Optimal dense coding with mixed state entanglement

2001 J. Phys. A: Math. Gen. 34 6907

(http://iopscience.iop.org/0305-4470/34/35/316)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 6907–6912 PII: S0305-4470(01)18237-5

Optimal dense coding with mixed state entanglement

Tohya Hiroshima

Fundamental Research Laboratories, NEC Corporation, 34 Miyukigaoka, Tsukuba 305-8501, Japan

E-mail: tohya@frl.cl.nec.co.jp

Received 20 October 2000
Published 24 August 2001

Abstract
I investigate dense coding with a general mixed state on the Hilbert space $C^d \otimes C^d$ shared between a sender and receiver. The following result is proved. When the sender prepares the signal states by mutually orthogonal unitary transformations with equal *a priori* probabilities, the capacity of dense coding is maximized. It is also proved that the optimal capacity of dense coding χ^* satisfies $E_R(\rho) \leqslant \chi^* \leqslant E_R(\rho) + \log_2 d$, where $E_R(\rho)$ is the relative entropy of entanglement of the shared entangled state.

PACS numbers: 03.67.−a, 03.67.Hk, 89.70.+c

1. Introduction

Quantum entanglement plays an essential role in various types of quantum information processing. A notable example is the dense coding (sometimes called superdense coding) originally proposed by Bennett and Wiesner [1]. Its scheme is as follows. Suppose that the sender (Alice) and receiver (Bob) initially share a maximally entangled pair of qubits (an Einstein–Podolsky–Rosen (EPR) state), $|\Psi^-\rangle = (|\uparrow\rangle_A |\downarrow\rangle_B - |\downarrow\rangle_A |\uparrow\rangle_B)/\sqrt{2}$, where $|\uparrow\rangle_{A(B)} = (1,0)^t$ and $|\downarrow\rangle_{A(B)} = (0,1)^t$. Alice performs one of four possible unitary transformations $\{\mathbf{I}_2, \sigma_1, \sigma_2, \sigma_3\}$ on her qubit, where $\mathbf{I}_2$ stands for the two-dimensional identity and σ_i $(i = 0, 1, 2, 3)$ are the Pauli matrices. According to her choice of transformations, the EPR state is transformed into one of four mutually orthogonal states $\{|\Psi^-\rangle, -|\Phi^-\rangle, \sqrt{-1}|\Phi^+\rangle, |\Psi^+\rangle\}$, where $|\Psi^+\rangle = (|\uparrow\rangle_A |\downarrow\rangle_B + |\downarrow\rangle_A |\uparrow\rangle_B)/\sqrt{2}$ and $|\Phi^\pm\rangle = (|\uparrow\rangle_A |\uparrow\rangle_B \pm |\downarrow\rangle_A |\downarrow\rangle_B)/\sqrt{2}$. Now she sends off her qubit to Bob, who performs an orthogonal measurement on the joint system of the received qubit and his original one. The measured outcome unambiguously distinguishes the signal state that Alice prepared. Thus, sending a *single* qubit transmits $\log_2 4 = 2$ bits of classical information. This is absolutely impossible without entanglement; the amount of information conveyed by an *isolated* qubit cannot exceed one bit. Mattle *et al* [2] have experimentally demonstrated dense coding transmission using polarization-entangled photons. Barenco and Ekert [3] and Hausladen *et al* [4] have argued about the generalization of two-state systems in the Bennett–Wiesner dense coding scheme to *N*-state quantum systems. Dense coding for continuous variables has also been proposed by Braunstein and Kimble [5]. Bose *et al* [6] have shown that equal probabilities for the signal states yield the maximum capacity when the initially shared entangled states of two qubits are pure states or Bell diagonal states under the condition that the set of unitary transformations is restricted to $\{\mathbf{I}_2, \sigma_1, \sigma_2, \sigma_3\}$. However, when the shared entangled state is a general mixed one, the optimal dense coding scheme is still unknown. In this paper, I prove that the dense coding scheme with the set of mutually orthogonal unitary transformations and equal signal probabilities is optimal for any entangled states in $C^d \otimes C^d$ shared between the sender and receiver.

2. Capacity for dense coding

The general density matrix for a system on $C^d \otimes C^d$ is written in the Hilbert–Schmidt representation as

$$\rho = \frac{1}{d^2}\left(\mathbf{I}_d \otimes \mathbf{I}_d + \sum_{i=1}^{d^2-1} r_i \lambda_i \otimes \mathbf{I}_d + \mathbf{I}_d \otimes \sum_{i=1}^{d^2-1} s_i \lambda_i + \sum_{i,j=1}^{d^2-1} t_{ij} \lambda_i \otimes \lambda_j\right) \tag{1}$$

where r_i, s_i, and t_{ij} are real numbers. In equation (1) the λ_i $(i = 1, 2, \ldots, d^2 - 1)$ are the generators of $SU(d)$ algebra satisfying

$$\mathrm{Tr}\,(\lambda_i) = 0. \tag{2}$$

The generators λ_i are given by [7]

$$\{\lambda_i\}_{i=1}^{d^2-1} = \{u_{1,2}, u_{1,3}, \ldots, u_{d-1,d}, v_{1,2}, v_{1,3}, \ldots, v_{d-1,d}, w_1, w_2, \ldots, w_{d-1}\} \tag{3}$$

where

$$u_{i,j} = P_{i,j} + P_{j,i} \tag{4}$$

and

$$v_{i,j} = \sqrt{-1}(P_{i,j} - P_{j,i}) \tag{5}$$

with $1 \leqslant i < j \leqslant d$, and

$$w_k = -\sqrt{\frac{2}{k(k+1)}}\left(\sum_{i=1}^{k} P_{i,i} - kP_{k+1,k+1}\right) \tag{6}$$

with $1 \leqslant k \leqslant d - 1$. In equations (4)–(6),

$$P_{i,j} = |i\rangle\,\langle j| \tag{7}$$

with $\{|i\rangle\}_{i=1}^{d}$ being the orthonormal basis set on C^d; $|1\rangle = (1, 0, \ldots, 0)^t$, $|2\rangle = (0, 1, \ldots, 0)^t, \ldots, |d\rangle = (0, 0, \ldots, 1)^t$.

In general dense coding, Alice performs one of the local unitary transformations $U_i \in U(d)$ on her d-dimensional quantum system to put the initially shared entangled state ρ in $\rho_i = (U_i \otimes \mathbf{I}_d)\rho(U_i^\dagger \otimes \mathbf{I}_d)$ with *a priori* probability $p_i (i = 0, 1, \ldots, i_{\max})$, and then she sends off her quantum system to Bob. Upon receiving this quantum system, Bob performs a suitable measurement on ρ_i to extract the signal. The optimal amount of information that can be conveyed is known to be bounded from above by the Holevo quantity [8]

$$\chi = S(\overline{\rho}) - \sum_{i=0}^{i_{\max}} p_i S(\rho_i) \tag{8}$$

where $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$ denotes the von Neumann entropy and $\overline{\rho} = \sum_{i=0}^{i_{\max}} p_i \rho_i$ is the average density matrix of the signal ensemble. Since the Holevo quantity is asymptotically achievable [9, 10], I use equation (8) here as the definition of the capacity of dense coding as in [4, 6]. Since the von Neumann entropy is invariant under unitary transformations, $S(\rho_i) = S(\rho)$. Therefore, the dense coding capacity χ of equation (8) can be rewritten as

$$\chi = S(\overline{\rho}) - S(\rho). \tag{9}$$

It is also written as

$$\chi = \sum_{i=0}^{i_{\max}} p_i S(\rho_i \| \overline{\rho}) \tag{10}$$

where $S(\rho\|\sigma) = \mathrm{Tr}\,[\rho(\log_2 \rho - \log_2 \sigma)]$ is the quantum relative entropy of ρ with respect to σ.

3. Optimal capacity

The problem is to find the optimal signal ensemble $\{\rho_i;\, p_i\}_{i=0}^{i_{\max}}$ that maximizes χ. Below I show that the d^2 signal states ($i_{\max} = d^2 - 1$) generated by mutually orthogonal unitary transformations with equal probabilities yield the maximum χ. This is the central result of this paper. The mutually orthogonal unitary transformations are constructed as

$$U_{i=(p,q)}|j\rangle = \exp\left(\sqrt{-1}\frac{2\pi}{d}pj\right)|j + q(\mathrm{mod}\, d)\rangle \tag{11}$$

where integers p and q run from 0 to $d-1$ such that the number of suffices i is d^2; $0 = (p = 0, q = 0)$, $1 = (p = 0, q = 1), \ldots, d^2 - 1 = (p = d-1, q = d-1)$. Note that $U_{i=0} = \mathbf{I}_d$. The unitary matrices thus defined satisfy the orthogonality relation, $d^{-1}\mathrm{Tr}\,(U_i^\dagger U_j) = \delta_{ij}$. From now on, the ensemble of signal states generated by the unitary transformations of equation (11) with the equal probabilities $p_i = d^{-2}$ is denoted $\mathcal{E}^*$:

$$\mathcal{E}^* = \left\{(U_i \otimes \mathbf{I}_d)\rho(U_i^\dagger \otimes \mathbf{I}_d);\ p_i = d^{-2}\right\}_{i=0}^{d^2-1}. \tag{12}$$

Furthermore, the capacity of dense coding with signal state ensemble $\mathcal{E}^*$ is denoted χ^*, which is given by $S(\overline{\rho}^*) - S(\rho)$, where $\overline{\rho}^* = d^{-2}\sum_{i=0}^{d^2-1}(U_i \otimes \mathbf{I}_d)\rho(U_i^\dagger \otimes \mathbf{I}_d)$ is the average state of $\mathcal{E}^*$. In verifying the main result (theorem 1), the following three lemmas are crucial.

Lemma 1. *The average state of* $\mathcal{E}^*$ *is separable and is given by*

$$\overline{\rho}^* = \frac{1}{d}\mathbf{I}_d \otimes \rho^B \tag{13}$$

where $\rho^B = \mathrm{Tr}_A(\rho)$.

Proof. It is easy to show that

$$\sum_{i=0}^{d^2-1} U_i P_{j,k} U_i^\dagger = \delta_{jk} d\mathbf{I}_d \tag{14}$$

where $P_{j,k}$ is defined in equation (7). Applying equation (14) to the definition of λ_j (equation (3) with equations (4)–(6)), we have

$$\sum_{i=0}^{d^2-1} U_i \lambda_j U_i^\dagger = 0 \tag{15}$$

for $j = 1, \ldots, d^2 - 1$. Making use of equation (15), $\overline{\rho}^*$ is calculated as

$$\overline{\rho}^* = \frac{1}{d^2}\sum_{i=0}^{d^2-1}(U_i \otimes \mathbf{I}_d)\rho(U_i^\dagger \otimes \mathbf{I}_d) = \frac{1}{d}\mathbf{I}_d \otimes \frac{1}{d}\left(\mathbf{I}_d + \sum_{i=1}^{d^2-1} s_i\lambda_i\right). \tag{16}$$

This is clearly separable or disentangled. By noting that $\rho^B = \mathrm{Tr}_A(\rho) = d^{-1}(\mathbf{I}_d + \sum_{i=1}^{d^2-1} s_i\lambda_i)$, we readily obtain equation (13). □

Lemma 2. *For any state ω written as $(U \otimes \mathbf{I}_d)\rho(U^\dagger \otimes \mathbf{I}_d)$ with $U \in U(d)$, the quantum relative entropy of ω with respect to $\overline{\rho}^*$ is equal to χ^*;*

$$S(\omega\|\overline{\rho}^*) = \chi^*. \tag{17}$$

Proof. The density matrix ρ of equation (1) is rewritten as

$$\rho = \frac{1}{d}\mathbf{I}_d \otimes \rho^B + \frac{1}{d^2}\left(\sum_{i=1}^{d^2-1} r_i\lambda_i \otimes \mathbf{I}_d + \sum_{i,j=1}^{d^2-1} t_{ij}\lambda_i \otimes \lambda_j\right). \tag{18}$$

Therefore,

$$\begin{aligned}\omega &= (U \otimes \mathbf{I}_d)\rho(U^\dagger \otimes \mathbf{I}_d)\\ &= \frac{1}{d}\mathbf{I}_d \otimes \rho^B + \frac{1}{d^2}\left[\sum_{i=1}^{d^2-1} r_i(U\lambda_iU^\dagger) \otimes \mathbf{I}_d + \sum_{i,j=1}^{d^2-1} t_{ij}(U\lambda_iU^\dagger) \otimes \lambda_j\right]. \end{aligned}\tag{19}$$

Now, from the result of lemma 1,

$$\log_2 \overline{\rho}^* = \mathbf{I}_d \otimes \log_2\left(\frac{\rho^B}{d}\right). \tag{20}$$

From equations (19) and (20),

$$\begin{aligned}\mathrm{Tr}\,(\omega \log_2 \overline{\rho}^*) = \mathrm{Tr}\,(\overline{\rho}^* \log_2 \overline{\rho}^*) + \frac{1}{d^2}\Bigg\{&\sum_{i=1}^{d^2-1} r_i \mathrm{Tr}\left[(U\lambda_iU^\dagger) \otimes \log_2\left(\frac{\rho^B}{d}\right)\right]\\ &+ \sum_{i,j=1}^{d^2-1} t_{ij}\,\mathrm{Tr}\left[(U\lambda_iU^\dagger) \otimes \lambda_j \log_2\left(\frac{\rho^B}{d}\right)\right]\Bigg\}. \end{aligned}\tag{21}$$

By using the formula $\mathrm{Tr}(A \otimes B) = \mathrm{Tr}(A)\mathrm{Tr}(B)$ and the properties of λ_i of equation (2), the last term of the right-hand side of equation (21) vanishes; $\mathrm{Tr}(\omega \log_2 \overline{\rho}^*) = \mathrm{Tr}(\overline{\rho}^* \log_2 \overline{\rho}^*) = -S(\overline{\rho}^*)$. We thus obtain

$$\begin{aligned}S(\omega\|\overline{\rho}^*) &= \mathrm{Tr}\,[\omega(\log_2 \omega - \log_2 \overline{\rho}^*)]\\ &= -S(\omega) + S(\overline{\rho}^*) = -S(\rho) + S(\overline{\rho}^*). \end{aligned}\tag{22}$$

In the last line of equation (22), the equality $S(\omega) = S(\rho)$ was used. Since $\chi^* = S(\overline{\rho}^*) - S(\rho)$, $S(\omega\|\overline{\rho}^*) = \chi^*$. This completes the proof. □

Lemma 3. *The average quantum relative entropy of signal ensemble $\{\rho_k; p_k\}$ with respect to a density matrix ρ' is given by*

$$\sum_k p_k S(\rho_k\|\rho') = \sum_k p_k S(\rho_k\|\overline{\rho}) + S(\overline{\rho}\|\rho') \tag{23}$$

where $p_k \geqslant 0$, $\sum_k p_k = 1$, and $\overline{\rho} = \sum_k p_k\rho_k$.

Equation (23) is known as Donald's identity [11].

Theorem 1. *The dense coding capacity* χ^* *is maximum. That is, for all possible signal ensembles* $\{\omega_i; q_i\}_{i=0}^{i_{\max}}$,

$$\chi^* \geqslant \sum_{i=0}^{i_{\max}} q_i S(\omega_i \| \bar{\omega}) \tag{24}$$

where $\bar{\omega} = \sum_{i=0}^{i_{\max}} q_i \omega_i$.

Proof. Since $S(\omega_i \| \bar{\rho}^*) = \chi^*$ for $i = 0, 1, \ldots, i_{\max}$ (lemma 2),

$$\chi^* = \sum_{i=0}^{i_{\max}} q_i S(\omega_i \| \bar{\rho}^*). \tag{25}$$

Applying Donald's identity (23) of lemma 3 to the right-hand side of equation (25), we obtain $\chi^* = \chi + S(\bar{\omega} \| \bar{\rho}^*)$, where $\chi = \sum_{i=0}^{i_{\max}} q_i S(\omega_i \| \bar{\omega})$, the dense coding capacity with ensemble $\{\omega_i; q_i\}_{i=0}^{i_{\max}}$. Since the relative entropy is strictly non-negative, $S(\bar{\omega} \| \bar{\rho}^*) \geqslant 0$, $\chi^* \geqslant \chi$. That is, χ^* is indeed the optimal dense coding capacity; i.e., $\mathcal{E}^*$ is the optimal signal ensemble. This completes the proof. □

Equation (17) means that the average ensemble $\bar{\rho}^*$ has the *maximal distance property* [13]; that is, $S(\omega \| \bar{\rho}^*)$ cannot exceed χ^* for any $\omega = (U \otimes \mathbf{I}_d)\rho(U^\dagger \otimes \mathbf{I}_d)$. Theorem 1 is also the direct consequence of this fact. Note that the optimal dense coding scheme for $d = 2$ is reduced to Bennett and Wiesner's scheme.

4. Bounds on optimal capacity

Next, I prove the following theorem concerning the bounds on χ^*.

Theorem 2. *The optimal capacity* χ^* *satisfies*

$$E_R(\rho) \leqslant \chi^* \leqslant E_R(\rho) + \log_2 d \tag{26}$$

where $E_R(\rho)$ *is the relative entropy of entanglement of* ρ.

The relative entropy of entanglement is defined as $E_R(\rho) = \min_{\sigma \in \mathcal{D}} S(\rho \| \sigma)$, where the minimum is taken over $\mathcal{D}$, the set of all disentangled states [12]. The proof of the first inequality of equation (26) is essentially the same as that given in [6] for $d = 2$. By noting that $\bar{\rho}^*$ is a disentangled state (lemma 1), we get

$$S(\rho_i \| \bar{\rho}^*) \geqslant \min_{\sigma \in \mathcal{D}} S(\rho_i \| \sigma) = E_R(\rho_i). \tag{27}$$

Consequently,

$$\chi^* = \frac{1}{d^2} \sum_{i=0}^{d^2-1} S(\rho_i \| \bar{\rho}^*) \geqslant \frac{1}{d^2} \sum_{i=0}^{d^2-1} E_R(\rho_i). \tag{28}$$

Since the relative entropy of entanglement is invariant under local unitary operations [12], $E_R(\rho_i) = E_R[(U_i \otimes \mathbf{I}_d)\rho(U_i^\dagger \otimes \mathbf{I}_d)] = E_R(\rho)$. Therefore, $\chi^* \geqslant E_R(\rho)$. The second part of the inequality in (26) for $d = 2$ has been conjectured previously in [6]. In the proof of this inequality, the following relation given by Plenio *et al* [14]

$$\max\{S(\rho^A) - S(\rho), S(\rho^B) - S(\rho)\} \leqslant E_R(\rho) \tag{29}$$

plays a key role. It implies that

$$S(\rho^B) - S(\rho) \leqslant E_R(\rho). \tag{30}$$

Now, from equations (13) and (20), we have

$$\begin{aligned} S(\overline{\rho}^{*}) &= -\mathrm{Tr}\,(\overline{\rho}^{*}\log_2\overline{\rho}^{*}) \\ &= -\mathrm{Tr}\left[\left(\mathbf{I}_d\otimes\frac{\rho^B}{d}\right)\left(\mathbf{I}_d\otimes\log_2\frac{\rho^B}{d}\right)\right] \\ &= -\mathrm{Tr}\,(\mathbf{I}_d)\mathrm{Tr}\left(\frac{\rho^B}{d}\log_2\frac{\rho^B}{d}\right) = S(\rho^B) + \log_2 d. \end{aligned} \tag{31}$$

In the last line of equation (31), the fact that Tr $(\rho^B) = 1$ was used. Substituting equation (31) into the left-hand side of (30), we readily obtain

$$S(\overline{\rho}^{*}) - S(\rho) \leqslant E_R(\rho) + \log_2 d. \tag{32}$$

Since the left-hand side of (32) is just χ^*, we have $\chi^* \leqslant E_R\,(\rho) + \log_2 d$. For $d = 2$, it has been proved that the equality holds when ρ is the Bell diagonal state with only two non-zero eigenvalues [6].

5. Conclusions

In summary, it has been proved that optimal dense coding with a general entangled state on the Hilbert space $C^d \otimes C^d$ is achieved when the sender prepares the signal states by mutually orthogonal unitary transformations with equal *a priori* probabilities. It is also proved that the optimal capacity of dense coding χ^* satisfies $E_R(\rho) \leqslant \chi^* \leqslant E_R(\rho) + \log_2 d$, where $E_R\,(\rho)$ is the relative entropy of entanglement of the shared entangled state.

References

[1] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[2] Mattle K, Weinfurter H, Kwiat P G and Zeilinger A 1996 *Phys. Rev. Lett.* **76** 4656
[3] Barenco A and Ekert A 1995 *J. Mod. Opt.* **42** 1253
[4] Hausladen P, Jozsa R, Schumacher B, Westmoreland M and Wootters W K 1996 *Phys. Rev.* A **54** 1869
[5] Braunstein S L and Kimble H J 2000 *Phys. Rev.* A **61** 042302
[6] Bose S, Plenio M B and Vedral V 2000 *J. Mod. Opt.* **47** 291
[7] Schlienz J and Mahler G 1995 *Phys. Rev.* A **52** 4396
[8] Kholevo A S 1973 *Probl. Peredachi Inf.* **9** 3
(Engl. transl. 1973 *Probl. Inf. Transm. (USSR)* **9** 110)
[9] Holevo A S 1998 *IEEE Trans. Inf. Theory* **44** 269
[10] Schumacher B and Westmoreland M D 1997 *Phys. Rev.* A **56** 131
[11] Donald M J 1987 *Math. Proc. Camb. Phil. Soc.* **101** 363
[12] Vedral V and Plenio M B 1998 *Phys. Rev.* A **57** 1619
[13] Schumacher B and Westmoreland M D 2001 *Phys. Rev.* A **63** 022308
Schumacher B and Westmoreland M D 2000 *Preprint* quant-ph/0004045
[14] Plenio M B, Virmani S and Papadopoulos P 2000 *J. Phys. A: Math. Gen.* **33** L193