ISSN 0021-3640, JETP Letters, 2014, Vol. 99, No. 7, pp. 419–423. © Pleiades Publishing, Ltd., 2014.
Original Russian Text © S.N. Molotkov, T.A. Potapova, 2014, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2014, Vol. 99, No. 7, pp. 488–492.

On the Compression of Information of a Classical Source with the Use of Side Quantum and Classical Information

S. N. Molotkov[a–c] and T. A. Potapova[d]

[a] *Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia*
[b] *Academy of Cryptography of the Russian Federation, Moscow, 121552 Russia*
[c] *Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, 119991 Russia*
e-mail: sergei.molotkov@gmail.com
[d] *Faculty of Information Technologies and Computer Engineering, National Research University Higher School of Economics, ul. Myasnitskaya 20, Moscow, 101000 Russia*

Received March 11, 2014

The problem of the compression of classical information when a receiver has access only to side quantum states associated with classical states of a source, which are not available directly, is examined. For the receiver to be able to reconstruct the entire information of the source, a certain additional amount of side classical information is required. A bound on the minimum necessary amount of side classical information has been obtained by simple means.

DOI: 10.1134/S0021364014070108

INTRODUCTION

A source of information can generate either classical or quantum states. One of the fundamental results of classical information theory is the theorem of the compression of information, which is also called the Shannon coding theorem for a classical source [1]. The situation in the quantum case is more diverse [2]. Classical information can be transmitted by quantum states. In particular, a key (random classical bit string) in quantum cryptography is distributed by quantum states. The upper bound of classical information that can be extracted from an ensemble of quantum states is the fundamental Holevo bound (Holevo coding theorem [3]). This bound was first obtained for pure states and, then, for mixed states [4, 5]. Schumacher coding [6] (compression of quantum information) provides the minimum dimension of the Hilbert space of states of a quantum communication channel into which quantum states of the source can be inserted without loss of quantum information (distortion of the initial quantum states). Quantum mechanics allows the transfer of an unknown quantum state from one quantum system to another by means of a preliminarily distributed entangled state (teleportation of a quantum state, i.e., quantum information) with the joint use of a quantum channel and an auxiliary classical communication channel. Teleportation was predicted in [7] and was experimentally demonstrated in the complete Bell basis in [8]. This phenomenon fundamentally does not have any classical analog. Quantum mechanics allows the transmission of classical information by means of an entangled state and an additional classical channel (superdense coding [9]).

Below, we consider the compression of classical information in the case where the states of the classical source are not available directly. Only side quantum states unambiguously associated with the classical states of the source are available. Such a situation occurs, e.g., in quantum cryptography. Having access only to side quantum states, which are generally nonorthogonal, the receiver fundamentally cannot identify all sequences of states generated by the source. The question is *what is the minimum amount of classical side information in addition to quantum information necessary for reliable discrimination (in the asymptotic limit) of all initial classical sequences*.

This problem is a quantum analog of a classical problem considered by Slepian and Wolf [10]. It is formulated as follows. There are two correlated classical sources. Each source sends states to one receiver. It is possible to indicate an upper bound of amount of information that can be obtained by the receiver having access only to one of two sources. It is necessary to obtain an upper bound of amount of information that can be obtained by the receiver having access simultaneously to two sources. In this situation, one of them can be considered as a source of side information with respect to the other source. In the quantum case, the problem of the compression of classical information with side quantum information was considered by Devetak and Winter [11] with the use of the method of projection on the typical space. Renes and Renner [12] solved this problem using the language of min and max von Neumann entropy.

Using simple means, we will show below that the solution of the formulated problem can be obtained as

a generalization of the remarkable Holevo coding theorem for a *quantum source* [2–4]. This way is the most direct and makes it possible to obtain more accurate estimates of the probability of error.

CLASSICAL SOURCE

Let a classical source generate states according to the alphabet $X = \{x_1, x_2, ..., x_m\}$ and the probability distribution $p_X(x)$ specified on it. The source is used n times, where n is sufficiently large. Let sequences $X^n = (x_{i_1}, x_{i_2}, ..., x_{i_n})$ with the length n be sent through an ideal channel without memory. The total number of sequences with the length n is $2^{n\log m}$ (here and below, log means base-2 logarithm). All sequences can be classified as typical and atypical. The set of typical sequences $T_{\delta,\varepsilon}$ has the dimension

$$2^{n[H(X)-\delta]} < |T_{\delta,\varepsilon}| < 2^{n[H(X)+\delta]}, \quad (1)$$

beginning with a certain length $n > n_0(\delta, \varepsilon)$ (where δ and ε are any infinitesimal values). The probabilities $p(X^n)$ of the appearance of all typical sequences are approximately identical (asymptotic equidistribution):

$$2^{-n[H(X)+\delta]} < p(X^n) < 2^{-n[H(X)-\delta]}. \quad (2)$$

At large n values, there are $(1-\varepsilon)2^{n[H(X)-\delta]}$ typical words. The probability of other atypical sequences is no more than ε. The number of bits of information that is generated by a source per message in the asymptotic limit of long sequences ($n \longrightarrow \infty$) is $nH(X)$ (where $H(X) = -\sum_{i=1}^{m} p_X(x_i)\log p_X(x_i)$).

The source coding theorem (the compression of classical information) informally means that integers from the range $1 \le J \le 2^{nH(X)}$ is sufficient for enumeration of all typical sequences. The representation of these integers requires no more than $[nH(X)] + 1$ binary positions (where [...] is the integer part of a number), and each carries one bit of information. Instead of the transmission of n positions that are generated by the source, the receiver and transmitter can preliminarily agree on a common code table presenting the correspondence between each typical sequence $X_J = (x_{i_1}, x_{i_2}, ..., x_{i_n})$ and $[nH(X)] + 1$-bit number J. The enumeration of typical sequences can be arbitrary because of their equidistribution. If the source generates one of the typical sequences, the ordinal number J of the sequence, rather than the sequence itself, is sent. The receiver uniquely reconstructs the generated sequence from the code table. If the source generates an atypical sequence, it is rejected and nothing is sent. Information is not lost in the asymptotic limit. *The access of transmitter and receiver to the preliminarily accepted code table is fundamentally important for the compression of information.*

QUANTUM SOURCE

Classical information can be transmitted by means of quantum states. The classical source with the alphabet $X = (x_1, x_2, ..., x_m)$ and probability distribution $p_X(x)$ on it is matched with the quantum alphabet $Q = (\rho_{x_1}, \rho_{x_2}, ..., \rho_{x_m})$ ($x_i \longrightarrow \rho_{x_i}$) with the same probability distribution. The amount of classical information that can be obtained from such a source is limited by the Holevo fundamental value [2–4]. When the channel is used n-times, only $2^{n\chi(\bar\rho)}$ quantum sequences of all $2^{nH(X)}$ classical typical sequences, which are assigned with quantum states, can be reliably distinguished, where

$$\chi(\bar\rho) = H(\bar{\bar\rho}) - \sum_{x}^{m} p_X(x) H(\rho_x),$$
$$\bar\rho = \sum_{x}^{m} p_X(x)\rho_x, \quad H(\rho) = -\mathrm{Tr}\{\rho\log\rho\} \quad (3)$$

(here and below, depending on the context, the Shannon and von Neumann entropies are denoted by the same letter H, which should not lead to misunderstanding). More precisely, no more than $2^{n\chi(\bar\rho)}$ sequences of all $2^{nH(X)}$ quantum sequences with the length n ($\rho_{x_{i_1}}, \rho_{x_{i_2}}, ..., \rho_{x_{i_n}}$) are reliably distinguished (with arbitrarily small probability of error in the asymptotic limit $n \longrightarrow \infty$). There are a code (code table of sequences and their ordinal numbers) with the size of no more than $2^{n\chi(\bar\rho)}$ and a set of quantum-mechanical measurements that make it possible to reliably distinguish all code sequences in the presence of the preliminarily accepted code table accessible to the transmitter and receiver. In other words, the Holevo fundamental bound is achievable [2, 4].

Thus, the receiver and transmitter should preliminarily accept the code table. According to this code table, the source generates first classical and then quantum states. The receiver constructs measurements (decoder) that make it possible to distinguish quantum sequences only inside the code table (code words).

CLASSICAL SOURCE WITH SIDE QUANTUM AND CLASSICAL STATES

In a number of important problems of quantum informatics, it is necessary to distinguish sequences of quantum states when the receiver does not have the preliminarily accepted code table. In particular, this is the case in quantum cryptography, when the transmitter sends sequences of quantum states matched with classical states to a communication channel:

$$(x_{i_1}, x_{i_2}, ..., x_{i_n}) \longrightarrow (|\phi_{x_{i_1}}\rangle, |\phi_{x_{i_2}}\rangle ... |\phi_{x_{i_n}}\rangle), \quad (4)$$

and an eavesdropper does not have the code table. Classical states remain for the receiver, whereas quantum states are sent to the communication channel. The transmitter generates $\approx 2^{nH(x)}$ classical words. However, if quantum states are nonorthogonal (as in quantum cryptography), the number of reliably distinguishable sequences *even in the presence of the code table* is no more than $\approx 2^{n\chi(\bar{\rho})}$ ($2^{n\chi(\bar{\rho})} < 2^{nH(x)}$). In the absence of the code table, the receiver "sees" an ensemble of states that is described by the density matrix

$$\begin{aligned}\rho_{XQ} &= \sum_{x_{i_1}, \ldots, x_{i_n}} p_X(x_{i_1})\ldots p_X(x_{i_n})|x_{i_n}\rangle\langle x_{i_1}| \otimes \\ &\ldots \otimes |x_{i_n}\rangle\langle x_{i_n}| \otimes \rho_{x_{i_1}} \otimes \ldots \otimes \rho_{x_{i_n}} \\ &= \left[\sum_x p_X(x)|x\rangle\langle x| \otimes \rho_x\right]^{\otimes n},\end{aligned} \tag{5}$$

and the receiver has access only to side quantum states (subsystem Q) and does not have access to classical states X.

The question is what is the minimum amount of additional (side) classical information that should be accessible to the receiver for reliable discrimination of all $2^{n\log m}$ sequences. The source generates a classical string and assigns it to a sequence of quantum states (quantum source). Furthermore, the transmitter transmits auxiliary side classical information to the receiver from the second classical source certainly correlated with the quantum source. (The Slepian–Wolf problem involves two correlated classical sources. In the problem under consideration, there are also two correlated sources: quantum and classical.) The auxiliary source has its alphabet Z and probability distribution on it $p_Z(z)$. *As will be shown below, the dimension of the alphabet and the type of distribution are insignificant. Only the Shannon entropy of this source is important*. Therefore, it is sufficient to take the simplest binary alphabet $Z = \{0, 1\}$, $p_Z(0) = q$ and $p_Z(1) = 1 - q$. *Side classical information is generated for each quantum sequence*, e.g., by means of n tossings of an asymmetric coin. The entropy of such a source is $nH(q) = nh(q)$ (where $h(q) = -q\log q - (1-q)\log(1-q)$ is the binary entropy function).

Side classical information can be represented in terms of *orthogonal quantum states* $|z\rangle$ ($z = 0, 1$):

$$\begin{aligned}&(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \\ &\longrightarrow (|\phi_{x_{i_1}}\rangle \otimes |z_{i_1}\rangle, |\phi_{x_{i_2}}\rangle \otimes |z_{i_2}\rangle\ldots|\phi_{x_{i_n}}\rangle \otimes |z_{i_n}\rangle) \\ &= (|\phi_{x_{i_1}, z_{i_1}}\rangle \otimes |\phi_{x_{i_2}, z_{i_2}}\rangle\ldots|\phi_{x_{i_n}, z_{i_n}}\rangle) = |\Phi_{J_{(x,z)}}\rangle.\end{aligned} \tag{6}$$

The side classical state $|z_{i_k}\rangle$ is generated for each event of generation of a quantum state $|\phi_{x_{i_k}}\rangle$. For subsequent consideration, it is convenient to denote the set of subscripts as $J_{(x,z)} = ((x_{i_1}, z_{i_1}); (x_{i_2}, z_{i_2}); \ldots; (x_{i_n}, z_{i_n}))$. The number of sets of subscripts is $2^{n\log m}$, which is the number of generated sequences $(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$. Each position of quantum states "is equipped" with auxiliary classical information whose amount per position is $h(q)$ bits. It is necessary to determine the minimum amount $h(q)$ of side classical information at which the receiver, having access to quantum states and side classical information $(z_{i_1}; z_{i_2}; \ldots; z_{i_n})$ and using quantum-mechanical measurements, can reliably distinguish all sequences $(|\phi_{x_{i_1}}\rangle, |\phi_{x_{i_2}}\rangle, \ldots, |\phi_{x_{i_n}}\rangle)$ generated by the source and, correspondingly, $(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$.

We will show below that the answer to the above question is in fact a consequence of the Holevo theorem [2–4]. We consider only the case of pure states and direct theorem. The case of mixed states can be considered similarly and is a consequence of the case of pure states [4]. The inverse coding theorem (strong inversion) can be proved by the Ogawa–Nagaoka method [13].

It is important that the transmitter and receiver use side quantum states and side classical information for a common quantum–classical code table. Knowing this table (correspondence between the subscript $J(x, z)$ and a certain quantum–classical sequence), the receiver performs measurements. Measurements of states (6) are represented by a decomposition of unity:

$$I = \sum_{J_{(x,z)}}^{N} M_{J(x,z)}, \tag{7}$$

where $M_{J_{(x,z)}}$ are positive operator-valued measures and N is the number of sets of subscripts $J_{(x,z)}$. The conditional probability that the sequence of states $|\Phi_{J_{(x,z)}}\rangle$ is sent and measurements provide the outcome $J'_{(x,z)}$ is $\Pr(J'_{(x,z)}|J_{(x,z)}) = \langle\Phi_{J_{(x,z)}}|M_{J'_{(x,z)}}|\Phi_{J_{(x,z)}}\rangle$.

The mean error probability over all sequences is

$$P_{\text{err}}(N) = \frac{1}{N}\sum_{J_{(x,z)}}^{N}(1 - \langle\Phi_{J_{(x,z)}}|M_{J_{(x,z)}}|\Phi_{J_{(x,z)}}\rangle), \tag{8}$$

where N is the number of sequences. Pretty good measurements are chosen in the form

$$\begin{aligned}M_{J_{(x,z)}} &= |\hat{\Phi}_{J_{(x,z)}}\rangle\langle\hat{\Phi}_{J_{(x,z)}}|, \\ |\hat{\Phi}_{J(x,z)}\rangle &= \Gamma^{-1/2}|\Phi_{J_{(x,z)}}\rangle, \text{ where}\end{aligned} \tag{9}$$

$$\Gamma = \sum_{J_{(x,z)}}^{N} |\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|$$

is the Gram operator. In view of Eq. (9), Eq. (8) can be written in the form

$$P_{\text{err}}(N) = \frac{1}{N}\sum_{J_{(x,z)}}^{N}(1 - |\langle\hat{\Phi}_{J_{(x,z)}}|\Phi_{J_{(x,z)}}\rangle|^2)$$

$$\leq \frac{2}{N}\sum_{J_{(x,z)}}^{N}(1 - |\langle\hat{\Phi}_{J_{(x,z)}}|\Gamma^{1/2}|\hat{\Phi}_{J_{(x,z)}}\rangle|^2) \qquad (10)$$

$$= \frac{2}{N}\text{Tr}(\Gamma - \Gamma^{1'2}).$$

Here, we used the equality

$$\text{Tr}((\ldots)|\hat{\Phi}_{J_{(x,z)}}\rangle\langle\hat{\Phi}_{J_{(x,z)}}|) = \langle\hat{\Phi}_{J_{(x,z)}}|((\ldots))|\hat{\Phi}_{J_{(x,z)}}\rangle.$$

Then, $2(\Gamma - \Gamma^{1/2}) \leq \Gamma^2 - \Gamma$ (see, e.g., [4, 14]). We calculate the average error probability for all possible implementations of the classical source according to the probability distributions $p_X(x)$ and $p_Z(z)$ on the side quantum and classical alphabets:

$$\overline{P_{\text{err}}(N)} \leq \frac{1}{N}\overline{\text{Tr}(\Gamma - \Gamma^{1/2})}$$

$$= \frac{1}{N}\text{Tr}\left\{\overline{\left(\sum_{J_{(x,z)}}^{N}|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|\right)} \right. \qquad (11)$$

$$\left. \times\overline{\left(\sum_{J'_{(x,z)}}^{N}|\Phi_{J'_{(x,z)}}\rangle\langle\Phi_{J'_{(x,z)}}|\right) - \sum_{J_{(x,z)}}^{N}|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|}\right\},$$

where averaging over the distributions $p_X(x)$ and $p_Z(z)$ means

$$\overline{(\ldots)} = \sum_{x_{i_1},\ldots,x_{i_n}}\sum_{z_{i_1},\ldots,z_{i_n}}[p_X(x_{i_1})p_X(x_{i_2})\ldots p_X(x_{i_n})]$$

$$\times [p_Z(z_{i_1})p_Z(z_{i_2})\ldots p_Z(z_{i_n})](\ldots),$$

$$\overline{P_{\text{err}}(N)} \leq \frac{1}{N}\text{Tr}\left\{\sum_{J_{(x,z)}\neq J'_{(x,z)}}\overline{(|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|)}\right.$$

$$\left.\times\overline{(|\Phi_{J'_{(x,z)}}\rangle\langle\Phi_{J'_{(x,z)}}|)}\right\}$$

$$= (N-1)\text{Tr}\left\{\left(\sum_{x_{i_1},x_{i_2},\ldots,x_{i_n}}p_X(x_{i_1})p_X(x_{i_2})\right.\right. \qquad (12)$$

$$\left.\left.\ldots p_X(x_{i_n})|\phi_{x_{i_1}}\rangle\langle\phi_{x_{i_1}}|\otimes|\phi_{x_{i_2}}\rangle\langle\phi_{x_{i_2}}|\otimes\ldots\otimes|\phi_{x_{i_n}}\rangle\langle\phi_{x_{i_n}}|\right)\right.$$

$$\left.\times\left(\sum_{z_{i_1},z_{i_2}\ldots z_{i_n}}p_Z(z_{i_1})p_Z(z_{i_2})\right.\right.$$

$$\left.\left.\ldots p_Z(z_{i_n})|z_{i_1}\rangle\langle z_{i_1}|\otimes|z_{i_2}\rangle\langle z_{i_2}|\otimes\ldots\otimes|z_{i_n}\rangle\langle z_{i_n}|\right)\right\}$$

$$= 2(N-1)\text{Tr}(\overline{\rho_x}^2)^{\otimes n}\text{Tr}(\overline{\rho_z}^2)^{\otimes n},$$

where

$$\overline{\rho}_x = \sum_x p_X(x)|\phi_x\rangle\langle\phi_x|, \quad \overline{\rho}_z = \sum_z p_Z(z)|z\rangle\langle z|. \qquad (13)$$

Using the inequality $\min(ab) \leq a^s b^{1-s}$, where $0 \leq s \leq 1$ (details see in [4, 14]), we obtain

$$\overline{P_{\text{err}}(N = 2^{nR})} \leq 2(N-1)^s\text{Tr}(\overline{\rho_x}^{1+s})^{\otimes n}\text{Tr}(\overline{\rho_z}^{1+s})^{\otimes n}$$

$$\leq 2\max_{0\leq s\leq 1}2^{-n(\max_s\{-\log[\text{Tr}(\overline{\rho_x}^{1+s})]\} - \log\text{Tr}(\overline{\rho_z}^{1+s}) - R)}, \qquad (14)$$

where R is the number of bits of information generated by the classical source per message. If only typical sequences are taken into account, then $R = H(X)$; if all sequences are considered, then $R = \log m$.

Since $-\log[\text{Tr}(\overline{\rho_x}^{1+s}]$ and $-\log[\text{Tr}(\overline{\rho_z}^{1+s})]$ are upward-convex functions of s and

$$\frac{1}{ds}\{-\log[\text{Tr}(\overline{\rho_x}^{1+s})]\}_{s=0} = H(\overline{\rho}_x),$$

$$\frac{1}{ds}\{-\log[\text{Tr}(\overline{\rho_z}^{1+s})]\}_{s=0} = H(\overline{\rho}_z), \qquad (15)$$

at $H(\overline{\rho}_x) + H(\overline{\rho}_z) > R$, the decoding error probability approaches zero with an increase in n.

In other words, if the entropy of the initial classical source R and quantum states are specified, the minimum amount of side classical information $H(\overline{\rho}_z)$ necessary for the receiver sequences having access only to side quantum and side classical information to be able to distinguish all classical sequences is

$$H(\overline{\rho}_z) > R - H(\overline{\rho}_x). \qquad (16)$$

According to the above consideration, the particular type of source of additional side classical information is insignificant. Only the entropy of the source is important.

S.N.M. is grateful to D.A. Kronberg for stimulating discussions.

REFERENCES

1. C. E. Shannon, Bell Syst. Tech. J. **27**, 397 (1948); Bell Syst. Tech. J. *27*, 623 (1948).
2. A. S. Holevo, *Quantum Systems, Channels, Information* (MTsMO, Moscow, 2010) [in Russian].
3. A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973); Probl. Inf. Transm. **15**, 247 (1979).
4. A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); A. S. Kholevo, Usp. Mat. Nauk **53**, 193 (1998).
5. B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
6. B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
7. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
8. Y.-Ho. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).
9. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
10. D. Slepian and J. K. Wolf, IEEE Trans. Inf. Theory **19**, 471 (1973).
11. I. Devetak and A. Winter, quant-ph/0209029.
12. J. M. Renes and R. Renner, quant-ph/1008.0452.
13. T. Ogawa and H. Nagaoka, quant-ph/9808063.
14. X. Zhan, *Matrix Inequalities*, Lecture Notes in Mathematics, Ed. by J.-M. Morel, F. Takens, and B. Teissier (Springer, Berlin, 2002), Vol. 1790.

Translated by R. Tyapaev

SPELL: OK