Probabilistic coding of quantum states

Andrzej Grudka, Antoni Wójcik, and Mikołaj Czechlewski
Faculty of Physics, Adam Mickiewicz University, Umultowska 85, 61-614 Poznań, Poland

(Received 27 March 2006; published 6 July 2006)

We discuss the properties of probabilistic coding of two qubits to one qutrit and generalize the scheme to higher dimensions. We show that the protocol preserves the entanglement between the qubits to be encoded and the environment and can also be applied to mixed states. We present a protocol that enables encoding of n qudits to one qudit of dimension smaller than the Hilbert space of the original system and then allows probabilistic but error-free decoding of any subset of k qudits. We give a formula for the probability of successful decoding.

DOI: 10.1103/PhysRevA.74.012302 PACS number(s): 03.67.Lx

I. INTRODUCTION

The pure state of a d-level quantum system is described by $2d-2$ real parameters. Thus the pure state of two nonentangled qubits is described by four real numbers, e.g., the Bloch sphere coordinates of each qubit. The same number of parameters specifies the state of one qutrit (a quantum system with three-dimensional Hilbert space). It is thus interesting to consider the possibility of encoding the states of two nonentangled qubits to one qutrit. The first constraint on such encoding is given by the Holevo bound [1], which states that using a d-dimensional quantum system (qudit) one can communicate at most $\log_2 d$ bits of classical information. So it is not possible to encode two qubits to a single qubit and then decode both of them. However, it has been recently shown theoretically [2] that one can encode two nonentangled qubits and then decode probabilistically one arbitrarily chosen qubit with perfect fidelity. It is important that one can decide which qubit to decode after the encoding took place. The protocol is probabilistic in the sense that the average probability of successful decoding is equal to $2/3$. Bertuskova *et al.* [3] have recently realized the above scheme experimentally for optical qubits. In their execution of the protocol the probability of successful decoding was $1/2$. This was due to the fact that in the experiment they replaced positive-operator-valued measure (POVM) measurements, whose implementation is rather difficult, with simpler von Neumann measurements. They also presented a generalization of the original scheme. Specifically, they showed how to encode N qudits of dimension d each in one qudit of dimension $N(d-1)+1$ and then decode one of them. In their protocol both the procedures of encoding and decoding succeed with a probability strictly less than 1. In the present paper we investigate properties of the original scheme and extend it in several ways. The paper is organized as follows. In Sec. II we review the original scheme and prove the optimality of the decoding. In Sec. III we show that the protocol preserves entanglement between the qubits and the environment and can also be applied to mixed states. In Sec. IV we present the protocol for encoding two qudits of dimension d in one qudit of dimension $2d-1$ and then probabilistically decoding one of them. In Sec. V we show how to encode n nonentangled qudits to one qudit of a dimension smaller than the Hilbert space of the original system and then probabilistically but with perfect fidelity decode any subset of k qudits. We also give a formula for the probability of successful decoding. The paper ends with a brief summary in Sec. VI.

II. OPTIMALITY OF DECODING

Let us first briefly describe the original protocol. We introduce two parties Alice and Bob. Alice performs the encoding while Bob tries to decode the qubit with perfect fidelity. We suppose that the states of the two qubits are

$$|\Psi_1\rangle = a_1|0\rangle_1 + b_1|1\rangle_1 \tag{1}$$

and

$$|\Psi_2\rangle = a_2|0\rangle_2 + b_2|1\rangle_2. \tag{2}$$

To encode the states of these qubits to one qutrit Alice performs measurement on the joint state of the system $|\Psi_1\rangle \otimes |\Psi_2\rangle$ given by the following measurement operators:

$$M_{0,0} = \frac{1}{\sqrt{3}}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|), \tag{3}$$

$$M_{0,1} = \frac{1}{\sqrt{3}}(|01\rangle\langle 01| + |00\rangle\langle 00| + |11\rangle\langle 11|), \tag{4}$$

$$M_{1,0} = \frac{1}{\sqrt{3}}(|10\rangle\langle 10| + |11\rangle\langle 11| + |00\rangle\langle 00|), \tag{5}$$

$$M_{1,1} = \frac{1}{\sqrt{3}}(|11\rangle\langle 11| + |10\rangle\langle 10| + |01\rangle\langle 01|). \tag{6}$$

It should be emphasized that this is a generalized measurement (a POVM). If as a result of the measurement Alice obtains 0,0, then the state of two qubits is projected onto a three-dimensional subspace and is now given as

$$|\Psi\rangle = N(a_1 a_2|00\rangle + a_1 b_2|01\rangle + b_1 a_2|10\rangle), \tag{7}$$

where N is a normalization constant. To recover the first qubit Bob performs a projective measurement given by the following operators:

$$P_{1,S} = |00\rangle\langle 00| + |10\rangle\langle 10|, \tag{8}$$

$$P_{1,F} = |01\rangle\langle 01|. \tag{9}$$

If Bob obtains 1, S as a result of the measurement then the state of the qutrit is projected onto a two-dimensional subspace and is identical to the state of the first qubit given by Eq. (1). If Bob obtains 1, F as a result of the measurement then the procedure of decoding fails. Averaging over all pure states of the first and second qubits one obtains that the probability of successful decoding is equal to $2/3$. Similarly, to recover the second qubit Bob performs a projective measurement described by the operators

$$P_{2,S} = |00\rangle\langle 00| + |01\rangle\langle 01|, \tag{10}$$

$$P_{2,F} = |10\rangle\langle 10|. \tag{11}$$

The procedure of decoding works similarly in the case when Alice obtains i,j as the result of the measurement. However, the choice of decoding operators depends on the three-dimensional subspace onto which Alice projected the original state of two qubits. Thus Alice has to send to Bob two bits of classical information identifying this subspace.

Let us now investigate whether one can decode one arbitrarily chosen qubit with average probability higher than $2/3$. The most general quantum operation corresponding to decoding of the first qubit can be written as

$$|\Psi_1\rangle\langle\Psi_1| = \frac{\sum_k E_k|\Psi\rangle\langle\Psi|E_k^\dagger}{\mathrm{Tr}\left(\sum_k E_k|\Psi\rangle\langle\Psi|E_k^\dagger\right)}, \tag{12}$$

where $|\Psi_1\rangle$ is the state of the first qubit given by Eq. (1), $|\Psi\rangle$ is the state of the qutrit given by Eq. (7), and E_k are operation elements of the form

$$E_k = \begin{pmatrix} e_k^{0,0} & e_k^{0,1} & e_k^{0,2} \\ e_k^{1,0} & e_k^{1,1} & e_k^{1,2} \end{pmatrix}. \tag{13}$$

Because on the left side of Eq. (12) we have a pure state we must have for each k

$$E_k|\Psi\rangle = \lambda_k|\Psi_1\rangle, \tag{14}$$

where λ_k are some complex numbers and depend on E_k and $|\Psi\rangle$. Substituting Eqs. (1) and (7) into Eq. (14) we obtain

$$e_k^{0,0}Na_1a_2 + e_k^{0,1}Na_1b_2 + e_k^{0,2}Nb_1a_2 = \lambda_k a_1, \tag{15}$$

$$e_k^{1,0}Na_1a_2 + e_k^{1,1}Na_1b_2 + e_k^{1,2}Nb_1a_2 = \lambda_k b_1. \tag{16}$$

Equations (15) and (16) have to be satisfied for any values of a_i and b_i satisfying the normalization condition $|a_i|^2+|b_i|^2=1$. The solution to these equations has the form

$$\lambda_k = e_k N a_2, \tag{17}$$

$$E_k = \begin{pmatrix} e_k & 0 & 0 \\ 0 & 0 & e_k \end{pmatrix}. \tag{18}$$

Because $\sum_k E_k^\dagger E_k \leqslant I$ one obtains $\sum_k |e_k|^2 \leqslant 1$. The probability of successful decoding is equal to

$$\begin{aligned} p_{1,S} &= \mathrm{Tr}\left(\sum_k E_k|\Psi\rangle\langle\Psi|E_k^\dagger\right) = \mathrm{Tr}\left(\sum_k E_k^\dagger E_k|\Psi\rangle\langle\Psi|\right) \\ &= \sum_k |e_k|^2 \mathrm{Tr}[(|00\rangle\langle 00| + |10\rangle\langle 10|)|\Psi\rangle\langle\Psi|] \\ &\leqslant \mathrm{Tr}(P_{1,S}|\Psi\rangle\langle\Psi|). \end{aligned} \tag{19}$$

We thus obtained that the quantum operation of Eq. (8) gives the highest probability of successful decoding.

III. CODING OF QUBITS ENTANGLED WITH THE ENVIRONMENT AND QUBITS IN MIXED STATES

Let us now investigate the possibility of coding the entangled and mixed states. We emphasize that the protocol does not enable encoding of qubits in nonseparable states but this does not reject the possibility of coding qubits entangled with two distinct environments. Thus we suppose that each of Alice's qubits is entangled with a qubit from the environment but they are not correlated (either quantum or classically) with each other. We assume that the first qubit and the qubit from the environment are in the pure state

$$|\Psi_1\rangle = a_1|0\rangle_{E_1}|0\rangle_1 + b_1|1\rangle_{E_1}|0\rangle_1 + c_1|0\rangle_{E_1}|1\rangle_1 + d_1|1\rangle_{E_1}|1\rangle_1. \tag{20}$$

Similarly, the state of the second qubit and the qubit from the environment is

$$|\Psi_2\rangle = a_2|0\rangle_{E_2}|0\rangle_2 + b_2|1\rangle_{E_2}|0\rangle_2 + c_2|0\rangle_{E_2}|1\rangle_2 + d_2|1\rangle_{E_2}|1\rangle_2. \tag{21}$$

It is convenient to write these states in the following way:

$$|\Psi_1\rangle = |\psi_1\rangle|0\rangle_1 + |\phi_1\rangle|1\rangle_1, \tag{22}$$

$$|\Psi_2\rangle = |\psi_2\rangle|0\rangle_2 + |\phi_2\rangle|1\rangle_2, \tag{23}$$

where

$$|\psi_{1(2)}\rangle = a_{1(2)}|0\rangle_{E_{1(2)}} + b_{1(2)}|1\rangle_{E_{1(2)}}, \tag{24}$$

$$|\phi_{1(2)}\rangle = c_{1(2)}|0\rangle_{E_{1(2)}} + d_{1(2)}|1\rangle_{E_{1(2)}} \tag{25}$$

are in general some unnormalized and not necessarily orthogonal vectors. If Alice performs the measurement given by the operators of Eqs. (3)–(6) and obtains, for example, 0,0 as the result of the measurement, then the state vector of the whole system collapses to

$$|\Psi\rangle = N(|\psi_1\rangle|\psi_2\rangle|00\rangle + |\psi_1\rangle|\phi_2\rangle|01\rangle + |\phi_1\rangle|\psi_2\rangle|10\rangle). \tag{26}$$

To recover the state of the first or the second qubit and the corresponding qubit from the environment, Bob performs a projective measurement given by the operators of Eqs. (8) and (9) or Eqs. (10) and (11), respectively. We see that the original protocol preserves the entanglement between the qubit to be recovered and the environment.

Let us now comment on the coding of mixed states. Let us suppose that we have two qubits. The first (second) qubit is in a state described by the density matrix $\rho_{1(2)}$ and the state of the whole system is

$$\rho = \rho_1 \otimes \rho_2. \tag{27}$$

It is well known that any mixed state can be purified [4]. Thus, we can assume that the mixed state $\rho_{1(2)}$ is obtained from the pure state of the system and the environment by tracing out the latter. Because the scheme preserves entanglement between the system and the environment, the density matrix of the qubit that is successfully decoded does not change and we conclude that the protocol can be applied to mixed states of the form (27).

IV. CODING OF TWO QUDITS

Let us now describe a generalization of the scheme for coding of two qudits. We assume that we have two nonentangled qudits of dimension d. Each of them is in a pure state [5]:

$$|\Psi\rangle = \sum_{i=0}^{d-1} a_i|i\rangle \otimes \sum_{i=0}^{d-1} b_i|i\rangle. \tag{28}$$

To encode the states of these two qudits in one qudit of dimension $2d-1$, Alice performs the measurement described by the following operators:

$$M_{i,j} = \frac{1}{\sqrt{2d-1}}\left(|ij\rangle\langle ij| + \sum_{\substack{k=0,\\ k\neq i}}^{d-1} |kj\rangle\langle kj| + \sum_{\substack{l=0,\\ l\neq j}}^{d-1} |il\rangle\langle il|\right). \tag{29}$$

These are Hermitian operators. Each term $|ij\rangle\langle ij|$ is present in $1+2(d-1)$ operators, namely, in $M_{i,j}$, $M_{k,j}$ $(k\neq i)$, and $M_{i,l}$ $(l\neq j)$, and thus these operators satisfy the condition

$$\sum_{i,j=0}^{d-1} M_{i,j}^{\dagger} M_{i,j} = I. \tag{30}$$

Taking it all together we see that the operators $M_{i,j}$ are indeed the measurement operators. Each of these operators projects the initial state of two qudits onto a $(2d-1)$-dimensional subspace of the original Hilbert space. We can now treat our system as a qudit of dimension $2d-1$. To decode the state of the first qudit, Bob performs a projective measurement described by the operators

$$P_{1,S} = \sum_{k=0}^{d-1} |kj\rangle\langle kj| \tag{31}$$

and

$$P_{1,F} = \sum_{l=0,l\neq j}^{d-1} |il\rangle\langle il|. \tag{32}$$

If he obtains $1,S$ as a result of the measurement then decoding succeeds; otherwise it fails. The procedure for decoding of the second qudit is similar.

V. CODING OF MANY QUDITS

We now describe the protocol for encoding n qudits in such a way that probabilistic, but error-free decoding of any subset of k qudits is possible. Let us suppose that we have n nonentangled qudits of dimension d. Each of these qudits is in a pure state [5] and the state of the whole system is

$$|\Psi\rangle = \sum_{i=0}^{d-1} a_i|i\rangle \otimes \sum_{i=0}^{d-1} b_i|i\rangle \otimes \sum_{i=0}^{d-1} c_i|i\rangle \cdots . \tag{33}$$

In order to encode these n qudits in such a way that Bob can later decode any subset of k qudits, Alice performs a measurement described by the operators

$$\begin{aligned} M_{i,j,k,\ldots} = \frac{1}{\sqrt{D_k}}\Bigg(&|ijk\cdots\rangle\langle ijk\cdots| + \sum_{\substack{p=0,\\ p\neq i}}^{d-1} |pjk\cdots\rangle\langle pjk\cdots| \\ &+ \sum_{\substack{q=0,\\ q\neq j}}^{d-1} |iqk\cdots\rangle\langle iqk\cdots| + \sum_{\substack{r=0,\\ r\neq k}}^{d-1} |ijr\cdots\rangle\langle ijr\cdots| + \cdots \\ &+ \sum_{\substack{p=0,q=0,\\ p\neq i,q\neq j}}^{d-1} |pqk\cdots\rangle\langle pqk\cdots| + \sum_{\substack{p=0,r=0,\\ p\neq i,r\neq k}}^{d-1} |pjr\cdots\rangle \\ &\times\langle pjr\cdots| + \sum_{\substack{q=0,r=0,\\ q\neq j,r\neq k}}^{d-1} |iqr\cdots\rangle\langle iqr\cdots| + \cdots \\ &+ (\text{other terms}), \end{aligned} \tag{34}$$

where "other terms" stands for similar sums over three, four,..., k indices. The constant D_k in the above equation is equal to the dimension of the subspace onto which $M_{i,j,k,\ldots}$ projects and

$$D_k = \sum_{i=0}^{k} \binom{n}{i} (d-1)^i. \tag{35}$$

Similar arguments as before can be used to show that these operators indeed describe a measurement. Because if $k<n$ then

$$D_k = \sum_{i=0}^{k} \binom{n}{i} (d-1)^i < \sum_{i=0}^{n} \binom{n}{i} (d-1)^i = [1+(d-1)]^n = d^n, \tag{36}$$

the qudits are encoded in a system with a Hilbert space of smaller dimension than the original one.

To decode k qudits Bob performs a projective measurement described by the operators

$$P_S = \sum_{p=0,q=0,\ldots}^{d-1} |pqk\cdots\rangle\langle pqk\cdots|, \tag{37}$$

$$P_F = I - P_S, \tag{38}$$

where the sum is taken over indices belonging to the qudits to be decoded and the other indices are equal to those that specify the result of the measurement (34). We also notice that if the qudits to be decoded are entangled between themselves then the procedure succeeds and preserves the entanglement. However, the qudits that are decoded cannot be correlated with those that are not decoded.

Let us now illustrate the whole protocol with a simple example. We assume that we have three qubits. Now we can encode them in two different ways: (1) Alice encodes three qubits in such a way that any one of them can be later decoded and (2) Alice encodes three qubits in such a way that any two of them can be later decoded. In both cases the initial state of the system is

$$|\Psi\rangle = a_1a_2a_3|000\rangle + a_1a_2b_3|001\rangle + a_1b_2a_3|010\rangle + a_1b_2b_3|011\rangle + b_1a_2a_3|100\rangle + b_1a_2b_3|101\rangle + b_1b_2a_3|110\rangle + b_1b_2b_3|111\rangle. \tag{39}$$

In the case of the first coding we have $n=3$, $d=2$, and $k=1$. To encode three qubits Alice projects the state of the system on a four-dimensional subspace with measurement operators defined in Eq. (34), for example,

$$M_{0,0,0} = \frac{1}{2}(|000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100|). \tag{40}$$

If Alice obtains 0,0,0 as a result of her measurement then the state of the system becomes

$$|\Psi\rangle = N(a_1a_2a_3|000\rangle + a_1a_2b_3|001\rangle + a_1b_2a_3|010\rangle + b_1a_2a_3|100\rangle). \tag{41}$$

If Bob wants to decode the state of the first qubit he performs a projective measurement described by the operators

$$P_{1,S} = |000\rangle\langle 000| + |100\rangle\langle 100|, \tag{42}$$

$$P_{1,F} = |010\rangle\langle 010| + |001\rangle\langle 001|. \tag{43}$$

If he obtains 1, S as a result of the measurement then he successfully decodes the first qubit.

In the case of the second coding we have $n=3$, $d=2$, and $k=2$. To encode three qubits Alice projects the state of the system onto a seven-dimensional subspace with measurement operators defined in Eq. (34), for example,

$$M_{0,0,0} = \frac{1}{\sqrt{7}}(|000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100| + |011\rangle\langle 011| + |101\rangle\langle 101| + |110\rangle\langle 110|). \tag{44}$$

It should be noted here that the dimension of the space onto which the original space is projected depends on two things: (1) the number of qudits to be encoded and (2) the number of qudits to be decoded.

If Alice obtains 0,0,0 as a result of her measurement then the state of the system becomes

$$|\Psi\rangle = N(a_1a_2a_3|000\rangle + a_1a_2b_3|001\rangle + a_1b_2a_3|010\rangle + b_1a_2a_3|100\rangle + a_1b_2b_3|011\rangle + b_1a_2b_3|101\rangle + b_1b_2a_3|110\rangle). \tag{45}$$

If Bob wants to decode the state of the first and second qubits he performs a projective measurement described by the operators

$$P_S = |000\rangle\langle 000| + |100\rangle\langle 100| + |010\rangle\langle 010| + |110\rangle\langle 110|, \tag{46}$$

$$P_F = |001\rangle\langle 001| + |011\rangle\langle 011| + |101\rangle\langle 101|. \tag{47}$$

If he obtains S as a result of the measurement then he has successfully decoded the first and second qubits.

In the protocols described the procedure of decoding is always successful; however, one does not know onto which subspace the initial state of the system will be projected. The choice of the decoding measurement depends on (1) the qudits to be decoded and (2) the subspace onto which the initial state was projected. Because of the latter Alice must send to Bob $n \log_2 d$ bits of classical information about the result of her measurement. The procedure of decoding is probabilistic and it only succeeds with some probability. If we assume that each qudit is prepared in a randomly chosen pure state then the average probability of successful decoding of k qudits of n encoded qudits is equal to

$$p_S = \frac{d^k}{D_k}. \tag{48}$$

This is the dimension of the Hilbert space of k decoded qudits divided by the dimension of the Hilbert space of the qudit to which n qudits were encoded.

VI. SUMMARY

We have shown that the scheme of Ref. [2] preserves the entanglement between the qubit to be decoded and the environment and can also be used for coding of mixed states. We also presented a much more general protocol that enables encoding of n qudits in one qudit of dimension smaller than the dimension of the Hilbert space of the original system and then probabilistically decode any subset of k of them. The probability of successful decoding is equal to the dimension of the Hilbert space of k qudits divided by the dimension of the qudit in which the n qudits are encoded.

ACKNOWLEDGMENTS

Two of us (A.G. and A.W.) would like to thank the State Committee for Scientific Research for financial support under Grant No. 0 T00A 003 23.

[1] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973)
[2] A. Grudka and A. Wójcik, Phys. Lett. A **314**, 350 (2003).
[3] L. Bertuskova *et al.*, e-print quant-ph/0603174.
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, U.K., 2000).
[5] The protocol applies to mixed states as well.