Extraction of distributed quantum information by LOCC

Mio Murao, Ryu Ebisawa, Masaki Owari

Department of Physics, The University of Tokyo, Tokyo 113-0033, Japan

June 13, 2003

Abstract

Extraction of distributed quantum information by LOCC

Quantum information of an unknown single qubit state is described by $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown complex parameters satisfying $|\alpha|^2 + |\beta|^2 = 1$. This information can be distributed into a N-qubit state $\left|\phi^{(N)}\right\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle$ where $|\psi_0\rangle$ and $|\psi_1\rangle$ are two bases in the N qubit Hilbert space ($\langle\psi_i|\psi_j\rangle = \delta_{ij}$). The basis states determine how the quantum information of a single qubit is distributed into several qubits. In general, the basis states are entangled states. The distribution of quantum information of a single qubit is represented by $\left|\phi^{(1)}\right\rangle \rightarrow \left|\phi^{(N)}\right\rangle$ and it creates entanglement in general. Therefore, global operations among different qubits or an appropriate entanglement resource (i.e., the telecloning state [1] for optimal cloning type distribution) is required.

The reverse process, the extraction of distributed quantum information $\left|\phi^{(N)}\right\rangle_{A\ldots N} \rightarrow \left|\phi^{(1)}\right\rangle_A$, destroys entanglement. Does extraction still require global operations or an appropriate entanglement resource? We obtain the conditions that extraction of distributed quantum information can be performed with only LOCC. For $N = 2$, the necessary and sufficient condition for LOCC extraction $\left|\phi^{(N)}\right\rangle_{AB} \rightarrow \left|\phi^{(1)}\right\rangle_A$ is that the two bases can be written in either of the following forms:

$$|\psi_0\rangle_{AB} = |\eta_0\rangle|\chi_0\rangle \quad (1)$$

$$|\psi_1\rangle_{AB} = \left|\eta_0^\perp\right\rangle|\chi_1\rangle \quad (2)$$

where $\left|\eta_i^\perp\right\rangle$ and $|\bar{i}\rangle$ are normalized states satisfying $\left\langle\eta_0^\perp|\eta_0\right\rangle = 0$ and $|\chi_0\rangle$ and $|\chi_1\rangle$ are arbitrary normalized states, or

$$|\psi_0\rangle_{AB} = \cos\theta|\eta_0\rangle|\bar{0}\rangle + \sin\theta|\eta_1\rangle|\bar{1}\rangle \quad (3)$$

$$|\psi_1\rangle_{AB} = \cos\theta\left|\eta_0^\perp\right\rangle|\bar{0}\rangle + \sin\theta\left|\eta_1^\perp\right\rangle|\bar{1}\rangle \quad (4)$$

where $0 \leq \theta \leq \pi/2$, and $|\eta_i\rangle$, $\left|\eta_i^\perp\right\rangle$ and $|\bar{i}\rangle$ are normalized states satisfying $\left\langle\eta_i^\perp|\eta_i\right\rangle = 0$ and $\langle\bar{i}|\bar{j}\rangle = \delta_{ij}$, but where $\langle\eta_0|\eta_1\rangle = 0$ is not necessary.

It is interesting to consider several asymmetries that appear in the distribution and extraction of quantum information. We can find a way of distributing quantum information which require a large amount of entanglement resource, i.e. the initially shared entangled state and global recovery operations as well as classical communications, but requires no entanglement for extraction. This strong asymmetry in terms of required resources may suggest the possibility of developing a quantum "one-way" function. There is another interesting point arising from the fact that

the condition for extracting distributed quantum information by LOCC is not symmetric in terms of the qubits A and B. This means that we can distribute quantum information in an "unfair" way, such that Alice can extract quantum information by LOCC but Bob cannot. These asymmetries of distribution/extraction in terms of entanglement may be useful for cryptographic protocols.

References

[1] M. Murao et al, Phys. Rev. A **59**, 156 (1999).