Classical information capacity of superdense coding

Garry Bowen*
Department of Physics, Australian National University, Canberra, Australian Capital Territory 0200, Australia

(Received 9 August 2000; published 10 January 2001)

Classical communication through quantum channels may be enhanced by sharing entanglement. Superdense coding allows the encoding, and transmission, of up to two classical bits of information in a single qubit. In this paper, the maximum classical channel capacity for states that are not maximally entangled is derived. Particular schemes are then shown to attain this capacity, first for pairs of qubits, and second for pairs of qutrits.

DOI: 10.1103/PhysRevA.63.022302 PACS number(s): 03.67.Hk

Quantum information exhibits many features that do not have analogs in classical information theory [1]. For this reason, when a quantum channel is used for communication, there exist a number of different capacities for the different types of information transmitted through the channel [2–5].

Superdense coding (referred to in this paper simply as dense coding), first proposed by Bennett and Wiesner [6], is where the transmission of classical information through a quantum channel is enhanced by shared entanglement between sender and receiver. The classical information capacity for a channel where sender and receiver share entanglement has been called the *entanglement-assisted classical capacity* C_E [5]. The classical capacity for dense coding, denoted here by C, provides a lower bound on C_E.

For completely general dense coding (CGDC) [7], the sender Alice and receiver Bob share qubits in the state ρ_{AB}. Alice may encode a message using a set of unitary transformations $\{U_A^k\}$, with *a priori* probabilities $\{p_k\}$, on her qubit. Alice then sends her qubit to Bob, who decodes the message by doing joint measurements on both qubits.

For pure states of pairs of D state systems, where $\rho_{AB} = |\Psi_{AB}\rangle\langle\Psi_{AB}|$, the channel capacity has been derived by both Hausladen *et al.* [8] and by Barenco and Ekert [9], and was shown to be $C = \log D + S(\rho_B)$. Here S is the von Neumann entropy $S(\rho) = -\mathrm{Tr}\,\rho\log\rho$, where the logarithm is base 2.

Bose, Plenio, and Vedral [7] have further proven that if Alice's alphabet of operators is restricted to the set of the identity and three Pauli matrices, $U_A^k \in \{I, \sigma_x, \sigma_y, \sigma_z\}$, then the capacity for a pair of qubits is maximized by setting $p_k = 1/4$. This scheme was labeled by the authors as special dense coding (SDC).

In this paper, a bound on the channel capacity for dense coding is derived for arbitrary sets of unitary operators on pairs of qubits. It is shown that the scheme of SDC attains that bound. Further, the proof for the case of pairs of qutrits is outlined, utilizing the higher dimensional analog of SDC.

Suppose Alice and Bob share pairs of qubits in the state ρ_{AB}, and Alice is restricted to using unitary operators and sending her message as a product state of letters, then the maximal amount of classical information that may be transferred is given by the Kholevo bound [10],

$$C = \max_{\{U_A^k, p_k\}} \left[S\left(\sum_k p_k (U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dagger \right) - \sum_k p_k S((U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dagger) \right]. \tag{1}$$

This bound has been shown to be asymptotically attainable by using product state block coding [8,11].

As the operators $U_A^k \otimes I_B$ are unitary, applying one of the operators to ρ_{AB} will not change the eigenvalues. Hence the entropy, which depends only on the eigenvalues, of each summand in the second term of Eq. (1) remains unchanged, and the second term reduces to $S(\rho_{AB})$. To maximize the capacity we must therefore maximize the first term,

$$S(\rho'_{AB}) = S\left(\sum_k p_k (U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dagger \right). \tag{2}$$

A general density matrix of a two qubit bipartite system may be expanded as

$$\rho_{AB} = \sum_{ij} \lambda_{ij} \sigma_A^i \otimes \sigma_B^j, \tag{3}$$

where the σ's consist of a scaled version of the set of Pauli matrices and the identity, that is,

$$\sigma^0 = \frac{1}{2} I_2 = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{4}$$

$$\sigma^1 = \frac{1}{2} \sigma_x = \frac{1}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{5}$$

$$\sigma^2 = \frac{1}{2} \sigma_y = \frac{1}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{6}$$

$$\sigma^3 = \frac{1}{2} \sigma_z = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{7}$$

By linearity we can obtain the reduced density matrices of ρ_{AB} and ρ'_{AB} by tracing over the expansions

*Present address: Centre for Quantum Computation, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, United Kingdom.

$$\rho_B=\mathrm{Tr}_A[\rho_{AB}] \tag{8}$$

$$=\mathrm{Tr}_A\left[\sum_{ij}\lambda_{ij}\sigma_A^i\otimes\sigma_B^j\right] \tag{9}$$

$$=\sum_{ij}\lambda_{ij}\mathrm{Tr}_A[\sigma_A^i]\sigma_B^j \tag{10}$$

$$=\sum_j\lambda_{0j}\sigma_B^j, \tag{11}$$

where the trace of each of the Pauli matrices is zero. Also,

$$\rho_B'=\mathrm{Tr}_A\left[\sum_k p_k(U_A^k\otimes I_B)\rho_{AB}(U_A^k\otimes I_B)^\dagger\right] \tag{12}$$

$$=\sum_{ij}\lambda_{ij}\sum_k p_k\mathrm{Tr}_A[U_A^k\sigma_A^i(U_A^k)^\dagger]\sigma_B^j \tag{13}$$

$$=\sum_j\lambda_{0j}\sigma_B^j \tag{14}$$

$$=\rho_B, \tag{15}$$

using the fact that the trace of a matrix does not change under unitary transformations.

Combining the above derivations leads to the main result of this paper. The amount of information that may be transferred for any $\{U_A^k,p_k\}$ using an arbitrary, two qubit mixed state ρ_{AB} is given by

$$C=S\left(\sum_k p_k(U_A^k\otimes I_B)\rho_{AB}(U_A^k\otimes I_B)^\dagger\right)$$

$$-\sum_k p_kS((U_A^k\otimes I_B)\rho_{AB}(U_A^k\otimes I_B)^\dagger) \tag{16}$$

$$=S(\rho_{AB}')-S(\rho_{AB}) \tag{17}$$

$$\leqslant S(\rho_A')+S(\rho_B')-S(\rho_{AB}) \tag{18}$$

$$\leqslant\log 2+S(\rho_B)-S(\rho_{AB}). \tag{19}$$

Here, Eq. (17) follows from the discussion following Eq. (1), and the first term is rewritten as for Eq. (2). Equation (18) uses the subadditivity of the entropies of a bipartite system, and Eq. (19) follows from the relations $S(\rho_B')=S(\rho_B)$, by Eq. (15), and the bound $S(\rho_A')\leqslant\log 2$ for a qubit.

This bound is attainable using special dense coding, where Alice uses the operators $U_A^k=2\sigma_A^k$, each occurring with *a priori* probability $p_k=1/4$. Using this scheme, the state received by Bob is completely disentangled, that is,

$$\rho_{AB}'=\sum_k p_kU_A^k\left(\sum_{ij}\lambda_{ij}\sigma_A^i\otimes\sigma_B^j\right)(U_A^k)^\dagger \tag{20}$$

$$=\sum_{ij}\lambda_{ij}\left(\sum_k\sigma_A^k\sigma_A^i\sigma_A^k\right)\otimes\sigma_B^j \tag{21}$$

$$=\sum_j\lambda_{0j}\sigma_A^0\otimes\sigma_B^j \tag{22}$$

$$=\frac{1}{2}I_A\otimes\rho_B, \tag{23}$$

where Eq. (22) follows from Eq. (21) due to the relationship $\sigma^j\sigma^i\sigma^j=\frac{1}{2}\delta_{ij}\sigma^j-\frac{1}{4}\sigma^i=\pm\frac{1}{4}\sigma^i$ for $i,j\in\{1,2,3\}$, and Eq. (23) is obtained by comparing Eq. (22) with Eq. (11). Thus, the capacity for SDC is equal to the bound given in Eqs. (16)–(19), and SDC has been shown to be an optimal method for CGDC.

A similar result applies for two qutrits, where Alice uses the operators

$$U_0=\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, \tag{24}$$

$$U_1=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, \tag{25}$$

$$U_2=\begin{pmatrix}1&0&0\\0&e^{i2\pi/3}&0\\0&0&e^{i4\pi/3}\end{pmatrix}, \tag{26}$$

$$U_3=\begin{pmatrix}1&0&0\\0&e^{i4\pi/3}&0\\0&0&e^{i2\pi/3}\end{pmatrix}, \tag{27}$$

$$U_4=-\frac{i}{\sqrt{3}}[U_0,U_2], \tag{28}$$

$$U_5=\frac{i}{\sqrt{3}}[U_0,U_3], \tag{29}$$

$$U_6=\frac{i}{\sqrt{3}}[U_1,U_2], \tag{30}$$

$$U_7=-\frac{i}{\sqrt{3}}[U_1,U_3], \tag{31}$$

$$U_8=I_3, \tag{32}$$

with *a priori* probability $p_j=1/9$, where $[U_i,U_j]$ denotes the commutator. Expanding the density matrix ρ_{AB} in terms of the identity and the traceless Hermitian generators $\{\lambda_i\}$ of SU(3) [12], we find

$$\rho'_{AB}=\sum_j p_j U_j \rho_{AB} U_j^\dagger \qquad (33)$$

$$=\frac{1}{3}I_3\otimes\rho_B, \qquad (34)$$

and the capacity is given by

$$C=\log 3+S(\rho_B)-S(\rho_{AB}). \qquad (35)$$

Similar constructions for arbitrary $N\times M$ state systems may easily be considered using analogs of the unitary transformations used in SDC. The transformations consist of the set of cyclic permutations of the D_A basis states of $\mathcal{H}_A$, where D_A is the dimension of the Hilbert space $\mathcal{H}_A$ of Alice's state, the set of unitary matrices derived from the cyclic group generated by the matrix consisting of the D_A roots of unity on the diagonal (up to overall phase), and the normalized commutators between elements of these two sets of transformations. The connection between sets of unitary depolarizers, the existence of orthonormal bases of maximally entangled states, and dense coding have previously been noted by Werner [13].

We thus make the conjecture that, for an $N\times M$ state system ρ_{AB}, the dense coding capacity is given by

$$C=\log D_A+S(\rho_B)-S(\rho_{AB}), \qquad (36)$$

with $D_A=N$.

The result obtained in this paper agrees with the previously obtained results in the case of pure states. The capacity may also be rewritten in the form

$$C(\rho_{AB})=\log D_A-S(\rho_A)+S(\rho_A)+S(\rho_B)-S(\rho_{AB}) \qquad (37)$$

$$=C(\rho_A)+S(A,B), \qquad (38)$$

for $C(\rho_A)$, the capacity of sending qubit A without access to qubit B, and $S(A,B)=S(\rho_A)+S(\rho_B)-S(\rho_{AB})$, the von Neumann mutual entropy of ρ_{AB}. In this way it is shown that the capacity due to the joint measurement of both qubits is enhanced over the use of a single qubit by a factor equal to the von Neumann mutual entropy of the combined state.

The capacity also gives an exact bound on the mixedness of a state for when dense coding with that state may be said to fail [14]. For an arbitrary bipartite state the capacity will not exceed $\log N$, for an $N\times M$ state system, with $N,M\in\{2,3\}$, whenever $S(\rho_B)-S(\rho_{AB})\leqslant 0$. Disentangled states [15] satisfy the inequality

$$S(\rho_{AB})\geqslant\max\{S(\rho_A),S(\rho_B)\}, \qquad (39)$$

and therefore cannot be used to transmit more than $\log N$ bits per state. The proof of Eq. (39) is given in the Appendix.

It may also be noted [16] that the result for the capacity of a two qubit system also proves the conjecture that the capacity for dense coding is bounded by [7]

$$C\leqslant 1+E_D, \qquad (40)$$

where E_D is the (one way) distillable entanglement of ρ_{AB}, provided the Hashing inequality [17] $E_D\geqslant S(\rho_B)-S(\rho_{AB})$ is true.

In summary, the classical information capacity of dense coding, through a noiseless channel, using arbitrary mixed states of two qubits or two qutrits, has been derived. A method of generalizing to $N\times M$ state systems has been outlined, and a conjecture made about the classical capacity of dense coding using such systems.

The author would like to thank Craig Savage and Tim Ralph for discussions. The author was supported by the DETYA.

APPENDIX

Proof of Eq. (39). Suppose ρ_{AB} is disentangled, then the density matrix may be written in the form $\rho_{AB}=\Sigma_i p_i\omega_A^i\otimes\omega_B^i$, with $\Sigma_i p_i=1$ and $p_i>0$, where the reduced density matrices ω^i are all pure states. By the convexity of the expression $S(\rho_B)-S(\rho_{AB})$ [18], we have

$$S(\rho_B)-S(\rho_{AB})\leqslant\sum_i p_i S(\omega_B^i)-\sum_i p_i S(\omega_A^i\otimes\omega_B^i)=0,$$

and hence $S(\rho_{AB})\geqslant S(\rho_B)$. Similarly for $S(\rho_{AB})\geqslant S(\rho_A)$.

[1] C. H. Bennett and D. P. DiVincenzo, Nature (London) **404**, 247 (2000).

[2] H. Barnum, M. A. Nielsen, and B. Schumacher, Phys. Rev. A **57**, 4153 (1998).

[3] C. Adami and N. J. Cerf, Phys. Rev. A **56**, 3470 (1997).

[4] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).

[5] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).

[6] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[7] S. Bose, M. Plenio, and V. Vedral, J. Mod. Opt. **47**, 291 (2000).

[8] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).

[9] A. Barenco and A. K. Ekert, J. Mod. Opt. **42**, 1253 (1995).

[10] A. S. Kholevo, Probl. Peredachi Inf. **9**, 3 (1973) [Probl. Inf. Transm. **9**, 177 (1973)].

[11] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**,

131 (1997).

[12] C. M. Caves and G. J. Milburn, Opt. Commun. **179**, 439 (2000).

[13] R. F. Werner, e-print quant-ph/0003070.

[14] S. Bose and V. Vedral, Phys. Rev. A **61**, 040101(R) (2000).

[15] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[16] S. Bose (private communication).

[17] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **85**, 433 (2000).

[18] E. H. Lieb and M. B. Ruskai, J. Math. Phys. **14**, 1938 (1973).