論文の内容の要旨

# 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）

秋笛　清石

The processing power of widely used *silicon-based computers* has been increasing exponentially due to steady improvements in nanotechnology. However this exponential growth is not sustainable, as the size of the components will eventually reach the atomic scale, where quantum mechanical effects become significant and the conventional design of computation will no longer work. *Quantum computation*, on the other hand, makes direct use of quantum mechanical effects to provide a new computational power. Indeed, it has been shown that a large-scale quantum computer can solve the factoring problem (finding the prime factors of large integers) much faster than any foreseeable conventional computers, a problem of the utmost importance for public key cryptography. Many different kinds of physical systems have been studied in order to decide their suitability for implementing quantum computation, such as ion traps, nuclear magnetic resonance, quantum dots and linear optics. However none of these have achieved computation on a scale large enough for practical quantum computation by using a single quantum system.

*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.

In the first part of this thesis, we study how to improve the performance of quantum communication, i.e. transmitting quantum states between different nodes of the quantum network, over a given quantum network resource. The performance of quantum communication through a quantum channel from one sender to one receiver has been extensively studied in *quantum Shannon theory*. 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, it has been recently shown that processing the packets in the intermediate nodes called *network coding* improves communication performance comparing to routing the packets. It was shown that the idea of network coding can be used for computation as well as communication, as communication can be regarded as a special case of computation.

We analyze what kinds of computation can be implemented over a given quantum network resource. 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. Two examples of quantum networks well studied in network coding theory are shown in Fig. 1.

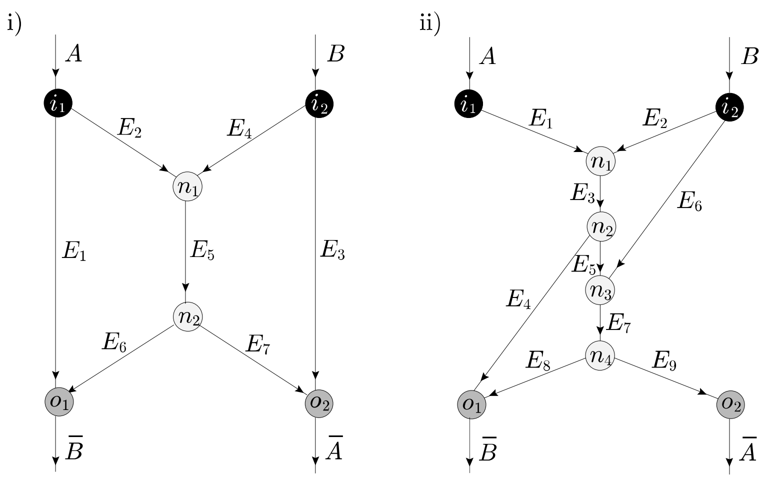



Fig. 1. **The butterfly and the grail quantum network.**

i) The butterfly network and ii) the grail network with input nodes ($i_1$ and $i_2$), output nodes ($o_1$ and $o_2$) and repeater nodes.

We consider a setting that quantum communication for each edge of a network is equivalent to *entanglement* and classical communication as a resource owing to *quantum teleportation*. Specifically, we analyze which *k*-qubit unitary operations are implementable over the given entanglement resources represented by a certain class of quantum 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. The cluster network is a subclass of the *k-pair network*, which has been an actively studied network in both classical network coding and quantum network coding. Since the entangled state represented by the cluster network is closely related to a *cluster state* used for *measurement based quantum computation* (MBQC), an extensively studied model of quantum computation, we discuss the relationship between our result and MBQC.

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) for implementing a joint quantum operation in SEP as summarized in the Fig. 2. For simplicity, we consider LOCC between two parties, however, a generalization of our results into several parties is straightforward.

Fig. 2 for implementing SEP

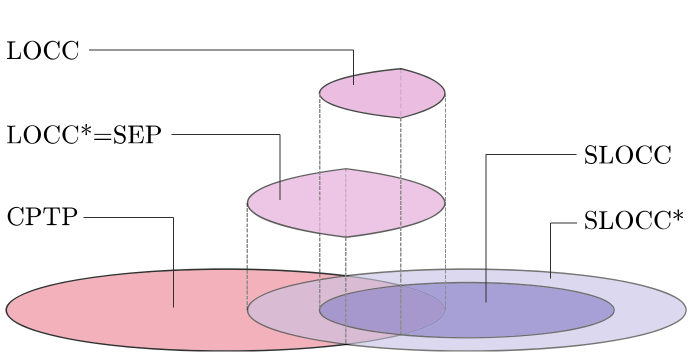

We start with analyzing the amount of the entanglement resource required for a specific DQC task known as *local state discrimination*. The task is discriminating a state from a given set of orthonormal basis states by LOCC with help of entanglement. We show that entanglement required for the discrimination task allowing only one-round classical communication can be substituted by *less* entanglement by *increasing* the rounds of classical communication.

Entanglement can be considered as a spatial resource since it can generate spatial quantum correlation, which can never be achieved by any laws of physics based on the local realism, e.g. classical mechanics. On the other hand, the rounds of classical communication between two parties can be considered as a temporal resource. Thus, our result shows that increasing the spatial resource enables decreasing the temporal resource, which can be interpreted as a power of entanglement for parallelizing information processing.

It has been known that there exists a quantum operation in SEP that cannot be implemented by infinite-round LOCC, namely, entanglement resource is necessary as long as using standard classical communication. However, we show another 'classical' resource completely substituting entanglement and classical communication consumed in entanglement assisted LOCC for implementing a quantum operation in SEP by relaxing the constraint of *special relativistic causality*. 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.

By considering the correspondence between LOCC* and a probabilistic version of LOCC called stochastic LOCC (SLOCC), we show that CC* 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 causal order (the quantum process formalism) recently developed by Ognyan Oreshkov et al. Finally we construct an example of non-LOCC SEP by using LOCC* for a three-party case. The result is summarized in Fig. 3.

Fig. 3. **Class of quantum operations.**




CPTP is a set of all the deterministic quantum operations. SLOCC* is a set of all the linear operations simulatable by SLOCC. The intersection of SLOCC* and CPTP is LOCC*.