Classical information capacity of superdense coding

Garry Bowen*
Department of Physics, Australian National University, Canberra, A.C.T. 0200, Australia.
(February 1, 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, firstly for pairs of qubits, and secondly for pairs of qutrits.

03.67.Hk

Quantum information exhibits many features which do not have analogues 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 $\rho_{AB}$. Alice may encode a message using a set of operators to 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, Barenco and Ekert [9], and was shown to be, $C = \log D + S(\rho_{AB})$. Here $S$ is the von Neumann entropy $S(\rho) = -\text{Tr}\rho\log\rho$, 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 analogue of SDC.

Suppose Alice and Bob share pairs of qubits in the state $\rho_{AB}$, 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)^\dag \right) ight] - \sum_k p_k S \left( (U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dag \right) \].$$

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 $\rho_{AB}$ 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,

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

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

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

where the $\sigma$’s consist of a scaled version of the set of Pauli matrices and the identity, that is,

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

(4)

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

(5)

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

(6)

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

(7)

By linearity we can obtain the reduced density matrices of $\rho_{AB}$ and $\rho'_{AB}$ by tracing over the expansions,
\( \rho_B = \text{Tr}_A[\rho_{AB}] \)
\[ = \text{Tr}_A \left[ \sum_{ij} \lambda_{ij} \sigma^i_A \otimes \sigma^j_B \right] \]
\[ = \sum_{ij} \lambda_{ij} \text{Tr}_A \left[ \sigma^i_A \right] \sigma^j_B \]
\[ = \sum_{j} \lambda_{0j} \sigma^j_B, \]
\[ \text{(9)} \]

where the trace of each of the Pauli matrices is zero. Also,
\[ \rho'_B = \text{Tr}_A \left[ \sum_k p_k (U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dagger \right] \]
\[ = \sum_{ij} \lambda_{ij} \sum_k p_k \text{Tr}_A \left[ U_A^k \sigma^i_A (U_A^k)^\dagger \right] \sigma^j_B \]
\[ = \sum_{j} \lambda_{0j} \sigma^j_B \]
\[ = \rho_B, \]
\[ \text{(12)} \]

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 the paper. The amount of information that may be transferred for any \( \{U_A^k, p_k\} \) using an arbitrary, two qubit mixed state \( \rho_{AB} \), is given by,
\[ C = S\left( \sum_k p_k (U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dagger \right) - \sum_k p_k S\left( (U_A^k \otimes I_B) \rho_{AB} (U_A^k \otimes I_B)^\dagger \right) \]
\[ = S(\rho'_B) - S(\rho_{AB}) \leq S(\rho'_A) + S(\rho'_B) - S(\rho_{AB}) \leq \log 2 + S(\rho_B) - S(\rho_{AB}). \]
\[ \text{(16)} \]

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

This bound is attainable using Special Dense Coding (SDC), 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,
\[ \rho'_{AB} = \sum_k p_k U_A^k \left( \sum_{ij} \lambda_{ij} \sigma^i_A \otimes \sigma^j_B \right) (U_A^k)^\dagger \]
\[ = \sum_{ij} \lambda_{ij} \left( \sum_k \sigma^i_A \sigma^j_B \right) \otimes \sigma^j_B \]
\[ = \sum_j \lambda_{0j} \sigma^j_B \]
\[ = \frac{1}{2} I_A \otimes \rho_B, \]
\[ \text{(20)} \]
where Eq. (22) follows from Eq. (21) due to the relationship \( \sigma^i \sigma^j = \frac{1}{2} \delta_{ij} \sigma^i - \frac{1}{2} \sigma^i = \pm \frac{1}{2} \sigma^i \), for \( i, j \in \{1, 2, 3\} \), and Eq. (23) is obtained by comparing Eq. (22) with Eq. (11).

A similar result applies for two qutrits, where Alice uses the operators,
\[ U_0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \]
\[ U_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \]
\[ U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\frac{\pi}{3}} & 0 \\ 0 & 0 & e^{i\frac{2\pi}{3}} \end{pmatrix}, \]
\[ U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\frac{\pi}{3}} & 0 \\ 0 & 0 & e^{i\frac{2\pi}{3}} \end{pmatrix}, \]
\[ \text{(24-27)} \]

with \( a_p \) priori probability \( p_j = 1/9 \), where \( [U_j, U_j] \) denotes the commutator. Expanding the density matrix \( \rho_{AB} \) in terms of the identity and the traceless Hermitian generators \( \{\lambda_i\} \) of \( SU(3) \) \[12\], we find,
\[ \rho'_{AB} = \sum_j p_j U_j \rho_{AB} U_j^\dagger \]
\[ = \frac{1}{3} I_A \otimes \rho_B, \]
\[ \text{(33-34)} \]

and the capacity is given by,
\[ C = \log 3 + S(\rho_B) - S(\rho_{AB}). \]
\[ \text{(35)} \]

Similar constructions for arbitrary \( N \times M \) state systems may easily be considered using analogues 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 has previously been noted by Werner [13].

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

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

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,

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

with $S(\rho_A) + S(\rho_B) = D_A$.

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 $\rho_{AB}$. 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 $S(\rho_B) - S(\rho_{AB}) \leq 0$. Disentangled states [15] satisfy the inequality,

$$S(\rho_{AB}) \geq \max\{S(\rho_A), S(\rho_B)\},$$

(39)

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

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],

$$C \leq 1 + E_D,$$

(40)

where $E_D$ is the (one way) distillable entanglement of $\rho_{AB}$, provided the Hashing Inequality [17], $E_D \geq S(\rho_B) - S(\rho_{AB})$, 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 is supported by the DETYA.

**APPENDIX A**

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

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

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