frac{1}{2} [\mathbf{0}]_C \quad (7.19)$$

implies

$$\forall i \in \{i | \langle \mathbf{0} | A_i | \mathbf{0} \rangle \neq 0 \wedge \langle \mathbf{0} | B_i | \mathbf{0} \rangle \neq 0\}, \exists p > 0, C_i = p[\mathbf{0}]_C, \quad (7.20)$$

where $\mathcal{H}_C = \mathcal{H}_5 \otimes \mathcal{H}_6$. By a similar calculation, we obtain

$$\begin{aligned} \forall i \in \{i | \langle \mathbf{1} | A_i | \mathbf{1} \rangle \neq 0 \wedge \langle \mathbf{2} | B_i | \mathbf{2} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{0}]_C \\ \forall i \in \{i | \langle \mathbf{2} | A_i | \mathbf{2} \rangle \neq 0 \wedge \langle \mathbf{3} | B_i | \mathbf{3} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{0}]_C \\ \forall i \in \{i | \langle \mathbf{3} | A_i | \mathbf{3} \rangle \neq 0 \wedge \langle \mathbf{1} | B_i | \mathbf{1} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{0}]_C \\ \forall i \in \{i | \langle \mathbf{0} | A_i | \mathbf{0} \rangle \neq 0 \wedge \langle \mathbf{3} | B_i | \mathbf{3} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{1}]_C \\ \forall i \in \{i | \langle \mathbf{1} | A_i | \mathbf{1} \rangle \neq 0 \wedge \langle \mathbf{1} | B_i | \mathbf{1} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{1}]_C \\ \forall i \in \{i | \langle \mathbf{2} | A_i | \mathbf{2} \rangle \neq 0 \wedge \langle \mathbf{0} | B_i | \mathbf{0} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{1}]_C \\ \forall i \in \{i | \langle \mathbf{3} | A_i | \mathbf{3} \rangle \neq 0 \wedge \langle \mathbf{2} | B_i | \mathbf{2} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{1}]_C \\ \forall i \in \{i | \langle \mathbf{0} | A_i | \mathbf{0} \rangle \neq 0 \wedge \langle \mathbf{1} | B_i | \mathbf{1} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{2}]_C \\ \forall i \in \{i | \langle \mathbf{1} | A_i | \mathbf{1} \rangle \neq 0 \wedge \langle \mathbf{3} | B_i | \mathbf{3} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{2}]_C \\ \forall i \in \{i | \langle \mathbf{2} | A_i | \mathbf{2} \rangle \neq 0 \wedge \langle \mathbf{2} | B_i | \mathbf{2} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{2}]_C \\ \forall i \in \{i | \langle \mathbf{3} | A_i | \mathbf{3} \rangle \neq 0 \wedge \langle \mathbf{0} | B_i | \mathbf{0} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{2}]_C \\ \forall i \in \{i | \langle \mathbf{0} | A_i | \mathbf{0} \rangle \neq 0 \wedge \langle \mathbf{2} | B_i | \mathbf{2} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{3}]_C \\ \forall i \in \{i | \langle \mathbf{1} | A_i | \mathbf{1} \rangle \neq 0 \wedge \langle \mathbf{0} | B_i | \mathbf{0} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{3}]_C \\ \forall i \in \{i | \langle \mathbf{2} | A_i | \mathbf{2} \rangle \neq 0 \wedge \langle \mathbf{1} | B_i | \mathbf{1} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{3}]_C \\ \forall i \in \{i | \langle \mathbf{3} | A_i | \mathbf{3} \rangle \neq 0 \wedge \langle \mathbf{3} | B_i | \mathbf{3} \rangle \neq 0\}, \exists p > 0, & C_i = p[\mathbf{3}]_C. \end{aligned} \quad (7.21)$$

Since A_i has at least one non-zero diagonal element and we have

$$\forall i, \langle \mathbf{4} | A_i | \mathbf{4} \rangle = \langle \mathbf{5} | A_i | \mathbf{5} \rangle = \langle \mathbf{6} | A_i | \mathbf{6} \rangle = \langle \mathbf{7} | A_i | \mathbf{7} \rangle = 0, \quad (7.22)$$

$$\forall i, \langle \mathbf{0} | A_i | \mathbf{0} \rangle \neq 0 \vee \langle \mathbf{1} | A_i | \mathbf{1} \rangle \neq 0 \vee \langle \mathbf{2} | A_i | \mathbf{2} \rangle \neq 0 \vee \langle \mathbf{3} | A_i | \mathbf{3} \rangle \neq 0. \quad (7.23)$$

The same property also holds for B_i . Thus,

$$\forall i, C_i \in \{p[\mathbf{0}]_C, p[\mathbf{1}]_C, p[\mathbf{2}]_C, p[\mathbf{3}]_C | p > 0\}. \quad (7.24)$$

The same property also holds for A_i and B_i :

$$\begin{aligned} \forall i, A_i \in \{p[\mathbf{0}]_A, p[\mathbf{1}]_A, p[\mathbf{2}]_A, p[\mathbf{3}]_A | p > 0\} \\ \forall i, B_i \in \{p[\mathbf{0}]_B, p[\mathbf{1}]_B, p[\mathbf{2}]_B, p[\mathbf{3}]_B | p > 0\}, \end{aligned} \quad (7.25)$$

$$(7.26)$$

where $\mathcal{H}_A = \mathcal{H}_1 \otimes \mathcal{H}_2$ and $\mathcal{H}_B = \mathcal{H}_3 \otimes \mathcal{H}_4$. \square

Next, we prove that the map Γ cannot be implemented by an operation in finite-round LOCC.

Proof. If there exists an element in finite-round LOCC implementing Γ , there exists *accumulated operator* $\{A_{\mathbf{m}} \in \mathbf{Pos}(\mathcal{H}_1 \otimes \mathcal{H}_2), B_{\mathbf{m}} \in \mathbf{Pos}(\mathcal{H}_3 \otimes \mathcal{H}_4), C_{\mathbf{m}} \in \mathbf{Pos}(\mathcal{H}_5 \otimes \mathcal{H}_6)\}$ which represents LOCC, where $\mathbf{m} = (m_1, m_2, \dots, m_N)$ represents all the measurement outcomes and m_i represents the i -th measurement outcome. By using Lemma 3, for all \mathbf{m} such that $A_{\mathbf{m}} \otimes B_{\mathbf{m}} \otimes C_{\mathbf{m}} \neq \mathbf{0}$, $(A_{\mathbf{m}}, B_{\mathbf{m}}, C_{\mathbf{m}})$ is an element of Eq.(7.18). Thus, we obtain that a set of all the measurement outcomes \mathbf{M} consists of eleven subsets corresponding to the measurement outcomes,

$$\mathbf{M} = \mathbf{M}_{null} \cup \left(\bigcup_{c \in \mathbf{C}} \mathbf{M}_c \right), \quad (7.27)$$

$$\begin{aligned} \mathbf{C} = \{ & 000, 111, + + +, - - -, 01+, 1+0, +01, 0+ -, \\ & + - 0, -0+, 0-1, -10, 10-, 1-+, -+1, +1-\}, \end{aligned} \quad (7.28)$$

such that

$$\begin{aligned} \forall \mathbf{m} \in \mathbf{M}_{null}, \text{tr}_{2,4,6}[A_{\mathbf{m}} \otimes B_{\mathbf{m}} \otimes C_{\mathbf{m}}] &= 0, \\ \forall c \in \mathbf{C}, \forall \mathbf{m} \in \mathbf{M}_c, \exists \alpha > 0 \text{tr}_{2,4,6}[A_{\mathbf{m}} \otimes B_{\mathbf{m}} \otimes C_{\mathbf{m}}] &= \alpha[c]. \end{aligned} \quad (7.29)$$

Since Γ is invariant under the permutation of parties, without loss of generality, we can assume that Alice performs the last measurement and obtain the measurement result denoted by m_N . Since Bob and Charlie's accumulated operators do not depend on m_N , i.e., we have

$$\forall m_1, \dots, \forall m_N, \forall m'_N, B_{(m_1, \dots, m_{N-1}, m_N)} = B_{(m_1, \dots, m_{N-1}, m'_N)}, \quad (7.30)$$

$$\forall m_1, \dots, \forall m_N, \forall m'_N, C_{(m_1, \dots, m_{N-1}, m_N)} = C_{(m_1, \dots, m_{N-1}, m'_N)}, \quad (7.31)$$

if $(m_1, \dots, m_{N-1}, m_N) \in \mathbf{M}_c$, for all m'_N

$$(m_1, \dots, m_{N-1}, m'_N) \in \mathbf{M}_c \cup \mathbf{M}_{null}. \quad (7.32)$$

This property holds for the other subsets except \mathbf{M}_{null} . Letting

$$\begin{aligned} \mathbf{m}' &= (m_1, \dots, m_{N-1}), \\ A_{\mathbf{m}'} &= \sum_{m_N} A_{\mathbf{m}} \end{aligned} \quad (7.33)$$

$$\begin{aligned} B_{\mathbf{m}'} &= B_{(m_1, \dots, m_{N-1}, 0)}, \\ C_{\mathbf{m}'} &= C_{(m_1, \dots, m_{N-1}, 0)}, \end{aligned} \quad (7.34)$$

$$(7.35)$$

we obtain

$$\begin{aligned} \forall \mathbf{m}' \in \mathbf{M}'_{null}, \text{tr}_{2,4,6}[A_{\mathbf{m}'} \otimes B_{\mathbf{m}'} \otimes C_{\mathbf{m}'}] &= 0 \\ \forall c \in \mathbf{C}, \forall \mathbf{m}' \in \mathbf{M}'_c, \exists \alpha > 0 \text{tr}_{2,4,6}[A_{\mathbf{m}'} \otimes B_{\mathbf{m}'} \otimes C_{\mathbf{m}'}] &= \alpha[c], \end{aligned} \quad (7.36)$$

where \mathbf{M}'_{null} and \mathbf{M}'_c are subsets of measurement outcomes (m_1, \dots, m_{N-1}) .

Since $\text{tr}_2[A_{\mathbf{m}'}] = \text{tr}_2[\sum_{m_N} A_{\mathbf{m}}]$ does not depend on m_{N-1} if the $(N-1)$ -th measurement is performed by Bob or Charlie, we can repeat this procedure until summing up all the measurement outcomes. Then we obtain

$$\text{tr}_{2,4,6} \left[\sum_{\mathbf{m}} A_{\mathbf{m}} \otimes B_{\mathbf{m}} \otimes C_{\mathbf{m}} \right] = 0. \quad (7.37)$$

This is a contradiction to the property of the accumulated operator of which trace of the sum is identity.

□

Chapter 8

Summary and Discussions of Part III

8.1 Summary

We have studied the roles of quantum communication connecting local operations in DQC, in particular a class of quantum operations implemented in DQC called SEP. Since quantum communication can be implemented by entanglement assisted classical communication, we analyze entanglement and classical communication required for DQC.

First, we have derived the necessary and sufficient amount of the entanglement resource for a DQC task to perfectly discriminate a state from a given orthonormal basis states by one-way LOCC in terms of an entanglement measure, the Schmidt rank of a required entanglement resource. We have constructed a two-way LOCC protocol which consumes less amount of entanglement resources than the optimal one-way LOCC protocol.

Second, we have developed a framework to describe deterministic joint quantum operations in DQC. In the framework, we have introduced a causal relation between the classical outputs and classical inputs of the local operations without predefined causal order but still within quantum mechanics, called “classical communication” without predefined causal order (CC^*). We have shown that local operations and CC^* ($LOCC^*$) with partial order can be simulated by local operations and normal classical communication. On the other hand, CC^* without partial order, which can be interpreted as “classical communication” without causal order, is necessary to implement non-LOCC SEP. Since we show that $LOCC^*$ is equivalent to SEP, entanglement and classical communication required for implementing SEP by entanglement assisted LOCC can be substituted by CC^* without using an entanglement resource.

Third, we have investigated the power of CC^* in terms of SLOCC and quantum processes. We have shown that the super class of LOCC^* is simulatable by SLOCC and vice versa, and LOCC^* is simulatable by SLOCC with a constant success probability independent of an input state and vice versa. Then, we have investigated the relationship between LOCC^* and local operations connected by a classical quantum process (LOCQP). We have shown that LOCQP is equivalent to a set of probabilistic mixtures of one-way LOCC in bipartite cases. On the other hand, we have shown that LOCQP is not included in LOCC in tripartite cases by constructing an example of operations in non-LOCC SEP by using LOCQP.

8.2 Discussion

- **The amount of entanglement required for local state discrimination**

We have analyzed the difference in the amount of entanglement required for local state discrimination in one-round LOCC and multi-round LOCC in terms of the Schmidt rank. However, the minimum amount of required entanglement in terms of entanglement entropy, widely used in quantum information science [107], is still unknown. Even the minimum entanglement entropy required for implementing V_d defined in Eq.(6.3) is unknown. In the following, we analyze a lower bound of the entanglement entropy necessary to implement V_d . We define the Schmidt strength $H(U)$ of a unitary operator U on $\mathcal{H}_A \otimes \mathcal{H}_B$ as the Shannon entropy of the square of the operator Schmidt coefficients of U . The Schmidt strength $H(V_d)$ gives a lower bound of the entanglement entropy necessary to implement V_d by LOCC [99].

Let an operator Schmidt decomposition of V_d be

$$V_d = \sum_k \lambda_k A_k \otimes B_k, \quad (8.1)$$

where $\{A_k \in \mathbf{L}(\mathcal{H}_A)\}_k$ and $\{B_k \in \mathbf{L}(\mathcal{H}_B)\}_k$ are sets of orthonormal operators. The Schmidt strength $H(V_d)$ is defined by

$$H(V_d) = \sum_k -\lambda_k^2 \log_2(\lambda_k^2). \quad (8.2)$$

In order to apply the operator Schmidt decomposition to V_d , we define $V'_d \in \mathbf{L}(\mathcal{H}_B \otimes \mathcal{H}_B : \mathcal{H}_A \otimes \mathcal{H}_A)$ by

$$V'_d = \sum_{i,j} (\langle i|_B V_d |j\rangle_A) \otimes |j\rangle_A \langle i|_B, \quad (8.3)$$

where $\{|i\rangle_X\}_i$ ($X = A, B$) is the computational basis. By using the operator Schmidt decomposition of V_d , V'_d can be decomposed into

$$V'_d = \sum_k \lambda_k \sqrt{\dim(\mathcal{H}_A) \dim(\mathcal{H}_B)} |A_k\rangle_{AA} \langle B_k|_{BB}, \quad (8.4)$$

where $|A_k\rangle = \frac{1}{\sqrt{\dim(\mathcal{H}_A)}} \sum_i (A_k|i\rangle_A) |i\rangle_A$, $\langle B_k| = \frac{1}{\sqrt{\dim(\mathcal{H}_B)}} \sum_i (\langle i|_B B_k) \langle i|_B$. Note that since $\{A_k\}_k$ and $\{B_k\}_k$ are sets of orthonormal operators, i.e. $\text{tr}(A_k^\dagger A_l) = \dim(\mathcal{H}_A) \delta_{k,l}$ and $\text{tr}(B_k^\dagger B_l) = \dim(\mathcal{H}_B) \delta_{k,l}$, $\{|A_k\rangle\}_k$ and $\{|B_k\rangle\}_k$ are sets of orthonormal states, i.e.

$$\langle A_k|A_l\rangle = \delta_{k,l}, \quad (8.5)$$

$$\langle B_k|B_l\rangle = \delta_{k,l}. \quad (8.6)$$

The operator Schmidt coefficients $\{\lambda_k\}_k$ is obtained by calculating the eigenvalues of

$$V'_d V_d'^\dagger = \sum_k \lambda_k^2 \dim(\mathcal{H}_A) \dim(\mathcal{H}_B) |A_k\rangle_{AA} \langle A_k|_{AA}. \quad (8.7)$$

By straightforward calculation, we obtain

$$V'_d V_d'^\dagger = \begin{pmatrix} d+1 & d-1 & d-1 \\ d-1 & d+1 & d+1 \\ d-1 & d+1 & d+1 \end{pmatrix}, \quad (8.8)$$

where we use the matrix representation in terms of the computational basis. Thus, the operator Schmidt coefficients are given by

$$\{\lambda_k^2\}_{k=0,1} = \left\{ \frac{3(d+1) - \sqrt{9d^2 - 14d + 9}}{6(d+1)}, \frac{3(d+1) + \sqrt{9d^2 - 14d + 9}}{6(d+1)} \right\}. \quad (8.9)$$

$H(V_d)$ decreases when d increases as shown in Fig. 8.1. Since when d goes to infinity, $\lambda_0 \rightarrow 0$, $\lambda_1 \rightarrow 1$ and $-\lambda_k^2 \log_2(\lambda_k^2) \rightarrow 0$ for $k = 0, 1$, $H(V_d)$ decreases to 0 when $d \rightarrow \infty$.

• Multipartite LOCC* and LOCQP

Multipartite LOCC* is defined by a set of CPTP maps \mathcal{M} given in the form of

$$\mathcal{M} = \sum_{i_1, \dots, i_N, o_1, \dots, o_N} p(i_1, \dots, i_N | o_1, \dots, o_N) \mathcal{E}_{o_1|i_1}^{(1)} \otimes \dots \otimes \mathcal{E}_{o_N|i_N}^{(N)}, \quad (8.10)$$

where $p(i_1, \dots, i_N | o_1, \dots, o_N)$ is a conditional probability distribution and $\{\mathcal{E}_{o_k|i_k}^{(k)} : \mathbf{L}(\mathcal{H}_{I_k}) \rightarrow \mathbf{L}(\mathcal{H}_{O_k})\}_{o_k}$ is a local operation performed by the k -th

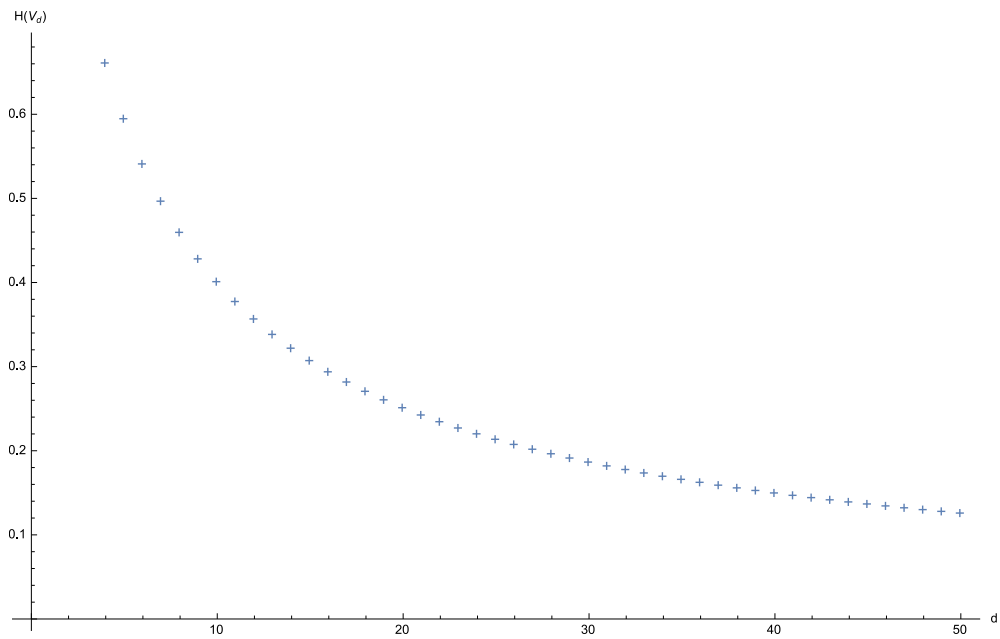


Figure 8.1: **A lower bound of entanglement for implementing V_d by LOCC.** A lower bound is calculated by evaluating $H(V_d) = \sum_i -\lambda_i^2 \log_2(\lambda_i^2)$, where $\{\lambda_i\}_i$ is the operator Schmidt coefficients of V_d .

party with a classical input i_k and a classical output o_k . In Appendix B.9, we show that multipartite LOCC* as well as bipartite LOCC* is equivalent to SEP.

On the other hand, multipartite LOCQP is defined by a set of CPTP maps \mathcal{M} given in the form of Eq.(8.10) where a conditional probability distribution $p(i_1, \dots, i_N | o_1, \dots, o_N)$ satisfies

$$\sum_{i_1, \dots, i_N, o_1, \dots, o_N} p(i_1, \dots, i_N | o_1, \dots, o_N) \mathcal{E}_{o_1 | i_1}^{(1)} \otimes \dots \otimes \mathcal{E}_{o_N | i_N}^{(N)} \in \mathbf{C}(\mathcal{H}_{I_1} \otimes \dots \otimes \mathcal{H}_{I_N} : \mathcal{H}_{O_1} \otimes \dots \otimes \mathcal{H}_{O_N}), \quad (8.11)$$

for all quantum instruments $\{\mathcal{E}_{o_1 | i_1}^{(1)}\}_{o_1}$, $\{\mathcal{E}_{o_2 | i_2}^{(2)}\}_{o_2}$ and so on. It is easy to verify that LOCC* is larger than LOCQP, however we do not know whether multipartite (more than two parties) LOCC* is strictly larger than multipartite LOCQP or not. In [106], multipartite causally non-separable CQP is proposed. This implies that we may be able to construct elements of non-LOCC SEP by using such multipartite causally non-separable CQP.

Part IV
Conclusion

In this thesis, we have focused on two questions concerning the roles of entanglement in DQC:

- Which unitary operations are implementable over a given quantum network represented by an entanglement resource?
- What are resources substituting entanglement and classical communication consumed in entanglement assisted LOCC for implementing SEP?

In Part II, we have investigated the first question by analyzing implementability of k -qubit unitary operations over the (k, N) -cluster networks where inputs and outputs of quantum computation are given in all separated nodes and quantum communication between nodes is restricted to sending just one-qubit while classical communication is freely allowed. We have considered a one-shot scenario where we can use a given cluster network only once and exact implementation without error is required. We have presented a method to obtain quantum circuit representations of unitary operations implementable over a given cluster network. For the (k, N) -cluster networks with $k = 2, 3$, we have shown that our method provides all implementable unitary operations over the cluster network. As a first step to find the fundamental primitive networks of network coding for quantum computation, we have shown that both the butterfly and grail networks are sufficient resources for implementing arbitrary two-qubit unitary operations, meanwhile the $(2, 2)$ -cluster network is not sufficient to implement arbitrary two-qubit unitary operations even probabilistically. Our methods are applicable to generalized cluster networks, which may be a first step to investigate quantum computation over a more general network. It also gives a new insight for implementable unitary operations in MBQC where the angle of each projective measurement can be restricted.

In Part III, we have investigated the second question in terms of entanglement and causal relation in classical communication. First, we have derived the amount of the entanglement resource that is necessary and sufficient for a DQC task that perfectly discriminates a state from a given orthonormal basis states by one-way LOCC in terms of the Schmidt rank of an entanglement resource. We have constructed a two-way LOCC protocol which consumes less amount of entanglement resources than the optimal one-way LOCC protocol. Second, we have developed a framework to describe deterministic joint quantum operations in DQC. In the framework, we have introduced a causal relation between the classical outputs and classical inputs of the local operations without predefined causal order but still within quantum mechanics, called “classical communication” without predefined causal order (CC^*). We have shown that local operations and CC^* ($LOCC^*$) with partial order can be simulated by normal LOCC. In contrast, CC^* without partial order, which can be interpreted as “classical communication” without causal order, is necessary to implement an operation in non-LOCC SEP. Since we show

that LOCC* is equivalent to SEP, entanglement and classical communication required for implementing SEP by entanglement assisted LOCC can be substituted by CC*. Note that in LOCC*, two assumptions of local operations, (a) they are partially ordered and (b) the choice of a local operation does not depend on resources connecting the local operation, are relaxed.

We have investigated the power of CC* in terms of SLOCC and quantum processes. We have shown that the super class of LOCC* is simulatable by SLOCC and vice versa, and LOCC* is simulatable by SLOCC with a constant success probability independent of an input state and vice versa. Next, we have investigated the relationship between LOCC* and local operations linked by a classical quantum process (LOCQP). We have shown that LOCQP is equivalent to a set of probabilistic mixtures of one-way LOCC in bipartite cases. On the other hand, we have shown that LOCQP is not included in LOCC in tripartite cases by constructing an example of operations in non-LOCC SEP by using LOCQP. In [58, 60], a few examples of joint quantum operations consisting of two local operations linked by quantum processes that cannot be implemented by using the local operations connected by a causally ordered quantum communication are shown. However, the joint quantum operations are implementable if we are allowed to use each local operation twice and a causally ordered quantum communication. In contrast, our example of LOCQP, which is an operation in non-LOCC SEP, cannot be implemented even if finite times use of local operations connected by a causally ordered classical communication are allowed. Thus, joint quantum operations respecting the restriction for classical quantum processes have a power of not only *folding* several local operations localized in a spacetime but more. LOCC* gives a unified description of LOCC and SEP, and provides a new operational meaning of the gap between LOCC and SEP. LOCQP gives a new method to construct an element in the gap between LOCC and SEP while very few examples are known. LOCQP also gives a new insight into the interpretation of the restriction for classical quantum processes.

Part V
Appendix

Appendix A

Quantum computation over quantum networks

A.1 A LOCC protocol for controlled unitary operations

We show a construction of a protocol to implement a three-qubit fully controlled unitary operation $C_{l,m;n}$ on qubits located at a set of vertically aligned nodes \mathcal{V}_j^v over the (k, N) -cluster networks, where l and m represent two control qubits at nodes $v_{l,j}$ and $v_{m,j}$ respectively, and n represents a target qubit at node $v_{n,j}$. We present a LOCC protocol to implement $C_{l,m;n}$ assisted by the resource states consisting of the EPR pairs corresponding to the vertical edges \mathcal{S}_j of the (k, N) -cluster networks.

We consider to implement $C_{l,m;n}$ on a state of three qubits indexed by Q_l , Q_m and Q_n at node $v_{l,j}$, $v_{m,j}$ and $v_{n,j}$, respectively, and its explicit form is given by

$$C_{l,m;n}(\{u_n^{(ab)}\}) := \sum_{a=0}^1 \sum_{b=0}^1 |ab\rangle\langle ab|_{lm} \otimes u_n^{(ab)} \quad (\text{A.1})$$

where $\{|ab\rangle\}_{a,b=\{0,1\}}$ is the two-qubit computational basis of $\mathcal{H}_{Q_l} \otimes \mathcal{H}_{Q_m}$ of the two controlled qubits and $u_n^{(ab)}$ acts on \mathcal{H}_{Q_n} of the target qubit.

To show how our LOCC protocol works, we consider an arbitrary state of the control qubits by $\sum \lambda_{ab}|ab\rangle_{lm} \in \mathcal{H}_{Q_l} \otimes \mathcal{H}_{Q_m}$ where $\{\lambda_{ab}\}$ is a set of arbitrary complex coefficients satisfying the normalization condition $\sum_{a,b} |\lambda_{ab}|^2 = 1$ and we represent an arbitrary state of the target qubit by $|\phi\rangle \in \mathcal{H}_{Q_n}$. In the following, we show that our protocol transforms the joint state of controlled qubits and a target qubit to

$$C_{l,m;n} \sum_{a,b} \lambda_{ab}|ab\rangle_{lm} |\phi\rangle_n = \sum_{a,b} \lambda_{ab}|ab\rangle_{lm} u_n^{(ab)} |\phi\rangle_n.$$

The protocol for implementing three qubit fully controlled unitary operations (see Fig. A.1) :

1. Ancillary qubits indexed by $Q_{l'}$, $Q_{m'}$ are introduced at nodes $v_{l,j}$ and $v_{m,j}$ respectively. Set both of the ancillary qubits to be in $|0\rangle$. Each of the two states of control qubits Q_l and Q_m is transformed to a two-qubit state by applying a CNOT gate on the control qubit and the ancillary qubit at the same node, namely applying CNOT on Q_l and $Q_{l'}$ and also Q_m and $Q_{m'}$. Then the joint state of five qubits Q_l , $Q_{l'}$, Q_m , $Q_{m'}$ and Q_n is given by

$$\sum_{a,b} \lambda_{ab} |ab\rangle_{lm} |ab\rangle_{l'm'} |\phi\rangle_n. \quad (\text{A.2})$$

2. By consuming the EPR pairs corresponding to the vertical edges \mathcal{S}_j between $v_{l,j}$ and $v_{n,j}$ and also between $v_{m,j}$ and $v_{n,j}$, perform quantum teleportation to transmit the states of qubits $Q_{l'}$ and $Q_{m'}$ from nodes $v_{l,j}$ and $v_{m,j}$ to $v_{n,j}$. A circuit representation of the protocol of quantum teleportation represented by \mathcal{T} in Fig. A.1 is given by Fig. 2.3. Note that in case of $n \neq l \pm 1$, we have to repeat the teleportation protocol to transmit a quantum state between the nodes via the neighboring nodes. Thus all the EPR pairs corresponding to the vertical edges between l and n are consumed for performing teleportation. We denote indices of two qubits at node $v_{n,j}$ representing the teleported states from $Q_{l'}$ and $Q_{m'}$ by $Q_{l''}$ and $Q_{m''}$, respectively.

3. At node $v_{n,j}$, perform $C_{l,m;n}$ on $\mathcal{H}_{Q_{l''}} \otimes \mathcal{H}_{Q_{m''}} \otimes \mathcal{H}_{Q_n}$. Then we obtain the state given by

$$\sum_{a,b} \lambda_{ab} |ab\rangle_{lm} |ab\rangle_{l''m''} u_n^{(ab)} |\phi\rangle_n. \quad (\text{A.3})$$

4. At node $v_{n,j}$, we apply the Hadamard operations and perform projective measurements in the computational basis on both $\mathcal{H}_{Q_{l''}}$ and $\mathcal{H}_{Q_{m''}}$. The measurement outcomes of qubits $Q_{l''}$ and $Q_{m''}$ are sent to nodes $v_{l,j}$ and $v_{m,j}$, respectively, by classical communication. At each of nodes $v_{l,j}$ and $v_{m,j}$, if the measurement outcome is 0, do nothing, and if the outcome is 1, perform Z for a correction on qubit Q_l or Q_m . By straightforward calculation, we obtain the state of three qubits Q_l , Q_m and Q_n at nodes $v_{l,j}$, $v_{m,j}$ and $v_{l,n}$, respectively, given by

$$\sum_{a,b} \lambda_{ab} |ab\rangle_{lm} u_n^{(ab)} |\phi\rangle_n. \quad (\text{A.4})$$

Therefore, $C_{l,m;n}$ is successfully applied on the control qubits at nodes $v_{l,j}$ and $v_{m,j}$ and the target qubit at node $v_{n,j}$ by LOCC assisted by the EPR pairs corresponding to the vertical edges \mathcal{S}_j between nodes $v_{l,j}$ and $v_{m,j}$.

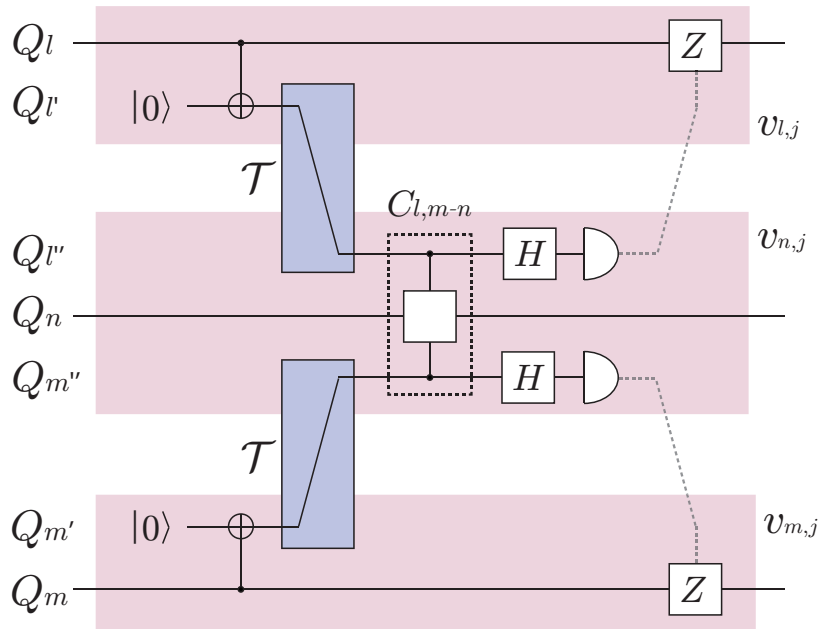


Figure A.1: A quantum circuit representation of the LOCC protocol implementing a three-qubit fully unitary operation $C_{l,m;n}$, where qubits in the first shaded region are at the node $v_{l,j}$, those in the second shaded region are at the node $v_{n,j}$ and those in the third shaded region are at the node $v_{m,j}$. \mathcal{T} represents teleportation of a qubit state. A circuit representation is given by Fig. 2.3. The protocol consists of introducing ancillary qubits $Q_{l'}$ and $Q_{m'}$ at the nodes $v_{l,j}$ and $v_{m,j}$, respectively, teleporting ancillary qubit states from the nodes $v_{l,j}$ and $v_{m,j}$ to the node $v_{n,j}$ represented by qubits $Q_{l''}$ and $Q_{m''}$ and a target qubit Q_n at the node $v_{n,j}$, performing Hadamard operations and measurements in the computational basis on $Q_{l''}$ and $Q_{m''}$ at node $v_{n,j}$ and finally applying conditional Z operations depending on the measurement outcome on two control qubits Q_l , Q_m at nodes $v_{l,j}$ and $v_{m,j}$, respectively.

A.2 LOCC implementation of converted quantum circuits

In Appendix A.1, we have shown a protocol to implement a three-qubit fully controlled unitary operation in a set of vertically aligned nodes \mathcal{V}_j^y . In some cases, we can implement more than one three-qubit or two-qubit controlled unitary operations *in parallel* by using the same resource. We show how a sequence of controlled unitary operations represented by converted circuits can be implemented by LOCC assisted by the resource state given by a collection of $(k-1)$ EPR pairs corresponding to a set of vertically aligned edges \mathcal{S}_j in this appendix.

We introduce a new notation for controlled unitary operations for simplifying and unifying descriptions of two-qubit and three-qubit controlled unitary operations. We represent a two-qubit controlled unitary operations that controls the i -th qubit and targets the j -th qubit as

$$(i, i; j), \quad (\text{A.5})$$

and a three-qubit controlled unitary gates that controls the i -th and j -th qubit and targets the k -th qubit as

$$(i, j; k). \quad (\text{A.6})$$

Note that we represented $(i, i; j)$ as $C_{i,j}$ and $(i, j; k)$ as $C_{i,j;k}$ in the previous sections. Let $G = \{g_n\}$ be a sequence of controlled unitary operations that is added in step 2 of the conversion protocol. For example, the converted circuit represented by Fig. A.2 is described by a sequence

$$g_1 = (1, 1; 2) \quad (\text{A.7})$$

$$g_2 = (4, 4; 2) \quad (\text{A.8})$$

$$g_3 = (1, 4; 2) \quad (\text{A.9})$$

$$g_4 = (4, 4; 5) \quad (\text{A.10})$$

$$g_5 = (4, 4; 3) \quad (\text{A.11})$$

$$g_6 = (5, 5; 6) \quad (\text{A.12})$$

$$g_7 = (4, 4; 5). \quad (\text{A.13})$$

Let \mathcal{C}_i be a set of controlled unitary operations that controls the i -th qubit:

$$\mathcal{C}_i = \{(a, b; c) \in G; a = i \vee b = i\}. \quad (\text{A.14})$$

For example, for G defined by Eqs. (A.7)-(A.13),

$$\mathcal{C}_1 = \{g_1, g_3\} \quad (\text{A.15})$$

$$\mathcal{C}_4 = \{g_2, g_3, g_4, g_5, g_7\} \quad (\text{A.16})$$

$$\mathcal{C}_5 = \{g_6\} \quad (\text{A.17})$$

$$\mathcal{C}_2 = \mathcal{C}_3 = \mathcal{C}_6 = \emptyset. \quad (\text{A.18})$$

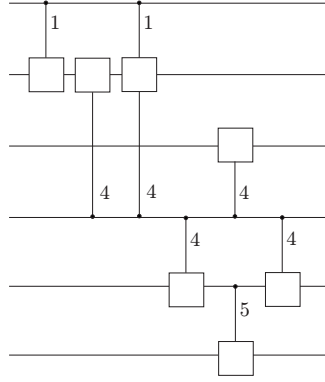


Figure A.2: An example of a converted quantum circuit obtained by step 2 of the conversion protocol.

Define the *range* of $\mathcal{C}_i \neq \emptyset$ as

$$\begin{aligned} \text{range}(\mathcal{C}_i) = & (\min\{i, \min_c\{(a, b; c) \in \mathcal{C}_i\}\}, \\ & \max\{i, \max_c\{(a, b; c) \in \mathcal{C}_i\}\}). \end{aligned} \quad (\text{A.19})$$

For example, for \mathcal{C}_i defined by Eqs. (A.15)-(A.18),

$$\text{range}(\mathcal{C}_1) = (1, 2) \quad (\text{A.20})$$

$$\text{range}(\mathcal{C}_4) = (2, 5) \quad (\text{A.21})$$

$$\text{range}(\mathcal{C}_5) = (5, 6). \quad (\text{A.22})$$

All the controlled unitary operations in G are implementable by using the following subroutines extending the one presented in Appendix A.1.

Subroutines for implementing a sequence of controlled unitary operation in G :

Subroutines

1. For applying gates in \mathcal{C}_i , we add an ancillary qubit state entangled to the i -th qubit state by preparing an ancillary qubit in $|0\rangle$ and applying CNOT where the ancillary qubit is the target qubit of CNOT. Then the ancillary qubit state is sent from the i -th node $v_{i,j} \in \mathcal{V}_j^v$ to the target node by using teleportation. If several different target qubits are included in \mathcal{C}_i , add another ancillary qubit by the same method at a target node, keep one of the ancillary qubits at the target node and send the other to the next target node. We consume n_i EPR pairs to teleport ancillary qubit states to the target nodes, where $n_i = b - a$ and $\text{range}(\mathcal{C}_i) = (a, b)$. Since there is no overlap between

ranges of \mathcal{C}_i and there is no target unitary operation inserted between control qubits, we can teleport all the ancillary qubit states entangled to the control states to all the target nodes by just consuming $(k - 1)$ EPR pairs.

2. We apply all the controlled unitary operations in G in the target nodes by using the teleported ancillary qubit states entangled to the control qubit states as the control qubits.
3. We decouple the ancillary qubit states by performing the projective measurements on the ancillary qubits similarly to the case of Appendix A.1 in the target nodes and apply correction unitary operations in the control nodes depending on the measurement outcomes.

A.3 Converted circuit of $(2, N)$ and $(3, N)$ -cluster network

First, we prove that any converted circuits of a $(2, N)$ -cluster network can be simulated by a circuit consisting of a sequence of N two-qubit unitary operations and local unitary operations. In this case, only two-qubit unitary operations $(1, 1; 2)$ or $(2, 2; 1)$ can be added in step 2 of the conversion protocol. Since applying the gate $(1, 1; 2)$ sequentially for $k \in \mathbb{N}$ times can be simulated by just one use of gate $(1, 1; 2)$ and gate $(2, 2; 1)$ can be simulated by one use of gate $(1, 1; 2)$ and additional local unitary operations, any circuits generated in step 2 of the conversion protocol can be simulated by one use of $(1, 1; 2)$ and local unitary operations.

Next, we prove that any converted circuits of a $(3, N)$ -cluster network can be simulated by the circuit of a sequence of N three-qubit fully controlled unitary operations given in the form of

$$\begin{aligned} & |00\rangle\langle 00|_{1,3} \otimes u_2^{(00)} + |01\rangle\langle 01|_{1,3} \otimes u_2^{(01)} \\ & + |10\rangle\langle 10|_{1,3} \otimes u_2^{(10)} + |11\rangle\langle 11|_{1,3} \otimes u_2^{(11)} \end{aligned} \quad (\text{A.23})$$

and local unitary operations. In step 2 of the conversion protocol, every converted circuits can be simulated by six classes of circuits shown in Fig. 10.

In the following, we show that all of these six classes (from class i) to class vi) represented in Fig. 10) can be simulated by a three-qubit fully controlled unitary operation and local unitary operations by investigating each class.

- i) A unitary operation obtained by circuit i) is given by

$$\begin{aligned} & |0\rangle\langle 0|_1 \otimes u_2^{(0)} \otimes u_3^{(0)} + |1\rangle\langle 1|_1 \otimes u_2^{(1)} \otimes u_3^{(1)} \\ \stackrel{\text{LU}}{=} & |0\rangle\langle 0|_1 \otimes \mathbb{I}_2 \otimes \mathbb{I}_3 + |1\rangle\langle 1|_1 \otimes u_2^{(1)} u_2^{(0)\dagger} \otimes u_3^{(1)} u_3^{(0)\dagger} \end{aligned} \quad (\text{A.24})$$

A.3. CONVERTED CIRCUIT OF $(2, N)$ AND $(3, N)$ -CLUSTER NETWORK 121

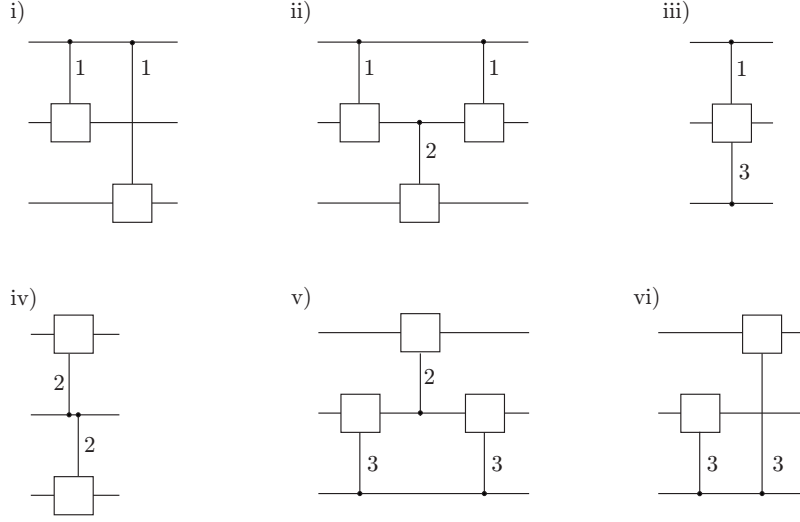


Figure A.3: The six classes of converted quantum circuits obtained by step 2 of the conversion protocol of a $(3, N)$ -cluster network.

where $u_j^{(i)}$ is a one-qubit unitary operation and $\stackrel{\text{LU}}{=}$ represents local unitary equivalence. Diagonalize $u_2^{(1)} u_2^{(0)\dagger}$ and $u_3^{(1)} u_3^{(0)\dagger}$ as

$$u_2^{(1)} u_2^{(0)\dagger} = v_2 \begin{pmatrix} e^{i\theta_1} & 0 \\ 0 & e^{i\theta_2} \end{pmatrix} v_2^\dagger \quad (\text{A.25})$$

$$u_3^{(1)} u_3^{(0)\dagger} = v_3 \begin{pmatrix} e^{i\theta_3} & 0 \\ 0 & e^{i\theta_4} \end{pmatrix} v_3^\dagger. \quad (\text{A.26})$$

Since the right handside of Eq. (A.24) is locally unitarily equivalent to a diagonal unitary operation in the computational basis, this circuit can be simulated by a three-qubit fully controlled unitary operation and local unitary operations.

- ii) In circuit ii), the two-qubit controlled unitary operation $(2, 2; 3)$ can be decomposed into

$$\begin{aligned} & |0\rangle\langle 0|_2 \otimes u_3^{(0)} + |1\rangle\langle 1|_2 \otimes u_3^{(1)} \\ = & v_3 \left(|0\rangle\langle 0|_2 \otimes \mathbb{I}_3 + |1\rangle\langle 1|_2 \otimes \begin{pmatrix} e^{i\theta_1} & 0 \\ 0 & e^{i\theta_2} \end{pmatrix} \right) v_3^\dagger u_3^{(0)} \\ = & (\mathbb{I}_2 \otimes v_3) \\ & \left(\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta_1} \end{pmatrix} \otimes |0\rangle\langle 0|_3 + \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta_2} \end{pmatrix} \otimes |1\rangle\langle 1|_3 \right) \\ & (\mathbb{I}_2 \otimes v_3^\dagger u_3^{(0)}), \end{aligned} \quad (\text{A.27})$$

where v_3 is a unitary operation that diagonalizes $u_3^{(1)}u_3^{(0)\dagger}$. Thus, this circuit is locally unitarily equivalent to a three-qubit fully controlled unitary operation.

- iii) Circuit iii) consists of just a three-qubit fully controlled unitary operation.
- iv) Circuit iv) can be simulated by a three-qubit fully controlled unitary operation and local unitary operations since we can diagonalize a unitary operation obtained by the circuit in the same way as circuit i).
- v) In the same way as circuit ii), circuit v) is locally unitarily equivalent to a three-qubit fully controlled unitary operation.
- vi) In the same way as circuit i), circuit vi) is locally unitarily equivalent to a three-qubit fully controlled unitary operation.

A.4 Maximally entangled state conversion by SEP

We prove a lemma about convertibility of maximally entangled states in this appendix. We analyze a property of bipartite separable maps which preserves entanglement of maximally entangled states.

Let $|\Psi_{in}\rangle = \frac{1}{\sqrt{d}} \sum_i^d |A_i\rangle|B_i\rangle$ and $|\Psi_{out}\rangle = \frac{1}{\sqrt{d}} \sum_i^d |a_i\rangle|b_i\rangle$, where $\{|A_i\rangle \in \mathcal{H}_A\}$ and $\{|B_i\rangle \in \mathcal{H}_B\}$ are orthonormal sets and $\{|a_i\rangle \in \mathcal{H}_a\}$ and $\{|b_i\rangle \in \mathcal{H}_b\}$ are orthonormal bases. Note that $\dim(\mathcal{H}_a) = \dim(\mathcal{H}_b) = d$ but the dimensions of \mathcal{H}_A and \mathcal{H}_B can be higher than d .

Lemma 4. *Let $\{E_k \in \mathbf{L}(\mathcal{H}_A : \mathcal{H}_a)\}, \{F_k \in \mathbf{L}(\mathcal{H}_B : \mathcal{H}_b)\}$ be sets of linear operators. If $\{E_k \otimes F_k\}$ satisfies*

$$\sum_k E_k^\dagger E_k \otimes F_k^\dagger F_k = \mathbb{I}_{AB} \quad (\text{A.28})$$

and for all k ,

$$E_k \otimes F_k |\Psi_{in}\rangle = \sqrt{p_k} |\Psi_{out}\rangle \quad (\text{A.29})$$

is satisfied, then for all $\{k | p_k \neq 0\}$,

$$\exists \alpha_k > 0, \exists U_k^M \in \mathbf{U}(\mathbb{C}^d), E_k^M = \alpha_k U_k^M, F_k^M = \frac{\sqrt{p_k}}{\alpha_k} \overline{U_k^M}, \quad (\text{A.30})$$

where E_k^M and F_k^M are d by d matrices such that $(E_k^M)_{i,j} = \langle a_i | E_k | A_j \rangle$, $(F_k^M)_{i,j} = \langle b_i | F_k | B_j \rangle$, $\mathbf{U}(\mathbb{C}^d)$ is the set of d by d unitary matrices and $\overline{U^M}$ is the complex conjugate of U^M .

Proof. By straightforward calculation, we obtain

$$\begin{aligned} \forall k, E_k^M (F_k^M)^T &= \sqrt{p_k} I_d \\ \Rightarrow \forall k \in \{k | p_k \neq 0\}, F_k^M &= \sqrt{p_k} ((E_k^M)^{-1})^T, \end{aligned} \quad (\text{A.31})$$

and

$$\sum_k (E_k^M)^\dagger E_k^M \otimes (F_k^M)^\dagger F_k^M = I_{d^2}. \quad (\text{A.32})$$

By using Eq. (A.31) and Eq. (A.32), we obtain

$$\begin{aligned} & \text{tr} \left(\sum_k E_k^{M\dagger} E_k^M \otimes F_k^{M\dagger} F_k^M \right) \\ &= \text{tr} \left(\sum_{\{k|p_k \neq 0\}} E_k^{M\dagger} E_k^M \otimes F_k^{M\dagger} F_k^M \right) + \epsilon \\ &= \sum_{\{k|p_k \neq 0\}} p_k \text{tr} \left(E_k^{M\dagger} E_k^M \otimes \overline{(E_k^{M\dagger} E_k^M)^{-1}} \right) + \epsilon = d^2 \\ &\Leftrightarrow \sum_{\{k|p_k \neq 0\}} p_k \text{tr} \left(E_k^{M\dagger} E_k^M \otimes \overline{(E_k^{M\dagger} E_k^M)^{-1}} \right) = d^2 - \epsilon, \end{aligned} \quad (\text{A.33})$$

where $\epsilon = \text{tr} \left(\sum_{\{k|p_k=0\}} E_k^{M\dagger} E_k^M \otimes F_k^{M\dagger} F_k^M \right) \geq 0$. Since E_k^M is a regular matrix, we can let $P_k = E_k^{M\dagger} E_k^M$ be a d by d positive matrix and $\{\lambda_k^i > 0 | i = 0, 1, \dots, d-1\}$ be the set of eigenvalues of P_k . Then the eigenvalues of $(E_k^{M\dagger} E_k^M)^{-1} = \overline{P_k^{-1}}$ are $\{1/\lambda_k^i | i = 0, 1, \dots, d-1\}$ and the condition Eq. (A.33) is given by

$$\sum_{\{k|p_k \neq 0\}} p_k \sum_i \lambda_k^i \sum_j \frac{1}{\lambda_k^j} = d^2 - \epsilon. \quad (\text{A.34})$$

Using the Cauchy-Schwarz inequality, we obtain

$$\begin{aligned} \sum_i \lambda_k^i \sum_j \frac{1}{\lambda_k^j} &= \left(\sum_i \sqrt{\lambda_k^i} \right) \left(\sum_j \sqrt{\frac{1}{\lambda_k^j}} \right) \\ &\geq \left(\sum_i 1 \right)^2 = d^2. \end{aligned} \quad (\text{A.35})$$

The equality holds if and only if $\lambda_k^i = \alpha^2$ for all i . By using Eqs. (A.34)-(A.35) and the fact that $\{p_k | p_k \neq 0\}$ is a probability distribution, we obtain for all $\{k | p_k \neq 0\}$,

$$\exists \alpha > 0; P_k = E_k^{M\dagger} E_k^M = \alpha^2 \mathbb{I}_d, \quad (\text{A.36})$$

$$\epsilon = 0. \quad (\text{A.37})$$

□

A.5 Two conditions in Theorem 1

We show that two conditions in Theorem 1 are equivalent in the case of the $(3, N)$ -cluster networks. For $k = 3$, the 2^k by 2^k unitary matrix V_i^M in Theorem 1 is written by

$$\begin{aligned} V_i^M &= E_{1,i}^{(0)} \otimes E_{2,i}^{(0,0)} \otimes E_{3,i}^{(0)} \\ &\quad + E_{1,i}^{(0)} \otimes E_{2,i}^{(0,1)} \otimes E_{3,i}^{(1)} \\ &\quad + E_{1,i}^{(1)} \otimes E_{2,i}^{(1,0)} \otimes E_{3,i}^{(0)} \\ &\quad + E_{1,i}^{(1)} \otimes E_{2,i}^{(1,1)} \otimes E_{3,i}^{(1)}. \end{aligned} \quad (\text{A.38})$$

By using the result on local unitary equivalence of unitary operations with operator Schmidt rank 2 obtained by Cohen and Yu [98] (Theorem 1 of [98]), we have

$$V_i^M \stackrel{\text{LU}}{=} |0\rangle\langle 0|_A \otimes W_{BC}^{(0)} + |1\rangle\langle 1|_A \otimes W_{BC}^{(1)} \quad (\text{A.39})$$

$$= W_{AB}^{(0)} \otimes |0\rangle\langle 0|_C + W_{AB}^{(1)} \otimes |1\rangle\langle 1|_C, \quad (\text{A.40})$$

where $W_{BC}^{(i)}$ and $W_{AB}^{(i)}$ are unitary matrices, $\stackrel{\text{LU}}{=}$ represents a local unitary equivalence and we identify a three-qubit unitary operation on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ as its matrix representation V_i^M . Thus, it is shown that

$$\begin{aligned} V_i^M \stackrel{\text{LU}}{=} & |00\rangle\langle 00|_{AC} \otimes W_B^{(00)} + |01\rangle\langle 01|_{AC} \otimes W_B^{(01)} \\ & + |10\rangle\langle 10|_{AC} \otimes W_B^{(10)} + |11\rangle\langle 11|_{AC} \otimes W_B^{(11)}, \end{aligned} \quad (\text{A.41})$$

where $W_B^{(ij)}$ is a 2 by 2 unitary matrix. Statements i) and ii) in Theorem 2 of the main text are equivalent in the case of $(3, N)$ -cluster networks since V_i^M is a fully controlled three-qubit unitary operation and N fully controlled three-qubit unitary operations are implementable by a converted circuit of the $(3, N)$ -cluster networks.

A.6 Network coding for the butterfly network

We show that the quantum circuit presented in Fig. 4.5 implements a two-qubit global unitary $U_{global}(x, y, z)$ given by Eq.(3.11) for arbitrary parameters $x, y, z \in \mathbb{R}$. $U_{global}(x, y, z)$ can be decomposed into

$$U_{global}(x, y, z) = \sum_i \lambda_i |\Phi^{(i)}\rangle \langle \Phi^{(i)}| \quad (\text{A.42})$$

by using its eigenvalues $\{\lambda_i\}_i$ and eigenvectors $\{|\Phi^{(i)}\rangle\}_i$ such that

$$\lambda_0 = e^{i(x-y+z)}, \lambda_1 = e^{i(-x+y+z)}, \lambda_2 = e^{i(x+y-z)}, \lambda_3 = e^{i(-x-y-z)} \quad (\text{A.43})$$

$$|\Phi^{(0)}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (\text{A.44})$$

$$|\Phi^{(1)}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (\text{A.45})$$

$$|\Phi^{(2)}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (\text{A.46})$$

$$|\Phi^{(3)}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \quad (\text{A.47})$$

Thus, in order to show an arbitrary input state $|\phi\rangle$ is transformed into $U_{global}(x, y, z)|\phi\rangle$ through the quantum circuit, it is sufficient to show that the eigenvectors $\{|\Phi^{(i)}\rangle\}_i$ are transformed into $\{\lambda_i|\Phi^{(i)}\rangle\}_i$ and when a measurement $\{M_m\}_{m \in \Omega}$ is performed, the probability of obtaining a measurement outcome must be equal, i.e. for all $m \in \Omega$,

$$\langle \Phi^{(0)} | M_m | \Phi^{(0)} \rangle = \langle \Phi^{(1)} | M_m | \Phi^{(1)} \rangle = \langle \Phi^{(2)} | M_m | \Phi^{(2)} \rangle = \langle \Phi^{(3)} | M_m | \Phi^{(3)} \rangle \quad (\text{A.48})$$

not to break coherence between the eigenvectors.

We divide the quantum circuit into seven steps from step (i) to step (vii) as shown in Fig. A.4. We show the detail of how the eigenvectors are transformed after each step.

First, we prepare a three-qubit input state

$$|\Phi^{(i)}\rangle_{1,3}|0\rangle_2 \quad (\text{A.49})$$

in step (i), where we denote the index of the qubit corresponding to the first horizontal wire as 1 and that of the others likewise. After applying Hadamard gates in step (ii), we obtain

$$H_1 H_3 |\Phi^{(i)}\rangle_{1,3} |+\rangle_2, \quad (\text{A.50})$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. After applying $C_{1,3;2}$ in step (iii), we obtain

$$\frac{1}{\sqrt{2}} (H_1 H_3 |\Phi^{(i)}\rangle_{1,3} |0\rangle_2 + Z_1 H_1 Z_3 H_3 |\Phi^{(i)}\rangle_{1,3} |1\rangle_2). \quad (\text{A.51})$$

After applying Hadamard gates and Pauli X operations in step (iv), we obtain

$$\frac{1}{\sqrt{2}} (X_1 X_3 |\Phi^{(i)}\rangle_{1,3} |+\rangle_2 + |\Phi^{(i)}\rangle_{1,3} |-\rangle_2) = \begin{cases} |\Phi^{(i)}\rangle_{1,3} |0\rangle_2 & (i = 0, 2) \\ -|\Phi^{(i)}\rangle_{1,3} |1\rangle_2 & (i = 1, 3). \end{cases} \quad (\text{A.53})$$

After applying $C'_{1,3;2}$ in step (v), we obtain

$$\begin{cases} e^{i(-y+z)} |\Phi^{(0)}\rangle_{1,3} |0\rangle_2 \\ i e^{i(y+z)} |\Phi^{(1)}\rangle_{1,3} |1\rangle_2 \\ e^{i(y-z)} |\Phi^{(2)}\rangle_{1,3} |0\rangle_2 \\ i e^{i(-y-z)} |\Phi^{(3)}\rangle_{1,3} |1\rangle_2. \end{cases} \quad (\text{A.54a})$$

After applying a single qubit unitary operation $u(x)$ given by

$$u(x) = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{ix} & -i e^{-ix} \\ e^{ix} & i e^{-ix} \end{pmatrix} \quad (\text{A.55})$$

in step (vi), we obtain

$$\begin{cases} e^{i(x-y+z)} |\Phi^{(0)}\rangle_{1,3} |+\rangle_2 \\ e^{i(-x+y+z)} |\Phi^{(1)}\rangle_{1,3} |-\rangle_2 \\ e^{i(x+y-z)} |\Phi^{(2)}\rangle_{1,3} |+\rangle_2 \\ e^{i(-x-y-z)} |\Phi^{(3)}\rangle_{1,3} |-\rangle_2. \end{cases} \quad (\text{A.56a})$$

After applying the projective measurement in the computational basis and conditional unitary operations in step (vii), we obtain

$$\begin{cases} e^{i(x-y+z)} |\Phi^{(0)}\rangle_{1,3} = \lambda_0 |\Phi^{(0)}\rangle_{1,3} \\ e^{i(-x+y+z)} |\Phi^{(1)}\rangle_{1,3} = \lambda_1 |\Phi^{(1)}\rangle_{1,3} \\ e^{i(x+y-z)} |\Phi^{(2)}\rangle_{1,3} = \lambda_2 |\Phi^{(2)}\rangle_{1,3} \\ e^{i(-x-y-z)} |\Phi^{(3)}\rangle_{1,3} = \lambda_3 |\Phi^{(3)}\rangle_{1,3}. \end{cases} \quad (\text{A.57a})$$

for any measurement outcome. We can verify that the probability of obtaining a measurement outcome is $\frac{1}{2}$ irrespective of eigenvectors.

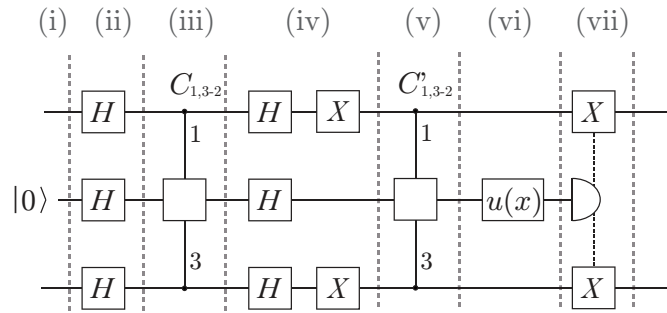


Figure A.4: A protocol to implement a two-qubit unitary operation $U_{global}(x, y, z)$ over the butterfly network. We consider 7 steps presented in the quantum circuit and denote the steps by Roman numerals, (i) to (vii). The symbols of gates of the circuit are same as the ones given for Fig. 4.5.

A.7 Analysis of four qubit states

We prove that there is no pure state of four qubits $|\Phi\rangle_{1,2,3,4}$ satisfying

$$\text{Sch}\#_{1,2}^{3,4}(|\Phi\rangle) = 4, \tag{A.58}$$

$$\text{Sch}\#_{2,4}^{1,3}(|\Phi\rangle) = 2, \tag{A.59}$$

$$\text{Sch}\#_{2,3}^{1,4}(|\Phi\rangle) = 2. \tag{A.60}$$

In [108], it is shown that any pure states of four qubits can, up to permutations of the qubits, be transformed into one of the following nine families of states by

determinant 1 SLOCC:

$$\begin{aligned}
|\Phi_1\rangle &= \frac{a+d}{2}(|0000\rangle + |1111\rangle) + \frac{a-d}{2}(|0011\rangle + |1100\rangle) \\
&\quad + \frac{b+c}{2}(|0101\rangle + |1010\rangle) + \frac{b-c}{2}(|0110\rangle + |1001\rangle) \\
|\Phi_2\rangle &= \frac{a+b}{2}(|0000\rangle + |1111\rangle) + \frac{a-b}{2}(|0011\rangle + |1100\rangle) \\
&\quad + c(|0101\rangle + |1010\rangle) + |0110\rangle \\
|\Phi_3\rangle &= a(|0000\rangle + |1111\rangle) + b(|0101\rangle + |1010\rangle) \\
&\quad + |0110\rangle + |0011\rangle \\
|\Phi_4\rangle &= a(|0000\rangle + |1111\rangle) + \frac{a+b}{2}(|0101\rangle + |1010\rangle) \\
&\quad + \frac{a-b}{2}(|0110\rangle + |1001\rangle) \\
&\quad + \frac{i}{\sqrt{2}}(|0001\rangle + |0010\rangle + |0111\rangle + |1011\rangle) \\
|\Phi_5\rangle &= a(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle) \\
&\quad + i|0001\rangle + |0110\rangle - i|1011\rangle \\
|\Phi_6\rangle &= a(|0000\rangle + |1111\rangle) + |0011\rangle + |0101\rangle + |0110\rangle \\
|\Phi_7\rangle &= |0000\rangle + |0101\rangle + |1000\rangle + |1110\rangle \\
|\Phi_8\rangle &= |0000\rangle + |1011\rangle + |1101\rangle + |1110\rangle \\
|\Phi_9\rangle &= |0000\rangle + |0111\rangle,
\end{aligned}$$

where a, b, c, d are complex parameters.

Since the Schmidt number of a state cannot be increased under SLOCC and determinant 1 SLOCC is invertible, the Schmidt number of a state is invariant under determinant 1 SLOCC. Thus, we show that no state of the nine families simultaneously satisfies Eqs. (A.58)-(A.60). There are three ways to divide four qubits into a pair of two qubits. We denote the set of Schmidt numbers of a four qubit state $|\Phi\rangle$ for all separations as $\text{Sch}\#(|\Phi\rangle) = \{\text{Sch}\#_{1,2}^{3,4}(|\Phi\rangle), \text{Sch}\#_{2,4}^{1,3}(|\Phi\rangle), \text{Sch}\#_{2,3}^{1,4}(|\Phi\rangle)\}$.

Theorem 6. *There is no four qubit state $|\Phi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4$ such that*

$$\text{Sch}\#(|\Phi\rangle) = \{4, 2, 2\}. \quad (\text{A.61})$$

Proof. By straightforward calculation, we can easily check that

$$\text{Sch}\#(|\Phi_6\rangle) = \{n_6, n_6, n_6\} \quad (\text{A.62})$$

$$\text{Sch}\#(|\Phi_7\rangle) = \{3, 3, 3\} \quad (\text{A.63})$$

$$\text{Sch}\#(|\Phi_8\rangle) = \{3, 3, 3\} \quad (\text{A.64})$$

$$\text{Sch}\#(|\Phi_9\rangle) = \{2, 2, 2\}, \quad (\text{A.65})$$

where $n_6 = \# \left\{ \sqrt{2}, \frac{1}{2} \sqrt{1+4|a|^2} + \frac{1}{2}, \frac{1}{2} \sqrt{1+4|a|^2} - \frac{1}{2} \right\}$ and $\#\mathcal{S}$ is the number of non-zero elements of set \mathcal{S} . Since $n_6 = 2$ or $n_6 = 3$, these four states do not satisfy Eq. (A.61).

An element of $\text{Sch}\#(|\Phi_5\rangle)$ is $\# \{1, \sqrt{2}, 2|a|\}$. To satisfy Eq. (A.61), $a = 0$ is required. Then

$$\text{Sch}\#(|\Phi_5\rangle) = \{2, 3, 3\}, \quad (\text{A.66})$$

which does not satisfy Eq. (A.61).

An element of $\text{Sch}\#(|\Phi_4\rangle)$ is $\#\{|b|\} + \#\{x|x^3 - (3|a|^2 + 2)x^2 + (3|a|^4 + 2|a|^2 + 1)x - |a|^6 = 0\}$. To satisfy Eq. (A.61), the element must be 2 or 4. If the element is 2, since $\#\{x|x^3 - (3|a|^2 + 2)x^2 + (3|a|^4 + 2|a|^2 + 1)x - |a|^6 = 0\}$ is larger than 1 and is 2 if and only if $a = 0$, we have

$$a = b = 0. \quad (\text{A.67})$$

Then $\text{Sch}\#(|\Phi_4\rangle) = \{2, 2, 2\}$. Thus, the element must be 4. Since $\#\{x|x^3 - (3|a|^2 + 2)x^2 + (3|a|^4 + 2|a|^2 + 1)x - |a|^6 = 0\}$ is 3 if and only if $a \neq 0$, we have

$$a \neq 0, b \neq 0. \quad (\text{A.68})$$

Another element of $\text{Sch}\#(|\Phi_4\rangle)$ is $\#\{|a-b|\} + \#\{x|64x^3 + (\dots)x^2 + (\dots)x - |a-b|^4|3a+b|^2 = 0\}$, where we abbreviate coefficients of x^2 and x . Since this element must be 2, it is necessary that

$$a - b = 0 \text{ or } 3a + b = 0. \quad (\text{A.69})$$

The other element of $\text{Sch}\#(|\Phi_4\rangle)$ is $\#\{|a+b|\} + \#\{x|64x^3 + (\dots)x^2 + (\dots)x - |a+b|^4|3a-b|^2 = 0\}$, where we abbreviate coefficients of x^2 and x . Since this element must be 2, it is necessary that

$$a + b = 0 \text{ or } 3a - b = 0. \quad (\text{A.70})$$

We can easily check that it is impossible to simultaneously satisfy Eqs. (A.68)-(A.70).

$\text{Sch}\#(|\Phi_3\rangle)$ is $\{n_3, n'_3, n'_3\}$, where

$$n_3 = \#\{\sqrt{2}, |a+b|, |a-b|\}, \quad (\text{A.71})$$

$$n'_3 = \#\{\sqrt{1+4|a|^2} \pm 1, \sqrt{1+4|b|^2} \pm 1\}. \quad (\text{A.72})$$

To satisfy Eq. (A.61), n'_3 must be 2, that is $a = b = 0$. Then $n_3 = 1$, which does not satisfy Eq. (A.61).

$\text{Sch}\#(|\Phi_2\rangle)$ is $\{n_2, n'_2, n''_2\}$, where

$$n_2 = \#\{|a|, |b|, \sqrt{1+4|c|^2} \pm 1\}, \quad (\text{A.73})$$

$$n'_2 = \#\{|a+b \pm 2c|, \sqrt{1+|a-b|^2} \pm 1\}, \quad (\text{A.74})$$

$$n''_2 = \#\{|a-b \pm 2c|, \sqrt{1+|a+b|^2} \pm 1\}. \quad (\text{A.75})$$

In the following, we verify that $\{n_2, n'_2, n''_2\}$ cannot be $\{4, 2, 2\}$, $\{2, 4, 2\}$ or $\{2, 2, 4\}$.

1. $\{n_2, n'_2, n''_2\} \neq \{4, 2, 2\}$:

If $n_2 = 4$, it is necessary that

$$a \neq 0, \quad b \neq 0, \quad c \neq 0. \quad (\text{A.76})$$

If $n'_2 = 2$, it is necessary that

$$a - b = a + b + 2c = 0, \quad (\text{A.77})$$

$$a - b = a + b - 2c = 0, \quad (\text{A.78})$$

$$\text{or } a + b - 2c = a + b + 2c = 0. \quad (\text{A.79})$$

If $n''_2 = 2$, it is necessary that

$$a + b = a - b + 2c = 0, \quad (\text{A.80})$$

$$a + b = a - b - 2c = 0, \quad (\text{A.81})$$

$$\text{or } a - b - 2c = a - b + 2c = 0. \quad (\text{A.82})$$

We can easily check that it is impossible to simultaneously satisfy Eqs. (A.76)-(A.82).

2. $\{n_2, n'_2, n''_2\} \neq \{2, 4, 2\}$:

If $n_2 = 2$, it is necessary that

$$a = b = 0, \quad (\text{A.83})$$

$$a = c = 0, \quad (\text{A.84})$$

$$\text{or } b = c = 0. \quad (\text{A.85})$$

With the necessary condition for $n''_2 = 2$, we obtain that

$$a = b = c = 0. \quad (\text{A.86})$$

Then, it is impossible to satisfy $n'_2 = 4$.

3. $\{n_2, n'_2, n''_2\} \neq \{2, 2, 4\}$:

If $n_2 = 2$, it is necessary that

$$a = b = 0, \quad (\text{A.87})$$

$$a = c = 0, \quad (\text{A.88})$$

$$\text{or } b = c = 0. \quad (\text{A.89})$$

With the necessary condition for $n'_2 = 2$, we obtain that

$$a = b = c = 0. \quad (\text{A.90})$$

Then, it is impossible to satisfy $n''_2 = 4$.

Finally, we analyze $\text{Sch}\#(|\Phi_1\rangle)$. $\text{Sch}\#(|\Phi_1\rangle)$ is $\{n_1, n'_1, n''_1\}$, where

$$n_1 = \#\{|a|, |b|, |c|, |d|\}, \quad (\text{A.91})$$

$$n'_1 = \#\{|a+b-c-d|, |a-b+c-d|, \\ |-a+b+c-d|, |a+b+c+d|\}, \quad (\text{A.92})$$

$$n''_1 = \#\{|-a+b+c+d|, |a-b+c+d|, \\ |a+b-c+d|, |a+b+c-d|\}. \quad (\text{A.93})$$

Note that n_1 , n'_1 and n''_1 are invariant under permutation of a , b , c and d . We verify that $\{n_1, n'_1, n''_1\}$ cannot be $\{4, 2, 2\}$, $\{2, 4, 2\}$ or $\{2, 2, 4\}$ in the following.

1. $\{n_1, n'_1, n''_1\} \neq \{4, 2, 2\}$:

If $n_1 = 4$, it is necessary that

$$a \neq 0, \quad b \neq 0, \quad c \neq 0, \quad d \neq 0. \quad (\text{A.94})$$

If $n'_1 = 2$, it is necessary that in general

$$a + b - c - d = 0, \quad a - b + c - d = 0 \quad (\text{A.95})$$

$$\Leftrightarrow a = d, \quad b = c. \quad (\text{A.96})$$

Then

$$n''_1 = \#\{|2b|, |2a|, |2a|, |2b|\} = 4. \quad (\text{A.97})$$

2. $\{n_1, n'_1, n''_1\} \neq \{2, 4, 2\}$ and $\{n_1, n'_1, n''_1\} \neq \{2, 2, 4\}$:

If $n_1 = 2$, it is necessary that in general

$$a = 0, \quad b = 0, \quad c \neq 0, \quad d \neq 0. \quad (\text{A.98})$$

Then

$$n'_1 = n''_1 = \#\{|c+d|, |c+d|, |c-d|, |c-d|\}. \quad (\text{A.99})$$

□

Appendix B

Role of entanglement and causal relation in DQC

B.1 Entanglement for one-way LOCC

Theorem 5. For any orthonormal basis $\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \subset \mathcal{H}_A \otimes \mathcal{H}_B$,

$$r_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right) = d_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right),$$

where $d_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right)$ is defined by

$$d_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right) := \min_{\mathcal{H}_A = \bigoplus_k \mathcal{M}_k} \max_k \left\{ \dim \mathcal{M}_k \mid \forall j, \exists k, \text{ s.t. } |\psi_j\rangle_{AB} \in \mathcal{M}_k \otimes \mathcal{H}_B \right\}.$$

Proof. First, we prove the inequality

$$r_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right) \leq d_{min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right). \quad (\text{B.1})$$

Suppose there exists an orthogonal decomposition $\mathcal{H}_A = \bigoplus_{k=1}^K \mathcal{M}_k$ such that for all j , there exists k satisfying $|\psi_j\rangle_{AB} \in \mathcal{M}_k \otimes \mathcal{H}_B$. Then, the following protocol discriminates any basis states in $\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B}$ perfectly:

1. Alice applies a measurement $\{P_k\}_{k=1}^K$ on her system ($\mathcal{H}_{AA'}$), and sends outcome k to Bob who has system \mathcal{H}_B , where P_k is the orthogonal projector onto the subspace \mathcal{M}_k .

2. Alice teleports the subspace \mathcal{M}_k to Bob by using a maximally entangled state $|\Phi\rangle_{A'B'} \in \mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$ whose Schmidt rank is given by $\text{Sch}\#_{B'}^{A'}(|\Phi\rangle_{A'B'}) = \max_k \left\{ \dim \mathcal{M}_k \mid \forall j, \exists k, \text{ s.t. } |\psi_j\rangle_{AB} \in \mathcal{M}_k \otimes \mathcal{H}_B \right\}$.
3. Bob discriminates the states $|\psi_j\rangle_{B'B} \in \mathcal{M}_k \otimes \mathcal{H}_B$ which is now on his subspace.

The existence of this protocol guarantees the inequality given by (B.1).

Second, we prove the inequality

$$r_{\min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right) \geq d_{\min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right). \quad (\text{B.2})$$

Suppose $|\Phi\rangle_{A'B'}$ attains the optimum defined by Eq. (6.2). That is, a set of states $\{|\psi_j\rangle_{AB} \otimes |\Phi\rangle_{A'B'}\}_{j=1}^{d_A d_B} \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ can be perfectly discriminated by one-way LOCC, and

$$r_{\min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right) = \text{Sch}\#_{B'}^{A'}(|\Phi\rangle_{A'B'}). \quad (\text{B.3})$$

Then, without loss of generality, we assume that all Alice's POVM elements are rank one. That is, Alice first applies the POVM represented by $\{|\xi_x\rangle\langle\xi_x|_{AA'}\}$ on her system $\mathcal{H}_{AA'}$, where $|\xi_x\rangle_{AA'}$ is an unnormalized state on $\mathcal{H}_{AA'}$. We define an unnormalized state $|\tilde{\psi}_{jx}\rangle_{AA'BB'} \in \mathcal{H}_{AA'} \otimes \mathcal{H}_{BB'}$ as a unnormalized state on the total system when the initial unknown state is denoted by $|\psi_j\rangle_{AB}$, and Alice applies the POVM and obtains outcome x , namely,

$$|\tilde{\psi}_{jx}\rangle_{A,B,A',B'} := (|\xi_x\rangle\langle\xi_x|_{AA'} \otimes I_{BB'}) |\psi_j\rangle_{A,B} \otimes |\Phi\rangle_{A'B'} \quad (\text{B.4})$$

Since Bob can discriminate any state from the set of states, $\langle\tilde{\psi}_{jx}|\tilde{\psi}_{j'x}\rangle = \mu_j \delta_{jj'}$ holds for all j and j' , where $\mu_j \geq 0$ for all j . This can be rewritten as

$$\langle\psi_j|S_x \otimes Id_B|\psi_{j'}\rangle = \mu_j \delta_{jj'}, \quad (\text{B.5})$$

by introducing a positive operator S_x on \mathcal{H}_A defined as

$$S_x := \sum_{k=1}^{\min(d_{A'}, d_{B'})} \lambda_k^2 \langle e_k|_{A'} (|\xi_x\rangle\langle\xi_x|_{AA'}) |e_k\rangle_{A'}, \quad (\text{B.6})$$

where $\{\lambda_k\}_{k=1}^{\min(d_{A'}, d_{B'})}$ and $\{|e_k\rangle_{A'} \otimes |f_{k'}\rangle_{B'}\}_{k=1, k'=1}^{d_{A'}, d_{B'}}$ are the Schmidt coefficients and the Schmidt basis of $|\Phi\rangle_{A'B'}$, respectively, thus $|\Phi\rangle_{A'B'} = \sum_k \lambda_k |e_k\rangle_{A'} \otimes |f_k\rangle_{B'}$. Eq. (B.6) clearly shows

$$\text{Sch}\#_{B'}^{A'}(|\Phi\rangle_{A'B'}) \geq \max_x \text{rank } S_x. \quad (\text{B.7})$$

On the other hand, by using Eq. (B.5), we derive

$$\sum_{j'} |\psi_{j'}\rangle \langle \psi_{j'} | S_x \otimes I_B | \psi_j \rangle = \sum_{j'} \mu_j \delta_{jj'} |\psi_{j'}\rangle \quad (\text{B.8})$$

$$\Leftrightarrow S_x \otimes I_B | \psi_j \rangle = \mu_j | \psi_j \rangle. \quad (\text{B.9})$$

This equation implies that $\{|\psi_j\rangle\}_{j=1}^{d_A d_B}$ is a simultaneous eigenbasis for a set of positive operators $\{S_x \otimes I_B\}_x$ on $\mathcal{H}_A \otimes \mathcal{H}_B$. In other words, a set $\{S_x \otimes I_B\}_x$ is commutative, i.e. $[S_x \otimes I_B, S_{x'} \otimes I_B] = 0$. Thus a set $\{S_x\}_x$ is commutative as well, $[S_x, S_{x'}] = 0$. Hence there exists a set of projectors $\{P_l^{(x)}\}_{l,x}$ satisfying

$$\forall x, \forall x', \forall l, \forall l', [P_l^{(x)}, P_{l'}^{(x')}] = 0 \quad (\text{B.10})$$

such that for all x ,

$$S_x = \sum_l \theta_l^{(x)} P_l^{(x)}$$

gives a spectral decomposition of S_x , and $\theta_l^{(x)} \neq \theta_{l'}^{(x)}$ for $l \neq l'$. That is, for all x ,

$$S_x \otimes I_B = \sum_l \theta_l^{(x)} P_l^{(x)} \otimes I_B \quad (\text{B.11})$$

gives a spectral decomposition of S_x . Eqs. (B.9), (B.10), and (B.11) lead to the existence of a set of projectors $\{Q_h\}_h$ on \mathcal{H}_A satisfying $Q_h Q_{h'} = \delta_{hh'} Q_h$, $\sum_h Q_h = I_A$, and

$$\forall h, \forall j, Q_h \otimes I_B | \psi_j \rangle = 0 \text{ or } | \psi_j \rangle,$$

and there exists a set of non-negative numbers $\{\theta_h'^{(x)}\}_{h,x}$ such that

$$\begin{aligned} \forall x, S_x &= \sum_h \theta_h'^{(x)} Q_h, \\ \forall h, \exists x, \theta_h'^{(x)} &> 0 \end{aligned} \quad (\text{B.12})$$

Therefore, by defining a subspace \mathcal{M}_h as the support of Q_h , $\{\mathcal{M}_h\}_h$ satisfies $\mathcal{H}_A = \bigoplus_h \mathcal{M}_h$ and for all j , there exists h such that $|\psi_j\rangle \in \mathcal{M}_h \otimes \mathcal{H}_B$. Hence, we derive

$$\max_x \text{rank} S_x \geq \max_h \text{rank} Q_h = \max_h \dim \mathcal{M}_h \geq d_{\min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right), \quad (\text{B.13})$$

where Eq. (B.12) leads to the first inequality, the definition of \mathcal{M}_h implies the equality, and the definition of $d_{\min} \left(\{|\psi_j\rangle_{AB}\}_{j=1}^{d_A d_B} \right)$ guarantees the last inequality. Finally, Eqs. (B.3), (B.7), and (B.13) implies the inequality given by (B.2).

Now, we have proven inequalities (B.1) and (B.2). This completes the proof of the theorem. \square

B.2 LOCC and causal order

We analyze the relationship between LOCC and special relativistic causal order of local operations performed in the spacetime by generalizing a LOCC scenario in a special relativistic framework. In this scenario, suppose Alice and Bob reside in separate laboratories in spacetime obeying special relativity. They perform local operations within each laboratory for N times. Each local operation is assumed to be implemented in a very short time so that it is performed at a single spacetime coordinate. We assume that the order of local operations in each laboratory is fixed. However, we do not require to fix the total ordering of local operations across the two parties in contrast to the standard LOCC scenario.

We denote the k -th local operations of Alice and Bob are represented by $\mathcal{A}_{o_k|i_k}^{(k)}$ and $\mathcal{B}_{o'_k|i'_k}^{(k)}$. In this generalized scenario, Alice (Bob) receives classical input i_k (i'_k) from outside her (his) laboratory and performs $\mathcal{A}_{o_k|i_k}^{(k)}$ ($\mathcal{B}_{o'_k|i'_k}^{(k)}$) and then sends classical output o_k (o'_k) to outside her (his) laboratory. The deterministic joint quantum operation in this case can be written in the form of Eq.(7.4) by means of $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ linking the classical outputs and the classical inputs of the local operations.

The assumption of special relativity adds two conditions for linking two local operations. An ordering denoted by “ \prec ” over local operations associated by the spacetime coordinates is introduced to represent these conditions. We define $a \prec b$ if the spacetime coordinate of operation a is in the past light cone of the spacetime coordinate of operation b . If neither $a \prec b$ nor $b \prec a$ holds then the spacetime coordinates of a and b are *spacelike* separated. Special relativity guarantees that this ordering is a partial ordering. Thus, there exists a partial ordering “ \prec ” over a set of local quantum operations. Since local operations within each laboratory are totally ordered by the assumption, the partial ordering must satisfy $\mathcal{A}_{o_1|i_1}^{(1)} \prec \dots \prec \mathcal{A}_{o_N|i_N}^{(N)}$ and $\mathcal{B}_{o'_1|i'_1}^{(1)} \prec \dots \prec \mathcal{B}_{o'_N|i'_N}^{(N)}$. Further, $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ must satisfy the no-signaling condition. That is, for all local operations, an output of a local operation cannot depend on the input of another local operation performed not in the past. For example, if $\mathcal{B}_{o'_l|i'_l}^{(l)} \prec \mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{B}_{o'_m|i'_m}^{(m)}$, then

$$\begin{aligned} & p(i_1, \dots, i_k, i'_1, \dots, i'_l | o_1, \dots, o_N, o'_1, \dots, o'_N) \\ &= p(i_1, \dots, i_k, i'_1, \dots, i'_l | o_1, \dots, o_{k-1}, o'_1, \dots, o'_{m-1}) \end{aligned} \quad (\text{B.14})$$

should be satisfied.

We can show that deterministic joint quantum operations is in LOCC if and only if it has a decomposition in Eq.(4), and there exists a partial ordering over local quantum operations and $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ in Eq.(7.4) satisfies the no-signaling condition with respect to the partial ordering. The proof of this statement

is slightly involved and given in Appendix B.3. This property of deterministic joint quantum operations in the form of Eq.(7.4) suggests that LOCC is a set of all possible deterministic joint quantum operations implementable by local operations and *classical communication respecting causal order*.

B.3 The rigorous proof of B.2

In Results, we presented a statement that any deterministic joint quantum operation in LOCC can be written in the form of Eq.(7.4) but not all quantum operations written as Eq.(7.4) are LOCC. In this section, we show a necessary and sufficient condition for a deterministic joint quantum operation in the form of Eq.(7.4) to be in LOCC. We show that the condition is related to special relativistic *causal order* of local operations.

We regard $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ in Eq.(7.4) linking the outputs and inputs of local operations as classical channel between $2N$ inputs $\{o_k\}_{k=1}^N \cup \{o'_k\}_{k=1}^N$ and $2N$ outputs $\{i_k\}_{k=1}^N \cup \{i'_k\}_{k=1}^N$. Note that an input i_k for a local operation $\mathcal{A}_{o_k|i_k}^{(k)}$ is an output of the classical channel. Suppose there exists a strict partial ordering “ \prec ” on the set of local operations $\{\mathcal{A}_{o_k|i_k}^{(k)}\}_{k=1}^N \cup \{\mathcal{B}_{o_k|i_k}^{(k)}\}_{k=1}^N$, where “strict” means that neither $\mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{A}_{o_k|i_k}^{(k)}$ nor $\mathcal{B}_{o_k|i_k}^{(k)} \prec \mathcal{B}_{o_k|i_k}^{(k)}$ holds, and $\{\mathcal{A}_{o_k|i_k}^{(k)}\}_{k=1}^N$ and $\{\mathcal{B}_{o_k|i_k}^{(k)}\}_{k=1}^N$ are local operations performed in the laboratories of Alice and Bob, respectively. Each local operation is assumed to be implemented in a very short time so that it is performed at a single spacetime coordinate and is associated with the spacetime coordinate. We assume the order of local operations in each laboratory is fixed and local operations are performed in the increasing order of k , which is the assumption of local temporal ordering we have introduced in Appendix B.2.

Suppose that this partial ordering \prec represents causal order of the spacetime coordinates of local operations. For example, $\mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{B}_{o'_l|i'_l}^{(l)}$ means that $\mathcal{B}_{o'_l|i'_l}^{(l)}$ is performed after $\mathcal{A}_{o_k|i_k}^{(k)}$ had been performed. Neither $\mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{B}_{o'_l|i'_l}^{(l)}$ nor $\mathcal{B}_{o'_l|i'_l}^{(l)} \prec \mathcal{A}_{o_k|i_k}^{(k)}$ holds if the spacetime coordinates of $\mathcal{A}_{o_k|i_k}^{(k)}$ and $\mathcal{B}_{o'_l|i'_l}^{(l)}$ are spacelike separated. Due to the assumption of local temporal ordering, $\mathcal{A}_{o_{k+1}|i_{k+1}}^{(k)}$ is performed after $\mathcal{A}_{o_k|i_k}^{(k)}$, thus “ \prec ” satisfies $\mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{A}_{o_{k+1}|i_{k+1}}^{(k)}$ for all $k = 1, \dots, N-1$. Similarly, it satisfies $\mathcal{B}_{o'_k|i'_k}^{(k)} \prec \mathcal{B}_{o'_{k+1}|i'_{k+1}}^{(k)}$ for all $k = 1, \dots, N-1$.

We define a set *past*(\mathfrak{J}) representing a set of all “*past*” inputs for a set of outputs \mathfrak{J} , where \mathfrak{J} is a subset of $\{i_k\}_{k=1}^N \cup \{i'_k\}_{k=1}^N$. Formally, by introducing a set of local operations $Op(\mathfrak{J})$ corresponding to \mathfrak{J} as

$$Op(\mathfrak{J}) := \left\{ \mathcal{A}_{o_k|i_k}^{(k)} \mid i_k \in \mathfrak{J} \right\} \cup \left\{ \mathcal{B}_{o'_k|i'_k}^{(k)} \mid i'_k \in \mathfrak{J} \right\}, \quad (\text{B.15})$$

$\text{past}(\mathfrak{J})$ is defined as

$$\text{past}(\mathfrak{J}) := \{o_k | \exists \chi \in \text{Op}(\mathfrak{J}), \mathcal{A}_{o_k|i_k}^{(k)} \prec \chi\} \cup \{o'_k | \exists \chi \in \text{Op}(\mathfrak{J}), \mathcal{B}_{o'_k|i'_k}^{(k)} \prec \chi\}, \quad (\text{B.16})$$

where χ represent any element of $\text{Op}(\mathfrak{J})$, that is, there exists l such that $\chi = \mathcal{A}_{o_l|i_l}^{(l)}$ or $\chi = \mathcal{B}_{o'_l|i'_l}^{(l)}$. Note that o_k is not in $\text{past}(\{i_k\})$ by definition.

Next we define a classical channel respecting the causal order. A classical channel $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ linking the classical outputs and inputs of local operations $\{\mathcal{A}_{o_k|i_k}^{(k)}\}_{k=1}^N \cup \{\mathcal{B}_{o'_k|i'_k}^{(k)}\}_{k=1}^N$ is said to be respecting causal order if there exists a partial ordering \prec on the set of local operations $\{\mathcal{A}_{o_k|i_k}^{(k)}\}_{k=1}^N \cup \{\mathcal{B}_{o'_k|i'_k}^{(k)}\}_{k=1}^N$ satisfying the following conditions:

- For all k , $\mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{A}_{o_{k+1}|i_{k+1}}^{(k)}$ and $\mathcal{B}_{o'_k|i'_k}^{(k)} \prec \mathcal{B}_{o'_{k+1}|i'_{k+1}}^{(k)}$.
- For all k and l ,

$$\begin{aligned} & p(i_1, \dots, i_k, i'_1, \dots, i'_l | o_1, \dots, o_N, o'_1, \dots, o'_N) \\ &= p(i_1, \dots, i_k, i'_1, \dots, i'_l | \text{past}(\{i_a\}_{a=1}^k \cup \{i'_b\}_{b=1}^l)). \end{aligned} \quad (\text{B.17})$$

Since the classical channel is represented by a conditional probability distribution,

$$\begin{aligned} & p(i_1, \dots, i_k, i'_1, \dots, i'_l | o_1, \dots, o_N, o'_1, \dots, o'_N) \\ &= \sum_{i_{k+1}, \dots, i_N, i'_{l+1}, \dots, i'_N} p(i_1, \dots, i_N, i'_1, \dots, i'_N | o_1, \dots, o_N, o'_1, \dots, o'_N) \end{aligned} \quad (\text{B.18})$$

holds. Hence Eq.(B.17) can be regarded to represent the no-signaling condition among multiple spacetime coordinates, namely, outputs of the classical channel never depend on the inputs that are not in the past of the outputs. In other words, classical communication represented by a classical channel respects causal order if and only if there exists a partial ordering among local operations and the classical channel satisfies the no-signaling condition with respect to the partial ordering.

We present the main proposition on the relationship between LOCC and causal order.

Proposition 3. *A deterministic joint quantum operation is in LOCC, if and only if it has a decomposition in the form of Eq.(7.4) with $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ respecting the causal order.*

From the proposition, we immediately derive the following corollary about LOCC*.

Corollary 1. *A deterministic joint quantum operation is in LOCC* and not in LOCC, if and only if it has a decomposition in the form of Eq.(7.4) with $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ and for all such decompositions, $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ does not respect causal order.*

Since the proposition is a necessary and sufficient condition for LOCC, it gives a new characterization of LOCC in terms of $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ and similarly, the corollary gives a new characterization of a deterministic joint quantum operation in LOCC* and not in LOCC, which is nothing but a non-LOCC separable quantum operation as we have shown in Results, in terms of causal order.

Proof

We provide a proof of the main proposition in the remaining part of this section. Since the conventional definition of LOCC in Eq.(7.2) using the totally ordered local operations immediately gives a decomposition with $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ respecting causal order, the “only if” part is trivial. Hence we concentrate on proving the “if” part of the proposition.

This proof consists of two parts. In Part A, we show that for given local operations $\{\mathcal{A}_{o_k|i_k}^{(k)}\}_{k=1}^N \cup \{\mathcal{B}_{o_k|i_k}^{(k)}\}_{k=1}^N$ and classical channel $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ representing a deterministic joint quantum operation by Eq. (7.4), it is always possible to construct sets of *totally* ordered local operations $\left\{\mathcal{C}_{\mathbb{O}_{f(k,0)}|\mathbb{J}_{f(k,0)}}^{(k)}\right\}_{k=1}^N$ and $\left\{\mathcal{D}_{\mathbb{O}_{f(k,1)}|\mathbb{J}_{f(k,1)}}^{(k)}\right\}_{k=1}^N$, where an input \mathbb{J}_l of a local operation depends only on an output \mathbb{O}_{l-1} of the previous local operation, representing the deterministic joint quantum operation by choosing an appropriate classical channel. In Part B, we show that another pair of sets of totally ordered local operations $\left\{\mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{J}_{f(k,0)}}^{(k)}\right\}_{k=1}^N$ and $\left\{\mathcal{D}'_{\mathbb{O}_{f(k,1)}|\mathbb{J}_{f(k,1)}}^{(k)}\right\}_{k=1}^N$ from the local operations and the classical channel constructed in Part A. The standard form of LOCC given by Eq. (7.2) is derived by using this pair of sets of totally ordered local operations.

Part A

Since there always exists a total ordering which preserves the structure of a given partial ordering on a finite set, we define a map f satisfying

- f is a bijection from $\{1, \dots, N\} \times \{0, 1\}$ to $\{1, \dots, 2N\}$.
- $f(k, b) < f(k+1, b)$ for all k and b .
- $\mathcal{A}_{o_k|i_k}^{(k)} \prec \mathcal{B}_{o'_l|i'_l}^{(l)} \Rightarrow f(k, 0) < f(l, 1)$, and $\mathcal{B}_{o'_k|i'_k}^{(k)} \prec \mathcal{A}_{o_l|i_l}^{(l)} \Rightarrow f(k, 1) < f(l, 0)$ for all k and l .

By means of f , we define a set of classical inputs $\{I_l\}_{l=1}^{2N}$ and a set of outputs $\{O_l\}_{l=1}^{2N}$ of which elements are given by

$$I_{f(k,0)} = i_k, \quad I_{f(k,1)} = i'_k, \quad O_{f(k,0)} = o_k, \quad \text{and} \quad O_{f(k,1)} = o'_k \quad (\text{B.19})$$

for all k . We further define a conditional probability distribution $q(I_1, \dots, I_{2N} | O_1, \dots, O_{2N})$ by

$$q(I_1, \dots, I_{2N} | O_1, \dots, O_{2N}) := p(i_1, \dots, i_N, i'_1, \dots, i'_N | o_1, \dots, o_N, o'_1, \dots, o'_N), \quad (\text{B.20})$$

where I_l and O_l are related to i_k , i'_k , o_k , and o'_k by Eq. (B.19). Thus $q(\dots | \dots)$ is another representation of $p(\dots | \dots)$ in terms of the newly defined classical inputs and outputs $\{I_l\}_{l=1}^{2N}$ and $\{O_l\}_{l=1}^{2N}$. Using $q(I_1, \dots, I_{2N} | O_1, \dots, O_{2N})$, the condition for $p(i_1, \dots, i'_N | o_1, \dots, o'_N)$ to respect causal order given by Eq.(B.17) for all k and l is expressed by

$$q(I_1, \dots, I_k | O_1, \dots, O_{2N}) = q(I_1, \dots, I_k | O_1, \dots, O_{k-1}) \quad (\text{B.21})$$

for all k .

Next, we define sets of all possible values of I_k and O_k denoted by \mathcal{I}_k and \mathcal{O}_k , respectively, for $k = 1, \dots, 2N$. We represent variables whose variations are over $\prod_{j=1}^k \mathcal{I}_j \times \prod_{j=1}^{k-1} \mathcal{O}_j$ and $\prod_{j=1}^k \mathcal{I}_j \times \prod_{j=1}^k \mathcal{O}_j$ by \mathbb{J}_k and \mathbb{O}_k , respectively. $\{\mathbb{J}_k\}_{k=1}^{2N}$ and $\{\mathbb{O}_k\}_{k=1}^{2N}$ are classical inputs and outputs of new local operations which will be introduced latter. We define a function $Q(\mathbb{J}_k | \mathbb{O}_{k-1})$ representing a classical channel linking between \mathbb{J}_k and \mathbb{O}_{k-1} as

$$Q(\mathbb{J}_k | \mathbb{O}_{k-1}) := \frac{q(I_1, \dots, I_k | O_1, \dots, O_{k-1})}{q(I_1, \dots, I_{k-1} | O_1, \dots, O_{k-2})} \cdot \delta(\mathbb{J}_k[1, k-1], \mathbb{O}_{k-1}[1, k-1]) \\ \cdot \delta(\mathbb{J}_k[k+1, 2k-1], \mathbb{O}_{k-1}[k, 2k-2]), \quad (2 \leq k \leq 2N) \quad (\text{B.22})$$

$$Q(\mathbb{J}_1) := q(I_1), \quad (\text{B.23})$$

where $\delta(x, y)$ is the Kronecker delta, $\mathbb{J}_k = (I_1, \dots, I_k, O_1, \dots, O_{k-1})$ for $2 \leq k \leq 2N$, $\mathbb{J}_1 = I_1$, and $\mathbb{J}_k[l, m]$ is a vector consisting of the partial entries of \mathbb{J}_k , from the l -th entry through the m -th entry for $l < m$.

It is easy to check that $Q(\mathbb{J}_k | \mathbb{O}_{k-1})$ satisfies

$$\sum_{\mathbb{J}_1, \dots, \mathbb{J}_{2N}} Q(\mathbb{J}_1) \cdot \delta(\mathbb{J}_1, \mathbb{O}_1[1]) \prod_{k=2}^{2N} Q(\mathbb{J}_k | \mathbb{O}_{k-1}) \cdot \delta(\mathbb{J}_k, \mathbb{O}_k[1, 2k-1]) \\ = q(I_1^{(2N)}, \dots, I_{2N}^{(2N)} | O_1^{(2N)}, \dots, O_{2N}^{(2N)}) \\ \prod_{k=2}^{2N} \delta\left((I_1^{(k)}, \dots, I_{k-1}^{(k)}, O_1^{(k)}, \dots, O_{k-1}^{(k)}), (I_1^{(k-1)}, \dots, I_{k-1}^{(k-1)}, O_1^{(k-1)}, \dots, O_{k-1}^{(k-1)})\right), \quad (\text{B.24})$$

where $I_l^{(k)}$ and $O_l^{(k)}$ are given by $\mathbb{O}_k = (I_1^{(k)}, \dots, I_k^{(k)}, O_1^{(k)}, \dots, O_k^{(k)})$, and $\mathbb{O}_k[l]$ denotes the l -th entry of \mathbb{O}_k . Eq. (B.24) indicates that $Q(\mathbb{J}_1) \prod_{k=2}^{2N} Q(\mathbb{J}_k | \mathbb{O}_{k-1})$ and $q(I_1^{(2N)}, \dots, I_{2N}^{(2N)} | O_1^{(2N)}, \dots, O_{2N}^{(2N)})$ represent the same classical channel if $\mathbb{J}_k = \mathbb{O}_k[1, k-1]$, $\mathbb{O}_k[1, k-1] = \mathbb{O}_{k-1}[1, k-1]$, and $\mathbb{O}_k[k+1, 2k] = \mathbb{O}_{k-1}[k, 2k-2]$ are satisfied.

We define a local operation performed in Alice's laboratory for $\mathbb{J}_{f(k,0)}$ and $\mathbb{O}_{f(k,0)}$ denoted by $\mathcal{C}_{\mathbb{O}_{f(k,0)} | \mathbb{J}_{f(k,0)}}^{(k)}$ as

$$\mathcal{C}_{\mathbb{O}_{f(k,0)} | \mathbb{J}_{f(k,0)}}^{(k)} := \delta(\mathbb{J}_{f(k,0)}, \mathbb{O}_{f(k,0)}[1, 2f(k,0) - 1]) \cdot \mathcal{A}_{\mathbb{O}_{f(k,0)}[2f(k,0)] | \mathbb{J}_{f(k,0)}[f(k,0)]}^{(k)}, \quad (\text{B.25})$$

where $\mathbb{O}_1[1, 1] := \mathbb{O}_1[1]$ for $f(k,0) = 1$ and $\mathbb{J}_k[l]$ represents the l -th entry of \mathbb{J}_k . Similarly, we define a local operation performed in Bob's laboratory denoted by $\mathcal{D}_{\mathbb{O}_{f(k,1)} | \mathbb{J}_{f(k,1)}}^{(k)}$ as

$$\mathcal{D}_{\mathbb{O}_{f(k,1)} | \mathbb{J}_{f(k,1)}}^{(k)} := \delta(\mathbb{J}_{f(k,1)}, \mathbb{O}_{f(k,1)}[1, 2f(k,1) - 1]) \cdot \mathcal{B}_{\mathbb{O}_{f(k,1)}[2f(k,1)] | \mathbb{J}_{f(k,1)}[f(k,1)]}^{(k)}. \quad (\text{B.26})$$

By linking classical outputs and inputs of local operations $\mathcal{C}_{\mathbb{O}_{f(k,0)} | \mathbb{J}_{f(k,0)}}^{(k)}$ and $\mathcal{D}_{\mathbb{O}_{f(k,1)} | \mathbb{J}_{f(k,1)}}^{(k)}$ respecting the total ordering introduced by the function f , we derive a representation of the deterministic joint quantum operation given by Eq. (7.4)

as follows:

$$\begin{aligned}
& \sum_{\mathbb{J}_1, \dots, \mathbb{J}_{2N}, \mathbb{O}_1, \dots, \mathbb{O}_{2N}} Q(\mathbb{J}_1) \cdot \left(\prod_{k=2}^{2N} Q(\mathbb{J}_k | \mathbb{O}_{k-1}) \right) \mathcal{C}_{\mathbb{O}_{f(N,0)} | \mathbb{J}_{f(N,0)}}^{(N)} \circ \dots \circ \mathcal{C}_{\mathbb{O}_{f(1,0)} | \mathbb{J}_{f(1,0)}}^{(1)} \\
& \otimes \mathcal{D}_{\mathbb{O}_{f(N,1)} | \mathbb{J}_{f(N,1)}}^{(N)} \circ \dots \circ \mathcal{D}_{\mathbb{O}_{f(1,1)} | \mathbb{J}_{f(1,1)}}^{(1)} \\
= & \sum_{\mathbb{J}_1, \dots, \mathbb{J}_{2N}, \mathbb{O}_1, \dots, \mathbb{O}_{2N}} Q(\mathbb{J}_1) \cdot \delta(\mathbb{J}_1 | \mathbb{O}_1[1]) \cdot \left(\prod_{k=2}^{2N} Q(\mathbb{J}_k | \mathbb{O}_{k-1}) \cdot \delta(\mathbb{J}_k, \mathbb{O}_k[1, 2k-1]) \right) \\
& \mathcal{A}_{\mathbb{O}_{f(N,0)}[2f(N,0)] | \mathbb{J}_{f(N,0)}[f(N,0)]}^{(N)} \circ \dots \circ \mathcal{A}_{\mathbb{O}_{f(1,0)}[2f(1,0)] | \mathbb{J}_{f(1,0)}[f(1,0)]}^{(1)} \\
& \otimes \mathcal{B}_{\mathbb{O}_{f(N,1)}[2f(N,1)] | \mathbb{J}_{f(N,1)}[f(N,1)]}^{(N)} \circ \dots \circ \mathcal{B}_{\mathbb{O}_{f(1,1)}[2f(1,1)] | \mathbb{J}_{f(1,1)}[f(1,1)]}^{(1)} \\
= & \sum_{\mathbb{O}_1, \dots, \mathbb{O}_{2N}} q(I_1^{(2N)}, \dots, I_{2N}^{(2N)} | O_1^{(2N)}, \dots, O_{2N}^{(2N)}) \cdot \\
& \prod_{k=2}^{2N} \delta\left((I_1^{(k)}, \dots, I_{k-1}^{(k)}, O_1^{(k)}, \dots, O_{k-1}^{(k)}), (I_1^{(k-1)}, \dots, I_{k-1}^{(k-1)}, O_1^{(k-1)}, \dots, O_{k-1}^{(k-1)}) \right), \\
& \mathcal{A}_{\mathbb{O}_{f(N,0)}[2f(N,0)] | \mathbb{O}_{f(N,0)}[f(N,0)]}^{(N)} \circ \dots \circ \mathcal{A}_{\mathbb{O}_{f(1,0)}[2f(1,0)] | \mathbb{O}_{f(1,0)}[f(1,0)]}^{(1)} \\
& \otimes \mathcal{B}_{\mathbb{O}_{f(N,1)}[2f(N,1)] | \mathbb{O}_{f(N,1)}[f(N,1)]}^{(N)} \circ \dots \circ \mathcal{B}_{\mathbb{O}_{f(1,1)}[2f(1,1)] | \mathbb{O}_{f(1,1)}[f(1,1)]}^{(1)} \\
= & \sum_{\mathbb{O}_{2N}} q(I_1^{(2N)}, \dots, I_{2N}^{(2N)} | O_1^{(2N)}, \dots, O_{2N}^{(2N)}) \cdot \\
& \mathcal{A}_{\mathbb{O}_{2N}[N+f(N,0)] | \mathbb{O}_{2N}[f(N,0)]}^{(N)} \circ \dots \circ \mathcal{A}_{\mathbb{O}_{2N}[N+f(1,0)] | \mathbb{O}_{2N}[f(1,0)]}^{(1)} \\
& \otimes \mathcal{B}_{\mathbb{O}_{2N}[N+f(N,1)] | \mathbb{O}_{2N}[f(N,1)]}^{(N)} \circ \dots \circ \mathcal{B}_{\mathbb{O}_{2N}[N+f(1,1)] | \mathbb{O}_{2N}[f(1,1)]}^{(1)} \\
= & \sum_{i_1, \dots, i_N, i'_1, \dots, i'_N, o_1, \dots, o_N, o'_1, \dots, o'_N} p(i_1, \dots, i_N, i'_1, \dots, i'_N | o_1, \dots, o_N, o'_1, \dots, o'_N) \\
& \mathcal{A}_{o_N | i_N}^{(N)} \circ \dots \circ \mathcal{A}_{o_1 | i_1}^{(1)} \otimes \mathcal{B}_{o'_N | i'_N}^{(N)} \circ \dots \circ \mathcal{B}_{o'_1 | i'_1}^{(1)}, \tag{B.27}
\end{aligned}$$

where we used Eqs. (B.25) and (B.26) in the first equality, Eqs. (B.22) and (B.23) in the second equality, Eq. (B.20) in the fourth equality, respectively. Note that in the first line of Eq. (B.27), classical input \mathbb{J}_k of a local operation only depends on classical output \mathbb{O}_{k-1} of the previous local operation in $Q(\mathbb{J}_k | \mathbb{O}_{k-1})$.

Part B

In this part, we define new local operations performed in Alice's and Bob's laboratories denoted by $\mathcal{C}_{\mathbb{O}_{f(k,0)} | \mathbb{O}_{f(k,0)-1}}^{(k)}$ and $\mathcal{D}_{\mathbb{O}_{f(k,1)} | \mathbb{O}_{f(k,1)-1}}^{(k)}$, respectively, and show that the first line of Eq. (B.27) can be transformed to the standard form of LOCC

using these local operations. We define $\mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)}$ and $\mathcal{D}'_{\mathbb{O}_{f(k,1)}|\mathbb{O}_{f(k,1)-1}}^{(k)}$ as

$$\begin{aligned}\mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)} &:= \sum_{\mathbb{J}_{f(k,0)}} Q(\mathbb{J}_{f(k,0)}|\mathbb{O}_{f(k,0)-1})\mathcal{C}_{\mathbb{O}_{f(k,0)}|\mathbb{J}_{f(k,0)}}^{(k)}, \\ \mathcal{D}'_{\mathbb{O}_{f(k,1)}|\mathbb{O}_{f(k,1)-1}}^{(k)} &:= \sum_{\mathbb{J}_{f(k,1)}} Q(\mathbb{J}_{f(k,1)}|\mathbb{O}_{f(k,1)-1})\mathcal{C}_{\mathbb{O}_{f(k,1)}|\mathbb{J}_{f(k,1)}}^{(k)},\end{aligned}\quad (\text{B.28})$$

where we have used $Q(\mathbb{J}_1|\mathbb{O}_0) := Q(\mathbb{J}_1)$. By means of Eqs. (B.22) and (B.23), we obtain a relation

$$\sum_{\mathbb{O}_{f(k,0)}} \mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)} = \sum_{I_{f(k,0)}, O_{f(k,0)}} \frac{q(I_1, \dots, I_{f(k,0)}|O_1, \dots, O_{f(k,0)-1})}{q(I_1, \dots, I_{f(k,0)-1}|O_1, \dots, O_{f(k,0)-2})} \mathcal{A}_{O_{f(k,0)}|(I_{f(k,0)})}^{(k)}, \quad (\text{B.29})$$

where $I_{f(N,0)}$ and $O_{f(N,0)}$ are the $f(N,0)$ -th and $2f(N,0)$ -th entries of $\mathbb{O}_{f(N,0)}$, respectively, and $\{I_l\}_{l=1}^{f(k,0)-1}$ and $\{O_l\}_{l=1}^{f(k,0)-1}$ are given by

$$\mathbb{O}_{f(k,0)-1} = (I_1, \dots, I_{f(k,0)-1}|O_1, \dots, O_{f(k,0)-1}).$$

Eq. (B.21) represents the property of $q(I_1, \dots, I_{2N}|O_1, \dots, O_{2N})$ respecting causal order and Eq. (B.29) guarantees that $\{\mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)}\}_{\mathbb{O}_{f(k,0)}}$ is indeed a quantum instrument for all k . Similarly, $\{\mathcal{D}'_{\mathbb{O}_{f(k,1)}|\mathbb{O}_{f(k,1)-1}}^{(k)}\}_{\mathbb{O}_{f(k,1)}}$ is also shown to be a quantum instrument for all k .

Now the deterministic joint quantum operation given in the form of Eq. (7.4) can be represented in terms of quantum instruments $\{\mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)}\}_{\mathbb{O}_{f(k,0)}}$ and $\{\mathcal{D}'_{\mathbb{O}_{f(k,1)}|\mathbb{O}_{f(k,1)-1}}^{(k)}\}_{\mathbb{O}_{f(k,1)}}$ as

$$\begin{aligned}& \sum_{i_1, \dots, i_N, i'_1, \dots, i'_N, o_1, \dots, o_N, o'_1, \dots, o'_N} p(i_1, \dots, i_N, i'_1, \dots, i'_N|o_1, \dots, o_N, o'_1, \dots, o'_N) \\ & \mathcal{A}_{o_N|i_N}^{(N)} \circ \dots \circ \mathcal{A}_{o_1|i_1}^{(1)} \otimes \mathcal{B}_{o'_N|i'_N}^{(N)} \circ \dots \circ \mathcal{B}_{o'_1|i'_1}^{(1)}, \\ = & \sum_{\mathbb{O}_1, \dots, \mathbb{O}_{2N}} \mathcal{C}'_{\mathbb{O}_{f(N,0)}|\mathbb{O}_{f(N,0)-1}}^{(N)} \circ \dots \circ \mathcal{C}'_{\mathbb{O}_{f(1,0)}|\mathbb{O}_{f(1,0)-1}}^{(1)} \otimes \mathcal{D}'_{\mathbb{O}_{f(N,1)}|\mathbb{O}_{f(N,1)-1}}^{(N)} \circ \dots \circ \mathcal{D}'_{\mathbb{O}_{f(1,1)}|\mathbb{O}_{f(1,1)-1}}^{(1)}.\end{aligned}\quad (\text{B.30})$$

by using Eq. (B.28). The right hand side of Eq. (B.30) is almost in the standard form of LOCC. The only case of Eq. (B.30) not fitting in LOCC is the case that Alice (Bob) successively performs two local operations. This case is absorbed in LOCC in the following manner. Suppose Alice successively performs two local

operations $\mathcal{C}'_{\mathbb{O}_{f(k-1,0)}|\mathbb{O}_{f(k-1,0)-1}}^{(k-1)}$ and $\mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)}$ where $f(k, 0) = f(k-1, 0) + 1$. Since

$$\left\{ \sum_{\mathbb{O}_{f(k-1,0)}} \mathcal{C}'_{\mathbb{O}_{f(k,0)}|\mathbb{O}_{f(k,0)-1}}^{(k)} \circ \mathcal{C}'_{\mathbb{O}_{f(k-1,0)}|\mathbb{O}_{f(k-1,0)-1}}^{(k-1)} \right\}_{\mathbb{O}_{f(k,0)}}$$

is a quantum instrument representing a local operation performed in Alice's laboratory, we regard these successive local operations as a single local operation performed in Alice's laboratory. Similarly, we combine successive local operations performed in Bob's laboratory as a single local operation. By repeating this procedure, we can rewrite in the standard form of LOCC, where a sequence of local operations are performed alternatively in Alice's and Bob's laboratories. Hence, we can conclude that Eq.(B.30) reduces to a standard decomposition of LOCC given in the form of Eq.(7.2). Therefore, the "if" part of the proposition is proven.

B.4 Formal mathematical formulation of LOCC*

We denote the Hilbert spaces of the systems of Alice's quantum input and Bob's quantum input as \mathcal{H}_X and \mathcal{H}_Y , respectively, and those of Alice's quantum output and Bob's quantum output as \mathcal{H}_A and \mathcal{H}_B , respectively. Since LOCC* is defined as a set of CPTP maps $\mathcal{M} : \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_Y) \rightarrow \mathbf{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ satisfying Eq.(7.5), LOCC* is represented by a set of CPTP maps in the CJ representation $M \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A \otimes \mathcal{H}_Y \otimes \mathcal{H}_B)$ as

$$M = \sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) A_{o_A | i_A} \otimes B_{o_B | i_B}, \quad (\text{B.31})$$

where i_A and i_B are classical inputs of Alice and Bob, respectively, and o_A and o_B are classical outputs of Alice and Bob respectively, and $p(i_A, i_B | o_A, o_B)$ is a conditional probability distribution, $A_{o_A | i_A} \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A)$ is the CJ operator of Alice's local operation and $B_{o_B | i_B} \in \mathbf{L}(\mathcal{H}_Y \otimes \mathcal{H}_B)$ is the CJ operator of the Bob's local operation. Note that these CJ operators must satisfy

$$\forall i_A, \forall o_A, A_{o_A | i_A} \geq 0, \quad (\text{B.32})$$

$$\forall i_A, \text{tr}_A \left[\sum_{o_A} A_{o_A | i_A} \right] = \mathbb{I}_X, \quad (\text{B.33})$$

$$\forall i_B, \forall o_B, B_{o_B | i_B} \geq 0, \quad (\text{B.34})$$

$$\forall i_B, \text{tr}_B \left[\sum_{o_B} B_{o_B | i_B} \right] = \mathbb{I}_Y. \quad (\text{B.35})$$

By taking a special conditional probability distribution given by $p(i_A, i_B | o_A, o_B) = \delta_{i_A, o_A} \delta_{i_B, o_B}$ in Eq.(B.31), the set of CPTP maps $M \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A \otimes \mathcal{H}_Y \otimes \mathcal{H}_B)$ satisfying

$$M = \sum_{a,b} A_{a|b} \otimes B_{b|a} \quad (\text{B.36})$$

is easily shown to be in a subset of LOCC*. We shall show the converse that any element of LOCC* can be decomposed into this form. For a given conditional probability distribution $p(i_A, i_B | o_A, o_B)$, let local operations of Alice and Bob be

$$A_{i_B, x | o_A, o_B} := \sum_{i_A} p(i_A, i_B | o_A, o_B) A_{x | i_A} \quad (\text{B.37})$$

$$B_{o_A, o_B | i_B, x} := \delta_{o_A}^{(x)} B_{o_B | i_B}, \quad (\text{B.38})$$

by introducing a new index x . Since these newly introduced operators $A_{i_B, x | o_A, o_B}$ and $B_{o_A, o_B | i_B, x}$ satisfy

$$\forall o_A, \forall o_B, \text{tr}_A \left[\sum_{i_B, x} A_{i_B, x | o_A, o_B} \right] = \mathbb{I}_X, \quad \forall i_B, \forall x, \text{tr}_B \left[\sum_{o_A, o_B} B_{o_A, o_B | i_B, x} \right] = \mathbb{I}_Y, \quad (\text{B.39})$$

they are elements of valid local operations. By using these local operations, we have

$$\sum_{i_B, x, o_A, o_B} A_{i_B, x | o_A, o_B} \otimes B_{o_A, o_B | i_B, x} = \sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) A_{o_A | i_A} \otimes B_{o_B | i_B}. \quad (\text{B.40})$$

Further introducing new classical indices $a := (i_B, x)$ and $b := (o_A, o_B)$, we obtain the form of Eq.(B.36) where $A_{a|b} \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A)$ and $B_{b|a} \in \mathbf{L}(\mathcal{H}_Y \otimes \mathcal{H}_B)$ satisfy

$$\forall b, \forall a, A_{a|b} \geq 0 \quad (\text{B.41})$$

$$\forall a, \text{tr}_A \left[\sum_a A_{a|b} \right] = \mathbb{I}_X \quad (\text{B.42})$$

$$\forall a, \forall b, B_{b|a} \geq 0 \quad (\text{B.43})$$

$$\forall a, \text{tr}_B \left[\sum_b B_{b|a} \right] = \mathbb{I}_Y. \quad (\text{B.44})$$

B.5 Equivalence of LOCC* and SEP

For a deterministic joint quantum operation $\mathcal{M} : \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_Y) \rightarrow \mathbf{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ in SEP defined by Eq.(7.9), the corresponding CJ operator $M \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A \otimes \mathcal{H}_Y \otimes \mathcal{H}_B)$ is given by

$$M = \sum_{k=1}^L E_k^A \otimes E_k^B, \quad (\text{B.45})$$

where $E_k^A \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A)$ and $E_k^B \in \mathbf{L}(\mathcal{H}_Y \otimes \mathcal{H}_B)$ satisfy

$$E_k^A \geq 0, \quad E_k^B \geq 0, \quad (\text{B.46})$$

for all k . It is easy to see that LOCC* represented by Eq.(B.36) is a subset of SEP. We shall show the converse that it is possible to construct local operators $A_{a|b} \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_A)$ and $B_{b|a} \in \mathbf{L}(\mathcal{H}_Y \otimes \mathcal{H}_B)$ LOCC* for any given SEP element.

First we show that we can restrict SEP operators to

$$\text{tr}_A [E_k^A] \leq \mathbb{I}_X, \quad \text{tr}_B [E_k^B] \leq \mathbb{I}_Y, \quad (\text{B.47})$$

for all k in addition to Eq.(B.46) without loss of generality. Since the CJ operator M defined by Eq. (B.87) is TP and SEP operators are positive, we obtain

$$\forall k, \text{tr}_{AB} [E_k^A \otimes E_k^B] = \text{tr}_A [E_k^A] \otimes \text{tr}_B [E_k^B] \leq \mathbb{I}_{XY}. \quad (\text{B.48})$$

Since $\text{tr}_A [E_k^A]$ and $\text{tr}_B [E_k^B]$ are positive, they are diagonalizable. Let the eigenvalues of $\text{tr}_A [E_k^A]$ and $\text{tr}_B [E_k^B]$ be $\{\lambda_i^A\}$ and $\{\lambda_j^B\}$, respectively. Eq.(B.48) implies

$$\max_i \{\lambda_i^A\} \max_j \{\lambda_j^B\} \leq 1. \quad (\text{B.49})$$

If $\max_i \{\lambda_i^A\} \leq 1$ and $\max_j \{\lambda_j^B\} \leq 1$, Eq.(B.89) is satisfied. We assume that $\max_i \{\lambda_i^A\} \geq 1$ and define

$$\tilde{E}_k^A = \frac{1}{\max_i \{\lambda_i^A\}} E_k^A, \quad \tilde{E}_k^B = \max_i \{\lambda_i^A\} E_k^B. \quad (\text{B.50})$$

Due to $\tilde{E}_k^A \otimes \tilde{E}_k^B = E_k^A \otimes E_k^B$, SEP operators E_k^A and E_k^B can be replaced by \tilde{E}_k^A and \tilde{E}_k^B . Then the validity of Eq.(B.89) is certified.

Now we present a construction of local operators for LOCC* as follows.

$$A_{k|k} = E_k^A \quad \text{for } 1 \leq k \leq L \quad (\text{B.51})$$

$$B_{k|k} = E_k^B \quad \text{for } 1 \leq k \leq L \quad (\text{B.52})$$

$$A_{L+1|k} = \frac{1}{\dim(\mathcal{H}_A)} (\mathbb{I}_X - \text{tr}_A [E_k^A]) \otimes \mathbb{I}_A \quad \text{for } 1 \leq k \leq L \quad (\text{B.53})$$

$$B_{L+1|k} = \frac{1}{\dim(\mathcal{H}_B)} (\mathbb{I}_Y - \text{tr}_B [E_k^B]) \otimes \mathbb{I}_B \quad \text{for } 1 \leq k \leq L \quad (\text{B.54})$$

$$A_{a|b} = \frac{1}{\dim(\mathcal{H}_A)} \mathbb{I}_X \otimes \mathbb{I}_A \quad \text{for } b > L, L+2 \leq a \leq L+3 \text{ and } a+b \equiv 1 \pmod{2} \quad (\text{B.55})$$

$$B_{b|a} = \frac{1}{\dim(\mathcal{H}_B)} \mathbb{I}_Y \otimes \mathbb{I}_B \quad \text{for } a > L, L+2 \leq b \leq L+3 \text{ and } a+b \equiv 0 \pmod{2} \quad (\text{B.56})$$

$$A_{a|b} = 0 \quad \text{else,} \quad (\text{B.57})$$

$$B_{b|a} = 0 \quad \text{else.} \quad (\text{B.58})$$

B.6 CC* and classical quantum processes

A quantum process [58] is a higher order map transforming quantum operations to another quantum operation. We analyze the relationship between CC* in LOCC* and classical quantum processes in the higher order formalism using the CJ operator representation. We denote the set of all positive semi-definite operators on a Hilbert space \mathcal{H} as $\mathbf{Pos}(\mathcal{H})$ and the set of all CJ operators on $\mathcal{H}_I \otimes \mathcal{H}_O$ representing CPTP maps from \mathcal{H}_I to \mathcal{H}_O as $CPTP(\mathcal{H}_I : \mathcal{H}_O) = \{Q \in \mathbf{Pos}(\mathcal{H}_I \otimes \mathcal{H}_O) | \text{tr}_O Q = \mathbb{I}_I\}$.

To be consistent with quantum mechanics, it has been proven in [58] that a quantum process linking two local operations represented by the CJ operators $M_A \in \mathbf{L}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{O_A})$ and $M_B \in \mathbf{L}(\mathcal{H}_{I_B} \otimes \mathcal{H}_{O_B})$ as inputs can be represented by a positive semi-definite operator $W \in \mathbf{Pos}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_{I_B} \otimes \mathcal{H}_{O_B})$ called a *process matrix* satisfying

$$\forall M_A \in CPTP(\mathcal{H}_{I_A} : \mathcal{H}_{O_A}), \forall M_B \in CPTP(\mathcal{H}_{I_B} : \mathcal{H}_{O_B}), \text{tr}[W(M_A^T \otimes M_B^T)] = 1, \quad (\text{B.59})$$

where Q^T represents the transposition of Q with respect to the computational basis used in defining the CJ representation.

A deterministic joint quantum operation $\mathcal{M} : \mathbf{L}(\mathcal{H}_X \otimes \mathcal{M}_Y) \rightarrow \mathbf{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ can be regarded to be obtained by transforming two local operations $\mathcal{A} : \mathbf{L}(\mathcal{H}_{I_A} \otimes \mathcal{H}_X) \rightarrow \mathbf{L}(\mathcal{H}_{O_A} \otimes \mathcal{H}_A)$ and $\mathcal{B} : \mathbf{L}(\mathcal{H}_{I_B} \otimes \mathcal{H}_Y) \rightarrow \mathbf{L}(\mathcal{H}_{O_B} \otimes \mathcal{H}_B)$ by a quantum

process $W \in \mathbf{Pos}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_{I_B} \otimes \mathcal{H}_{O_B})$ linking the Hilbert spaces \mathcal{H}_{I_A} , \mathcal{H}_{O_A} , \mathcal{H}_{I_B} and \mathcal{H}_{O_B} . The CJ operator $M \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_A \otimes \mathcal{H}_B)$ of \mathcal{M} obtained by transforming the CJ operators of local operations $A \in \mathbf{L}(\mathcal{H}_{I_A} \otimes \mathcal{H}_X \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_A)$ and $B \in \mathbf{L}(\mathcal{H}_{I_B} \otimes \mathcal{H}_Y \otimes \mathcal{H}_{O_B} \otimes \mathcal{H}_B)$ corresponding to \mathcal{A} and \mathcal{B} , respectively, by W satisfying Eq.(B.59) is represented by

$$M = \text{tr}_{I_A, O_A, I_B, O_B} [W(A^{\text{T}_{I_A, O_A}} \otimes B^{\text{T}_{I_B, O_B}})], \quad (\text{B.60})$$

where $Q^{\text{T}_{I_X, O_X}}$ is the partial transposition of Q , taking the transposition only in terms of \mathcal{H}_{I_X} and \mathcal{H}_{O_X} .

Quantum communication from Alice to Bob or Bob to Alice can be described by W if W is equivalent to the CJ operator representing a quantum channel linking two causally ordered local operations belonging to different parties. Moreover, quantum processes can represent “quantum communication” without causal order, which is not implementable when the partial order of local operations is fixed but is not ruled out in the framework of quantum mechanics [58]. The restriction for quantum processes given by Eq. (B.59) can be interpreted to represent a new kind of causality required for linking local operations in quantum mechanics.

We consider a special class of quantum process where Alice and Bob can communicate only by “classical” states, namely, the states on the Hilbert spaces of W (\mathcal{H}_{I_A} , \mathcal{H}_{O_A} , \mathcal{H}_{I_B} and \mathcal{H}_{O_B}) are restricted to be diagonal with respect to the computational basis. In such a case, *classical* quantum processes representing classical communication between the parties can be described by a conditional probability distribution $p(i_A, i_B | o_A, o_B)$ satisfying

$$\sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) A_{o_A | i_A} \otimes B_{o_B | i_B} \in \text{CPTP}(\mathcal{H}_X \otimes \mathcal{H}_Y : \mathcal{H}_A \otimes \mathcal{H}_B) \quad (\text{B.61})$$

for all quantum instruments $\{A_{o_A | i_A}\}_{o_A}$ and $\{B_{o_B | i_B}\}_{o_B}$, where $\{A_{o_A | i_A} \in \mathbf{Pos}(\mathcal{H}_X \otimes \mathcal{H}_A)\}_{o_A}$ and $\{B_{o_B | i_B} \in \mathbf{Pos}(\mathcal{H}_Y \otimes \mathcal{H}_B)\}_{o_B}$ satisfying $\sum_{o_A} \text{tr}_A[A_{o_A | i_A}] = \mathbb{I}_X$ and $\sum_{o_B} \text{tr}_B[B_{o_B | i_B}] = \mathbb{I}_Y$. The proof is given in Appendix B.7.

A deterministic joint quantum operation \mathcal{M} implementable by a classical quantum process connecting two local operations is given in the form of

$$\mathcal{M} = \sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) \mathcal{A}_{o_A | i_A} \otimes \mathcal{B}_{o_B | i_B}, \quad (\text{B.62})$$

where $p(i_A, i_B | o_A, o_B)$ is a conditional probability distribution satisfying Eq.(B.61). We refer to the set of such joint quantum operations as LOCQP. By definition, LOCC* is a larger set than LOCQP since the condition for $p(i_A, i_B | o_A, o_B)$ given by Eq.(B.61) should be satisfied for *all* local operations in LOCQP while it should be satisfied only for *some* local operations in LOCC*. In Appendix B.7, we prove

that LOCQP is equivalent to a probability mixture of one-way LOCC in a bipartite scenario. Thus, CC* used in implementing a deterministic joint quantum computation in LOCC* but not in LOCC cannot be represented by a classical quantum process. This indicates that the required causal property for classical communication linking local operations is weakened for CC* comparing to the special relativistic causality and also to the restriction for classical quantum processes.

B.7 CQP and LOCC

This section consists of two parts. In Part A, we give a rigorous definition of a classical quantum process (CQP) and show a correspondence between a CQP and a conditional probability distribution. In Part B, we show that a set of joint quantum operations consisting local operations and CQP (LOCQP) is equivalent to a set of probabilistic mixture of one-way LOCC in bipartite cases

Part A

A *classical quantum process* represents a link of local operations for a situation that Alice and Bob can communicate only by “classical” states. In this case, the states on the local input and output Hilbert spaces \mathcal{H}_{I_A} , \mathcal{H}_{O_A} , \mathcal{H}_{I_B} and \mathcal{H}_{O_B} of a process matrix W are restricted to be diagonal with respect to the computational basis. By denoting the computational basis of \mathcal{H}_X as $\{|x\rangle_X\}$, local operations $M_A \in CPTP(\mathcal{H}_{I_A} : \mathcal{H}_{O_A})$, $M_B \in CPTP(\mathcal{H}_{I_B} : \mathcal{H}_{O_B})$, and a classical quantum process described by a diagonal process matrix $W \in \mathbf{Pos}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_{I_B} \otimes \mathcal{H}_{O_B})$ can be decomposed into

$$M_A = \sum_{i_A, o_A} p_A(o_A|i_A) |i_A, o_A\rangle \langle i_A, o_A|_{I_A, O_A}, \quad (\text{B.63})$$

$$M_B = \sum_{i_B, o_B} p_B(o_B|i_B) |i_B, o_B\rangle \langle i_B, o_B|_{I_B, O_B}, \quad (\text{B.64})$$

$$W = \sum_{i_A, o_A, i_B, o_B} w(i_A, i_B, o_A, o_B) |i_A\rangle \langle i_A|_{I_A} \otimes |i_B\rangle \langle i_B|_{I_B} \otimes |o_A\rangle \langle o_A|_{O_A} \otimes |o_B\rangle \langle o_B|_{O_B}, \quad (\text{B.65})$$

where $w(i_A, i_B, o_A, o_B)$ represents a diagonal element of W , and $p_A(o_A|i_A)$ and $p_B(o_B|i_B)$ are conditional probability distributions since M_A and M_B are CPTP maps. In the following, we show that classical quantum processes correspond to conditional probability distributions, namely, $w(i_A, i_B, o_A, o_B)$ must be a conditional probability distribution so that Eq. (B.59) holds. The non-negativity of W implies $w(i_A, i_B, o_A, o_B) \geq 0$ and the condition given by Eq. (B.59) is equivalent

to

$$\sum_{i_A, i_B, o_A, o_B} w(i_A, i_B, o_A, o_B) p_A(o_A|i_A) p_B(o_B|i_B) = 1 \quad (\text{B.66})$$

for all conditional probability distributions $p_A(o_A|i_A)$ and $p_B(o_B|i_B)$. By choosing $p_A(o_A|i_A) = \delta_{o_A, a}$ and $p_B(o_B|i_B) = \delta_{o_B, b}$, we obtain $\sum_{i_A, i_B} w(i_A, i_B, a, b) = 1$ for arbitrary a and b . Thus $w(i_A, i_B, o_A, o_B)$ can be represented by a conditional probability distribution conditioned by o_A and o_B and we define

$$p(i_A, i_B|o_A, o_B) := w(i_A, i_B, o_A, o_B). \quad (\text{B.67})$$

Next, we define a set of deterministic joint quantum operations consisting of local operations linked by a classical quantum process, denoted by LOCC**. Local operations $A \in \text{CPTP}(\mathcal{H}_{I_A} \otimes \mathcal{H}_X : \mathcal{H}_{O_A} \otimes \mathcal{H}_A)$ and $B \in \text{CPTP}(\mathcal{H}_{I_B} \otimes \mathcal{H}_Y : \mathcal{H}_{O_B} \otimes \mathcal{H}_B)$ linked by a diagonal process matrix $W \in \mathbf{Pos}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{I_B} \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_{O_B})$ given in the form of Eq. (B.65) can be decomposed into

$$A = \sum_{i_A, o_A} A_{o_A|i_A} \otimes |i_A, o_A\rangle\langle i_A, o_A|_{I_A, O_A}, \quad (\text{B.68})$$

$$B = \sum_{i_B, o_B} B_{o_B|i_B} \otimes |i_B, o_B\rangle\langle i_B, o_B|_{I_B, O_B}, \quad (\text{B.69})$$

where $\{A_{o_A|i_A} \in \mathbf{Pos}(\mathcal{H}_X \otimes \mathcal{H}_A)\}_{o_A}$ and $\{B_{o_B|i_B} \in \mathbf{Pos}(\mathcal{H}_Y \otimes \mathcal{H}_B)\}_{o_B}$ are the CJ operators of quantum instruments since A and B are CPTP maps. By straightforward calculation, the CJ operator of a deterministic joint quantum operation is written by

$$M = \text{tr}_{I_A, O_A, I_B, O_B} [W(A^{\text{T}_{I_A, O_A}} \otimes B^{\text{T}_{I_B, O_B}})] \quad (\text{B.70})$$

$$= \sum_{i_A, i_B, o_A, o_B} p(i_A, i_B|o_A, o_B) A_{o_A|i_A} \otimes B_{o_B|i_B}, \quad (\text{B.71})$$

which shows the equivalence of the representations of M given by Eq. (B.31) and Eq. (B.60) when the process is diagonal/classical. LOCQP is defined by a set of deterministic joint quantum operations of which CJ operators can be represented by Eq. (B.71), where $p(i_A, i_B|o_A, o_B)$ satisfies

$$\sum_{i_A, i_B, o_A, o_B} p(i_A, i_B|o_A, o_B) p_A(o_A|i_A) p_B(o_B|i_B) = 1 \quad (\text{B.72})$$

for all conditional probability distributions $p_A(o_A|i_A)$ and $p_B(o_B|i_B)$.

Further, the condition given by Eq. (B.72) is equivalent to that of Eq. (B.61) if $p(i_A, i_B|o_A, o_B)$ is a conditional probability distribution. This can be shown as follows. By letting $\dim(\mathcal{H}_X) = \dim(\mathcal{H}_Y) = \dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = 1$,

$A_{o_A|i_A} = p(o_A|i_A)$ and $B_{o_B|i_B} = p(o_B|i_B)$, it is easily checked that Eq. (B.72) holds if Eq. (B.61) holds. To show the converse, we first check that a map decomposable in the form of Eq. (B.61) is completely positive. This is also easily checked since every term in the summation is non-negative. Then we show that a map decomposable in the form of Eq. (B.61) is trace preserving when Eq. (B.72) holds in the following. For any operator $\sigma \in \mathbf{L}(\mathcal{H}_X \otimes \mathcal{H}_Y)$,

$$\mathrm{tr}_{A,B} \left[\mathrm{tr}_{X,Y} \left[\sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) (A_{o_A|i_A} \otimes B_{o_B|i_B}) \sigma^T \right] \right] \quad (\text{B.73})$$

$$= \sum_{k,l} \lambda_{k,l} \sum_{i_A, i_B, o_A, o_B} p(i_A, i_B | o_A, o_B) \mathrm{tr}_{A,X} [A_{o_A|i_A} \rho_k^T] \mathrm{tr}_{B,Y} [B_{o_B|i_B} \rho_l^T] \quad (\text{B.74})$$

$$= \sum_{k,l} \lambda_{k,l} = \mathrm{tr}[\sigma], \quad (\text{B.75})$$

where σ is decomposed as $\sigma = \sum_{k,l} \lambda_{k,l} \rho_k \otimes \rho_l$ by using density operators $\{\rho_k\}_k$ as a basis of the linear space of the operator. Note that $\mathrm{tr}_{A,X} [A_{o_A|i_A} \rho_k^T]$ is a conditional probability distribution conditioned by i_A since it satisfies $\sum_{o_A} \mathrm{tr}_{A,X} [A_{o_A|i_A} \rho_k^T] = \mathrm{tr}_{A,X} [\sum_{o_A} A_{o_A|i_A} \rho_k^T] = \mathrm{tr}_X [\rho_k^T] = 1$.

Part B

We show a proof of the following lemma.

Lemma 5. *LOCQP is equivalent to a probability mixture of one-way LOCC in bipartite cases.*

Proof. In [58], it has been shown that any classical quantum process is *causally separable*, i.e. the CJ operator of a classical quantum process W can be decomposed into the form

$$W = qW_{A \rightarrow B} + (1 - q)W_{B \rightarrow A}, \quad (\text{B.76})$$

where $q \in [0, 1]$, $W_{A \rightarrow B} \in \mathbf{Pos}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_{I_B} \otimes \mathcal{H}_{O_B})$ is diagonal with respect to the computational basis and satisfies the conditions given by

$$W_{A \rightarrow B} = \mathbb{I}_{O_B} \otimes W_{I_A, O_A, I_B}, \quad \mathrm{tr}_{I_B} [W_{I_A, O_A, I_B}] = \mathbb{I}_{O_A} \otimes \rho_{I_A}, \quad \mathrm{tr}_{I_A} [\rho_{I_A}] = 1 \quad (\text{B.77})$$

and the similar conditions are satisfied by $W_{B \rightarrow A} \in \mathbf{Pos}(\mathcal{H}_{I_A} \otimes \mathcal{H}_{O_A} \otimes \mathcal{H}_{I_B} \otimes \mathcal{H}_{O_B})$.

In [59], it has been proven that an operator $W_{A \rightarrow B}$ satisfying the conditions given by Eq. (B.77) but not necessarily being diagonal in the computational basis corresponds to a special type of quantum process called *quantum comb* where Alice's operation and Bob's operation are linked by quantum communication from Alice to Bob. Thus a causally separable process can be interpreted as a probabilistic mixture of quantum communication from Alice to Bob and that from Bob to Alice. When a causally separable process is classical (diagonal with respect to the computational basis), the process can be interpreted as a probabilistic mixture of classical communication from Alice to Bob and that from Bob to Alice.

Let denote the diagonal elements of $W_{A \rightarrow B}$ and $W_{B \rightarrow A}$ with respect to the computational basis by $p_{A \rightarrow B}(i_A, i_B | o_A, o_B)$ and $p_{B \rightarrow A}(i_A, i_B | o_A, o_B)$, respectively. It is easy to verify that $p_{A \rightarrow B}(i_A, i_B | o_A, o_B)$ and $p_{B \rightarrow A}(i_A, i_B | o_A, o_B)$ are conditional probability distributions since $W_{A \rightarrow B}$ and $W_{B \rightarrow A}$ correspond to classical quantum processes.

Then $p(i_A, i_B | o_A, o_B)$ satisfying Eq. (B.61) can be decomposed into

$$p(i_A, i_B | o_A, o_B) = qp_{A \rightarrow B}(i_A, i_B | o_A, o_B) + (1 - q)p_{B \rightarrow A}(i_A, i_B | o_A, o_B). \quad (\text{B.78})$$

Eq. (B.77) implies $p_{A \rightarrow B}(i_A, i_B | o_A, o_B)$ does not depend on o_B . We define $p_{A \rightarrow B}(i_A, i_B | o_A) := p_{A \rightarrow B}(i_A, i_B | o_A, o_B)$. The operator W_{I_A, o_A, I_B} in Eq. (B.77) is given by

$$W_{I_A, o_A, I_B} = \sum_{i_A, i_B, o_A} p_{A \rightarrow B}(i_A, i_B | o_A) |i_A\rangle \langle i_A|_{I_A} \otimes |o_A\rangle \langle o_A|_{o_A} \otimes |i_B\rangle \langle i_B|_{I_B}. \quad (\text{B.79})$$

Due to Eq. (B.77), $\sum_{i_B} p_{A \rightarrow B}(i_A, i_B | o_A)$ does not depend on o_A . We define $p_{A \rightarrow B}(i_A) := \sum_{i_B} p_{A \rightarrow B}(i_A, i_B | o_A)$. We further define a set $X = \{x | p_{A \rightarrow B}(x) \neq 0\}$ and

$$p'_{A \rightarrow B}(i_B | o_A, i_A) := \frac{p_{A \rightarrow B}(i_A, i_B | o_A)}{p_{A \rightarrow B}(i_A)} \quad (i_A \in X) \quad (\text{B.80})$$

$$p'_{A \rightarrow B}(i_B | o_A, i_A) := p'_{A \rightarrow B}(i_B) \quad (i_A \notin X), \quad (\text{B.81})$$

where $p'_{A \rightarrow B}(y)$ is an arbitrary probability distribution. Note that $p'_{A \rightarrow B}(i_B | o_A, i_A)$ satisfies all properties required for a conditional probability distribution. Thus, we have

$$p_{A \rightarrow B}(i_A, i_B | o_A, o_B) = p_{A \rightarrow B}(i_A) p'_{A \rightarrow B}(i_B | o_A, i_A), \quad (\text{B.82})$$

and similarly,

$$p_{B \rightarrow A}(i_A, i_B | o_A, o_B) = p_{B \rightarrow A}(i_B) p'_{B \rightarrow A}(i_A | o_B, i_B). \quad (\text{B.83})$$

Combining these results, a deterministic joint quantum operation \mathcal{M} in LOCQP is given by

$$\begin{aligned} \mathcal{M} &= q \sum_{i_A, i_B, o_A, o_B} p_{A \rightarrow B}(i_A, i_B | o_A, o_B) \mathcal{A}_{o_A | i_A} \otimes \mathcal{B}_{o_B | i_B} \\ &\quad + (1 - q) \sum_{i_A, i_B, o_A, o_B} p_{B \rightarrow A}(i_A, i_B | o_A, o_B) \mathcal{A}_{o_A | i_A} \otimes \mathcal{B}_{o_B | i_B}. \end{aligned} \quad (\text{B.84})$$

Since $\sum_{i_A, i_B, o_A, o_B} p_{A \rightarrow B}(i_A, i_B | o_A, o_B) \mathcal{A}_{o_A | i_A} \otimes \mathcal{B}_{o_B | i_B} = \sum_m \mathcal{A}_m \otimes \mathcal{B}_m$ where

$$m := (i_A, o_A), \quad \mathcal{A}_{i_A, o_A} := p_{A \rightarrow B}(i_A) \mathcal{A}_{o_A | i_A}, \quad \mathcal{B}_{i_A, o_A} := \sum_{i_B, o_B} p'_{A \rightarrow B}(i_B | o_A, i_A) \mathcal{B}_{o_B | i_B} \quad (\text{B.85})$$

represents operations in one-way LOCC, the deterministic joint quantum operation \mathcal{M} in LOCQP is concluded to be a probability mixture of one-way LOCC. \square

B.8 Classical causally non-separable process

We analyze a tripartite case for describing deterministic joint quantum operations. Consider Alice performs a CPTP map $A \in CPTP(\mathcal{H}_1 \otimes \mathcal{H}_7 : \mathcal{H}_2 \otimes \mathcal{H}_8)$, Bob performs a CPTP map $B \in CPTP(\mathcal{H}_3 \otimes \mathcal{H}_9 : \mathcal{H}_4 \otimes \mathcal{H}_{10})$, Charlie performs a CPTP map $C \in CPTP(\mathcal{H}_5 \otimes \mathcal{H}_{11} : \mathcal{H}_6 \otimes \mathcal{H}_{12})$ and spaces \mathcal{H}_i ($7 \leq i \leq 12$) are connected by a process matrix $W \in \mathbf{Pos}(\mathcal{H}_7 \otimes \mathcal{H}_8 \otimes \mathcal{H}_9 \otimes \mathcal{H}_{10} \otimes \mathcal{H}_{11} \otimes \mathcal{H}_{12})$, where $\dim(\mathcal{H}_i) = 2$ ($7 \leq i \leq 12$).

$$W = \frac{1}{8} [\mathbb{I}_{7,8,9,10,11,12} + Z_7 \mathbb{I}_8 \mathbb{I}_9 Z_{10} Z_{11} Z_{12} + Z_7 Z_8 Z_9 \mathbb{I}_{10} \mathbb{I}_{11} Z_{12} + \mathbb{I}_7 Z_8 Z_9 Z_{10} Z_{11} \mathbb{I}_{12}] \quad (\text{B.86})$$

is known to be a classical causally non-separable process matrix [106], where we abbreviate \otimes . This process matrix corresponds to CC^* given in Eq. (7.11).

B.9 Multipartite LOCC*

For a deterministic joint quantum operation \mathcal{M} in SEP, the corresponding CJ operator M is given by

$$M = \sum_{l=1}^L E_l^{(1)} \otimes \cdots \otimes E_l^{(N)}, \quad (\text{B.87})$$

where $E_l^{(n)} \in \mathbf{L}(\mathcal{H}_{I_n} \otimes \mathcal{H}_{O_n})$ satisfies

$$E_l^{(n)} \geq 0, \quad (\text{B.88})$$

for all l and n . It is easy to see that LOCC^* represented by Eq.(8.10) is a subset of SEP. We shall show the converse that it is possible to construct a probability distribution $p(i_1, \dots, i_N | o_1, \dots, o_N)$ and local operators $\{\{E_{o_n | i_n}^{(n)} \in \mathbf{L}(\mathcal{H}_{I_n} \otimes \mathcal{H}_{O_n})\}_{o_n}\}_{n=1}^N$ in LOCC^* for any given SEP element.

Without loss of generality, we can assume that

$$\text{tr}_{O_n} [E_l^{(n)}] \leq \mathbb{I}_{I_n}, \quad (\text{B.89})$$

for all l and n .

Now we present a construction of local operators for LOCC* as follows.

$$p(i_1, \dots, i_N | o_1, \dots, o_N) = \prod_{n=1}^N \delta_{i_n, o_n} \quad (\text{B.90})$$

$$E_{l|l}^{(n)} = E_l^{(n)} \quad \text{for } 1 \leq n \leq N, 1 \leq l \leq L \quad (\text{B.91})$$

$$E_{L+1|l}^{(n)} = \frac{1}{\dim(\mathcal{H}_{O_n})} \left(\mathbb{I}_{I_n} - \text{tr}_{O_n} [E_l^{(n)}] \right) \otimes \mathbb{I}_{O_n} \\ \text{for } 1 \leq n \leq N, 1 \leq l \leq L+1 \quad (\text{B.92})$$

$$E_{1|L+1}^{(n)} = \frac{1}{\dim(\mathcal{H}_{O_n})} \mathbb{I}_{I_n} \otimes \mathbb{I}_{O_n} \quad \text{for } 1 \leq n \leq N \quad (\text{B.93})$$

$$E_{o_n|i_n}^{(n)} = 0 \quad \text{else.} \quad (\text{B.94})$$

Bibliography

- [1] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (1932).
- [2] P. Dirac, *The Principles of Quantum Mechanics* (1930).
- [3] C. Shannon, A Mathematical Theory of Communication, *Bell System Technical Journal*, **27**, pp.379–423 and 623–656, (1948).
- [4] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Classical information capacity of a quantum channel, *Phys. Rev. A* **54**, 1869, (1996).
- [5] B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channels, *Phys. Rev. A* **56**, 131, (1997).
- [6] A. M. Turing, On Computable Numbers with an application to the Entscheidungsproblem. *Proc. London Math. Soc. s2* **43**: pp.230–265, (1937).
- [7] R. P. Feynman, Simulating physics with computers. *International J. of Theo. Phys.* **21**: pp.467f, (1982).
- [8] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Proc. Annual Symposium on the Foundations of Computer Science*, **35**, 124, (1994).
- [9] D. Deutsch and R. Jozsa. Rapid solutions of problems by quantum computation. *Proc. R. Soc. A* **439**, 553, (1992).
- [10] L. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* **79**, 325 (1997).
- [11] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE International Conference on Computers Systems and Signal Processing*, pp.175–179, (1984).

- [12] A. K. Ekert, Quantum cryptography based on Bell ' s theorem, *Phys. Rev. Lett.* **67**, 661, (1991).
- [13] J. I. Cirac and P. Zoller, Quantum Computations with Cold Trapped Ions, *Phys. Rev. Lett.* **74**, 4091, (1995).
- [14] N. A. Gershenfeld and I. L. Chuang, Quantum Computing with Molecules, *Scientific American* **278**, pp.66–71, (1997).
- [15] D. Loss and D. P. DiVincenzo, Quantum computation with quantum dots, *Phys. Rev. A* **57**, 120 (1998).
- [16] E. Knill, R. Laflamme and G. J. Milburn, A scheme for efficient quantum computation with linear optics, *Nature*, **409**, pp.46–52, (2001).
- [17] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood and I. L. Chuang, Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, *Nature* **414**, pp.883–887, (2001).
- [18] A. Politi, J. C. F. Matthews and J. L. O'Brien, Quantum Factoring Algorithm on a Photonic Chip, *Science* **325**, no. 5945, pp.1221f., (2009).
- [19] S. Lloyd, Quantum Computation over Continuous Variables, *Phys. Rev. Lett.* **82**, 1784, (1999).
- [20] A. Broadbent, J. Fitzsimons, E. Kashefi, Universal blind quantum computation. Proc. of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS), (2009).
- [21] E. Knill and R. Laflamme, *Phys. Rev. Lett.* **81**, 5672, (1998).
- [22] A. Datta, G. Vidal, On the role of entanglement and correlations in mixed-state quantum computation, *Phys. Rev. A* **75**, 042310, (2007).
- [23] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, Experimental Quantum Computing without Entanglement, *Phys. Rev. Lett.* **101**, 200501, (2008).
- [24] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wothers, *Phys. Rev. Lett.* **70**, 1895, (1993).
- [25] M. M. Wilde, *Quantum Information Theory*, Cambridge University Press (2013).
- [26] A. Winter. The capacity of the quantum multiple access channel. *IEEE Trans. on Information Theory*, **47**, pp.3059–3065, (2001).

- [27] J. Yard, P. Hayden, and I. Devetak. Capacity theorems for quantum multiple-access channels: Classical-quantum and quantum-quantum capacity regions. *IEEE Trans. Information Theory*, **54** (7), pp.3091–3113, (2008).
- [28] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, *Network Information Flow* **46**, 1204, (2000).
- [29] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger, Network coding for computing: Cut-set bounds, *IEEE Trans. Information Theory*, **57**, no.2, pp.1015–1030, (2011).
- [30] A. Soeda, Y. Kinjo, P.S. Turner and M. Muraio, Quantum computation over the butterfly network, *Phys. Rev. A* **84**, 012333, (2011).
- [31] A. R. Lehman, *Network Coding*, PhD thesis, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, (2005).
- [32] H. Kobayashi, F. Le Gall, H. Nishimura and M. Roetteler, General Scheme for Perfect Quantum Network Coding with Free Classical Communication, *LNCS* **5555**, pp.622f. (2009).
- [33] H. Kobayashi, F. Le Gall, H. Nishimura, and M. Rotteler, Perfect Quantum Network Communication Protocol Based on Classical Network Coding, *Proceedings of IEEE International Symposium on Information Theory 2010 (ISIT 2010)*, pp.2686–2690, (2010).
- [34] H. Kobayashi, F. Le Gall, H. Nishimura and M. Rotteler, Constructing Quantum Network Coding Schemes from Classical Nonlinear Protocols, *Proceedings of IEEE International Symposium on Information Theory 2011 (ISIT 2011)*, pp.109–113, (2011).
- [35] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, *Phys. Rev. Lett.* **86**, 5188, (2001).
- [36] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels, *Phys. Rev. Lett.* **70**, 1895, (1993).
- [37] J. S. Bell, *Physics* **1**, 195, (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880, (1969).
- [38] S. Popescu and D. Rohrlich, *Foundations of Physics* **24**, 3, pp.379–385, (1994).

- [39] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett.* **69**, 2881, (1992).
- [40] G. Vidal, Efficient Classical Simulation of Slightly Entangled Quantum Computations, *Phys. Rev. Lett.* **91**, 147902, (2003).
- [41] R. Jozsa and N. Linden, On the role of entanglement in quantum computational speed-up, *Proc. of the Royal Society of London. Series A. Mathematical, Physical and Engineering Sciences* **459**, pp.2011–2032, (2003).
- [42] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Local Distinguishability of Multipartite Orthogonal Quantum States, *Phys. Rev. Lett.* **85**, 4972, (2000).
- [43] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin and W. K. Wootters, Quantum nonlocality without entanglement, *Phys. Rev. A* **59**, pp.1070–1091, (1999).
- [44] J. Niset and N. J. Cerf, Multipartite nonlocality without entanglement in many dimensions, *Phys. Rev. A* **74**, 52103, (2006).
- [45] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin and B. M. Terhal, Unextendible Product Bases, Uncompletable Product Bases and Bound Entanglement, *Comm. Math. Phys.* **238**, pp.379–410, (2003).
- [46] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Entanglement-Assisted Classical Capacity of Noisy Quantum Channels, *Phys. Rev. Lett.* **83**, 3081, (1999).
- [47] H. Buhrman, R. Cleve, and W. van Dam, Quantum Entanglement and Communication Complexity, *SIAM J. Comput.*, **30**(6), pp.1829–1841, (2001).
- [48] G. Brassard, R. Cleve, and A. Tapp, Cost of Exactly Simulating Quantum Entanglement with Classical Communication, *Phys. Rev. Lett.* **83**, 1874, (1999).
- [49] C. Kiefer, Conceptual Problems in Quantum Gravity and Quantum Cosmology, *ISRN Mathematical Physics Volume* **2013**, 509316, (2013).
- [50] A. Cobham, The Recognition Problem for the Set of Perfect Squares, Technical report RC-1704, IBM, (1966).
- [51] E. Kushilevitz, N. Nisan, *Communication Complexity*, Cambridge University Press, Chapter 12, (1997).
- [52] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Quantifying Entanglement, *Phys. Rev. Lett.* **78**, 2275, (1997).

- [53] M. B. Plenio and S. Virmani, An introduction to entanglement measures, *Quant. Inf. Comp.* **7**, pp.1–51, (2007).
- [54] M. Horodecki, P. Horodecki, and R. Horodecki, Limits for Entanglement Measures, *Phys. Rev. Lett.* **84**, 2014, (2000).
- [55] E. Chitambar, D. Leung, L. Mancinska, M. Ozols, A. Winter, Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask), *Commun. Math. Phys.* **328**, no. 1, pp.303–326, (2014).
- [56] K. Gödel, An example of a new type of cosmological solution of Einstein ' s field equations of gravitation, *Rev. Mod. Phys.* **21** pp.447–450, (1949).
- [57] C. M. DeWitt, and D. Rickles, The Role of Gravitation in Physics. Report from the 1957 Chapel Hill Conference. Edition Open Sources, (2011).
- [58] O. Oreshkov, F. Costa, C. Brukner, Quantum correlations with no partial order, *Nature communications* **3**, 1092, (2012).
- [59] G. Chiribella, Theoretical framework for quantum networks, *Phys. Rev. A* **80**, 022339, (2009).
- [60] G. Chiribella, Quantum computations without definite causal structure, *Phys. Rev. A* **88**, 022318, (2012).
- [61] L. Hardy, Probability Theories with Dynamic Causal Structure: A New Framework for Quantum Gravity, arXiv:gr-qc/0509120, (2005).
- [62] N. D. Birrell and P. C. W. Davies, *Quantum Fields in Curved Space*, Cambridge University Press, (1982).
- [63] V. Gheorghiu and R. B. Griffiths, Separable operations on pure states, *Phys. Rev. A* **78**, 020304, (2008).
- [64] E. Chitambar and R. Duan, Nonlocal Entanglement Transformations Achievable by Separable Operations, *Phys. Rev. Lett.* **103**, 110502, (2009).
- [65] G. Chiribella, G. M. D ' Ariano, and P. Perinotti, Informational derivation of quantum theory, *Phys. Rev. A* **84**, 012311, (2011).
- [66] A. S. Holevo, Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel, *Probl. Peredachi Inf.*, **9**, Issue 3, pp.3–11, (1973).
- [67] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777, (1935).

- [68] M. Choi, Completely Positive Linear Maps on Complex matrices, *Linear Algebra and Its Applications* **10**, 3, pp.285–290, (1975).
- [69] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory*, Springer Verlag, (1983).
- [70] W. F. Stinespring, Positive Functions on C^* -algebras, *Proceedings of the American Mathematical Society*, 211, (1955).
- [71] A. Soeda and M. Murao, Delocalization power of global unitary operations on quantum information, *New J. Phys.* **12**, 093013, (2010).
- [72] S. Akibue and M. Murao, Network coding for distributed quantum computation over cluster and butterfly networks, arXiv:1503.07740, (2015).
- [73] A. Chefles, Condition for unambiguous state discrimination using local operations and classical communication, *Phys. Rev. A* **69**, 050307(R), (2004).
- [74] S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time. *Proc. of the Royal Society A*, **461** 2063: pp.3473–3482, (2005).
- [75] D. Deutsch, Quantum computational networks *Proc. R. Soc. Lond. A* **425**, pp.73–90, (1989).
- [76] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* **299**, pp.802–803, (1982).
- [77] A. Soeda, P. S. Turner and M. Murao, Entanglement cost of implementing controlled-unitary operations, *Phys. Rev. Lett.* **107**, 180501, (2011).
- [78] D. Stahlke and R. B. Griffiths, Entanglement requirements for implementing bipartite unitary operations, *Phys. Rev. A* **84**, 032316, (2011).
- [79] J. Eisert, K. Jakobs, P. Papadopoulos and M. B. Plenio, Optimal local implementation of nonlocal quantum gates, *Phys. Rev. A* **62**, 052317, (2000).
- [80] C. C. Wang and N. B. Shroff, Beyond the Butterfly – A Graph-Theoretic Characterization of the Feasibility of Network Coding with Two Simple Unicast Sessions, *ISIT2007, Nice, France*, (2007).
- [81] K. Iwama, H. Nishimura, M. Paterson, R. Raymond and S. Yamashita, Polynomial-Time Construction of Linear Network Coding, *LNCS* **5125**, pp.271f, (2008).

- [82] D. Leung, J. Oppenheim, and A. Winter, Quantum Network Communication The Butterfly and Beyond, *IEEE Trans. Information Theory* **56**, 3478, (2010).
- [83] M. Hayashi, Prior entanglement between senders enables perfect quantum network coding with modification, *Phys. Rev. A* **76**, 040301(R), (2007).
- [84] N. Khaneja, R. Brockett, and S. J. Glaser, Time optimal control in spin systems, *Phys. Rev. A* **63**, 032308, (2001).
- [85] B. Kraus and J. I. Cirac, Optimal creation of entanglement using a two-qubit gate, *Phys. Rev. A* **63**, 062309, (2001).
- [86] J. Zhang, J. Vala, Sh. Sastry, and K. B. Whaley, Geometric theory of nonlocal two-qubit operations, *Phys. Rev. A* **67**, 042313, (2003).
- [87] A. Soeda, S. Akibue and M. Muraio, Two-party LOCC convertibility of quadripartite states and Kraus-Cirac number of two-qubit unitaries, *J. Phys. A: Math. Theory* **47**, 424036, (2014).
- [88] L. Valiant, Quantum circuits that can be simulated classically in polynomial time, *SIAM J. Computing* **31**, 1229, (2002).
- [89] B. M. Terhal and D. P. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits, *Phys. Rev. A* **65**, 32325, (2002).
- [90] R. Jozsa and A. Miyake, Matchgates and classical simulation of quantum circuits, *Proc. R. Soc. A* **464**, 3089, (2008).
- [91] W. Dür, G. Vidal and J. I. Cirac, Optimal Conversion of Nonlocal Unitary Operations, *Phys. Rev. Lett.* **89**, 057901, (2002).
- [92] F. Vatan and C. Williams, Optimal quantum circuits for general two-qubit gates, *Phys. Rev. A* **69**, 032315, (2004).
- [93] E. Tyrtysnikov, Tensor ranks for the inversion of tensor-product binomials, *Journal of Comp. and Applied Math.* archive **234** Issue 11, pp.3170–3174, (2010).
- [94] V. Danos and E. Kashefi, Determinism in the one-way model, *Phys. Rev. A*, **74**, 052310, (2006).
- [95] D. Browne, E. Kashefi, M. Mhalla, and S. Perdrix, Generalized flow and determinism in measurement-based quantum computation, *New Journal of Physics*, **9**, 250, (2007).

- [96] M. Mhalla, M. Muraio, S. Perdrix, M. Someya and P. S. Turner, Which Graph States are Useful for Quantum Information Processing?, *Theory of Quantum Computation, Communication, and Cryptography* **6745** of the series LNCS pp.174–187, (2014).
- [97] R. Duan, Y. Feng, Y. Xin, and M. Ying, Distinguishability of Quantum States by Separable Operations, *IEEE Trans. Information Theory*, **55**, no. 3, (2009).
- [98] S. Cohen, All unitaries having operator Schmidt rank 2 are controlled unitaries, *Phys. Rev. A* **87**, 022329, (2013).
- [99] E. Wakakuwa and M. Muraio, Asymptotic Compressibility of Entanglement and Classical Communication in Distributed Quantum Computation, arXiv:1310.3991 (2013).
- [100] C. H. Bennett. talk at QUPON, Vienna, Austria, May (2005).
- [101] S. Lloyd, L. Maccone, R. Garcia-Patron, V. Giovannetti, and Y. Shikano, Quantum mechanics of time travel through post-selected teleportation, *Phys. Rev. D* **84**, 025007, (2011).
- [102] S. Lloyd, L. Maccone, R. Garcia-Patron, V. Giovannetti, Y. Shikano, S. Pirandola, L. A. Rozema, A. Darabi, Y. Soudagar, L. K. Shalm, and A. M. Steinberg, Closed Timelike Curves via Postselection: Theory and Experimental Test of Consistency, *Phys. Rev. Lett.* **106**, 040403, (2011).
- [103] T. Colnaghi, G. M. D’Ariano, S. Facchini, P. Perinotti, Quantum computation with programmable connections between gates, *Phys. Lett. A* **376**, 45, (2012).
- [104] K. Nakago, M. Hajdusek, S. Nakayama and M. Muraio, Parallelizable adiabatic gate teleportation, arXiv:1310.4061 (2013).
- [105] L. M. Procopio, A. Moqanaki, M. Araujo, F. Costa, I. A. Calafell, E. G. Dowd, D. R. Hamel, L. A. Rozema, C. Brukner and P. Walther, Experimental superposition of orders of quantum gates, *Nature Communications* **6**, 7913, (2015).
- [106] Ä. Baumeler, S. Wolf, Perfect signaling among three parties violating pre-defined causal order, arXiv:1312.5916 (2014).
- [107] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, *Phys. Rev. A* **53**, 2046, (1996).

- [108] F. Verstraete, J. Dehaene, B. De Moor and H. Verschelde, Four qubits can be entangled in nine different ways, *Phys. Rev. A* **65**, 052112, (2002).