Compressibility of quantum mixed-state signals

Masato Koashi and Nobuyuki Imoto
CREST Research Team for Interacting Carrier Electronics, School of Advanced Sciences, The Graduate University for Advanced Studies (SOKEN), Hayama, Kanagawa, 240-0193, Japan

We present a formula that determines the optimal number of qubits per message that allows asymptotically faithful compression of the quantum information carried by an ensemble of mixed states. The set of mixed states determines a decomposition of the Hilbert space into three parts, and the von Neumann entropy of the ensemble is also written as the sum of three parts, redundant ($I_{\rm R}$), classical ($I_{\rm C}$), and nonclassical ($I_{\rm NC}$) ones. The optimal compression rate in blind protocol is then given by $I_{\rm C}+I_{\rm NC}$. When classical bits are available, the required number of qubits reduces to $I_{\rm NC}$.

Consider a source that generates a message i with probability p_i. Sequences of the messages independently drawn from this source can be compressed into sequences of bits and decompressed back to the original sequences of messages. The necessary and sufficient number of bits per message allowing asymptotically faithful compression and decompression is given by the Shannon entropy $S=-\sum_i p_i \log_2 p_i$ [1]. This is one of the core results of the classical information theory. The quantum analogue of this theorem, which will naturally form a basis of quantum information theory, was first considered by Schumacher [2]. In this quantum data compression, the source emits a system in a quantum state ρ_i with probability p_i, and sequences of the systems emitted from this source are assumed to be compressed into qubits. When all ρ_i are pure [2,3], it was shown that the least number $I_{\rm p}$ of qubits per message allowing asymptotically faithful recovery of the original states is given by the von Neumann entropy $S(\rho)=-{\rm Tr}\rho\log_2\rho$ of the density operator of the ensemble $\rho=\sum_i p_i\rho_i$. When $\{\rho_i\}$ includes mixed states, the problem is still open [4].

We derived the formula for $I_{\rm p}$ using a principle [5] that gives a definite distinction between what one can do and what one cannot do without changing the state of a system, which was secretly prepared in one of the states $\{\rho_i\}$. Given $\{\rho_i\}$, we can find a decomposition of their support $\mathcal{H}_{\rm A}$ written as $\mathcal{H}_{\rm A}=\bigoplus_l \mathcal{H}_{\rm J}^{(l)}\otimes\mathcal{H}_{\rm K}^{(l)}$, such that any unitary operation U acting on $\mathcal{H}_{\rm A}$ and the ancilla space $\mathcal{H}_{\rm E}$ that preserves $\{\rho_i\}$ is expressed in the following form

$$U(\mathbf{1}_{\rm A}\otimes\Sigma_{\rm E})=\bigoplus_l \mathbf{1}_{\rm J}^{(l)}\otimes U_{\rm KE}^{(l)}(\mathbf{1}_{\rm K}^{(l)}\otimes\Sigma_{\rm E}), \tag{1}$$

where $U_{\rm KE}^{(l)}$ are unitary operators acting on the combined space $\mathcal{H}_{\rm K}^{(l)}\otimes\mathcal{H}_{\rm E}$. Under this decomposition, ρ_i is written as

$$\rho_i=\bigoplus_l q^{(i,l)}\rho_{\rm J}^{(i,l)}\otimes\rho_{\rm K}^{(l)}, \tag{2}$$

and the total density operator ρ for the ensemble $\{p_i,\rho_i\}$ is written as $\rho=\bigoplus_l p^{(l)}\rho_{\rm J}^{(l)}\otimes\rho_{\rm K}^{(l)}$. The von Neumann entropy of ρ is written by the sum of three parts, $S(\rho)\equiv I_{\rm C}+I_{\rm NC}+I_{\rm R}$, as follows,

$$S(\rho)=\sum_l p^{(l)}\left[-\log_2 p^{(l)}+S(\rho_{\rm J}^{(l)})+S(\rho_{\rm K}^{(l)})\right] \tag{3}$$

The form (2) means that $I_{\rm p}\le I_{\rm C}+I_{\rm NC}$, since $\rho_{\rm K}^{(l)}$ is independent of i and redundant. Since the combined process of compression and decompression is regarded as a quantum operation that (nearly) preserves $\{\rho_i\}$, it must be (approximately) written by the form (1). Then, we can show that using an orthogonal pure-state ensemble as an input to the combined process, we can transmit $I_{\rm C}+I_{\rm NC}$ bits of information. This gives $I_{\rm p}\ge I_{\rm C}+I_{\rm NC}$, and we obtain the formula $I_{\rm p}=I_{\rm C}+I_{\rm NC}$ [6]. A similar argument using an ensemble with states entangled to another system proves that only $I_{\rm C}$ qubits can be replaced by the same number of classical bits [7].

The present results elucidate the property of information stored in a quantum ensemble as follows. The information can always be decomposed into three parts, namely, redundant, classical, and nonclassical parts. The classical part can be copied, compressed into bits, and transmitted through a classical channel. The nonclassical part of the information cannot be extracted without disturbing the states, can be compressed only into qubits, and must consume entanglement when transmitted over a classical channel.

---

[1] E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[2] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
[3] R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994); H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. A **54**, 4707 (1996); H. Barnum, P. Hayden, R. Jozsa, and A. Winter, `arXiv quant-ph/0011072`.
[4] M. Horodecki, Phys. Rev. A **57**, 3364 (1998); M. Horodecki, Phys. Rev. A **61**, 052309 (2000); H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, `arXiv quant-ph/0008024`; W. Dür, G. Vidal, and J. I. Cirac, `arXiv quant-ph/0101111`; G. Kramer and S. A. Savari, `arXiv quant-ph/0101119`.
[5] M. Koashi and N. Imoto, `arXiv quant-ph/0101144`.
[6] M. Koashi and N. Imoto, Phys. Rev. Lett. **87**, 017902 (2001).
[7] M. Koashi and N. Imoto, `arXiv quant-ph/0104001`.