Criterion for faithful teleportation with an arbitrary multiparticle channel

Chi-Yee Cheung*
Institute of Physics, Academia Sinica, Taipei, Taiwan 11529, Republic of China

Zhan-Jun Zhang†
School of Physics & Material Science, Anhui University, Hefei 230039, China
(Received 1 April 2009; published 21 August 2009)

We present a general criterion which allows one to judge if an arbitrary multiparticle entanglement channel can be used to teleport faithfully an unknown quantum state of a given dimension. We also present a general multiparticle teleportation protocol which is applicable for all channel states satisfying this criterion.

DOI: 10.1103/PhysRevA.80.022327 PACS number(s): 03.67.Ac, 03.67.Hk, 03.67.Mn

I. INTRODUCTION

Quantum teleportation is arguably the most novel application of quantum mechanics in quantum information science. This protocol provides a means of recreating an arbitrary unknown quantum state at a remote site without the need of transferring any particles or a large amount of classical information. The magic of teleportation is made possible by prior quantum entanglement between the sender (Alice) and the receiver (Bob). It is well known that, in the original protocol proposed by Bennett *et al.* [1], if Alice and Bob share a two-qubit entangled state (Bell or Einstein-Podolsky-Rosen state), then Alice can teleport any one-qubit state to Bob. This protocol is linear; that means if Alice and Bob share N Bell states, then Alice will be able to teleport an arbitrary N-qubit state to Bob. In recent years, quantum teleportation has been experimentally realized in several different quantum systems [2–6].

To facilitate the ensuing discussions, we first demonstrate the teleportation of an arbitrary N-qubit state below. The four Bell states are given by

$$|\phi^1\rangle_{ab} = \frac{1}{\sqrt{2}}(|01\rangle_{ab} - |10\rangle_{ab}), \tag{1}$$

$$|\phi^2\rangle_{ab} = \frac{1}{\sqrt{2}}(|01\rangle_{ab} + |10\rangle_{ab}), \tag{2}$$

$$|\phi^3\rangle_{ab} = \frac{1}{\sqrt{2}}(|00\rangle_{ab} - |11\rangle_{ab}), \tag{3}$$

$$|\phi^4\rangle_{ab} = \frac{1}{\sqrt{2}}(|00\rangle_{ab} + |11\rangle). \tag{4}$$

Suppose Alice shares a Bell state $|\phi^1\rangle_{ab}$ with Bob (Alice holds qubit a and Bob holds qubit b), and in addition she owns an arbitrary N-qubit pure state $|\Psi\rangle_{12\ldots N}$ to be teleported to Bob. Note that actually $|\Psi\rangle_{12\ldots N}$ is not restricted to pure states. However, if it is a mixed state, then one can always purify it by introducing ancilla qubits [7]. Since the ancillas do not participate in the teleportation process, we will ignore their possible existence in the following discussions.

The product of $|\Psi\rangle_{12\ldots N}$ and $|\phi^1\rangle_{ab}$ can be rewritten as

$$|\Psi\rangle_{12\ldots N}|\phi^1\rangle_{ab} = -\frac{1}{2}\left(\sum_{i=1}^{4}|\phi^i\rangle_{1a}U_b^i\right)|\Psi\rangle_{b2\ldots N}, \tag{5}$$

where $\{U^i\}=\{I,\sigma^z,-\sigma^x,i\sigma^y\}$, and I is the 2×2unit matrix. Therefore if Alice makes a Bell state measurement on the qubit pair $(1,a)$ and sends a two-bit classical message to inform Bob of the outcome (i), then Bob can reconstruct the original N-qubit state by applying a local unitary operation U_b^i on his qubit. The only difference is that Alice's qubit 1 has been renamed b and is now in Bob's possession. It is easy to see that, with more Bell states, this process can be repeated on the other qubits in $|\Psi\rangle_{12\ldots N}$. Therefore if Alice shares N pairs of Bell states with Bob, then she will be able to teleport perfectly the entire state $|\Psi\rangle_{12\ldots N}$ to Bob.

However in practice the channel state shared by Alice and Bob may not always be a tensor product of N Bell states. Then one must consider each case individually to decide if it is useful for teleportation and if so how to proceed; there exists no general rule. Some special cases have been studied in the literature [8–14] and most of them are concerned with four-qubit channels. For example, Yeo and Chua [8] introduced a so-called "genuinely four-qubit entangled state" which is not reducible to a pair of Bell states and showed that it could be used to teleport an arbitrary two-qubit state. Chen *et al.* [9] generalized the results of [8] to N-qubit teleportation. Rigolin [11] constructed 16 four-qubit entangled states which are useful for two-qubit teleportation. Agrawal and Pati considered teleportation using asymmetric W states. Muralidharan and Panigrahi [13] employed a "genuinely entangled" channel of five qubits to teleport two qubits. A criterion has been proposed by Zha and Song [14] in terms of the unitarity property of a "transformation matrix," which tells if a four-qubit entanglement channel supports two-qubit teleportation. However no general results exist in the literature when the quantum channel in question is an arbitrary multiparticle entangled state. In this paper we consider the most general situation where the channel state shared by Alice and Bob is arbitrary. In the following, we derive a crite-

*cheung@phys.sinica.edu.tw
†zjzhang@ahu.edu.cn

rion which allows one to judge if a given channel state is useful for teleportation, and if so, to find the maximum number of qubits it can faithfully teleport.

II. CRITERION

Let Alice and Bob share an arbitrary bipartite state $|X\rangle_{A_1\ldots A_m B_1\ldots B_n}$ of $(m+n)$ qubits, of which m qubits belong to Alice and n to Bob. We shall first assume $m\geq n$; the $m<n$ case can later be included in a straightforward manner. As mentioned before, entanglement is the key ingredient which makes quantum teleportation possible. For an arbitrary bipartite state $|X\rangle_{A_1\ldots A_m B_1\ldots B_n}$ (or $|X\rangle_{AB}$ for short), the degree of entanglement between Alice's and Bob's subsystems can be quantified by the von Neumann entropy of either of two subsystems [15,16], which is given by

$$E_{AB} = -\operatorname{Tr}(\rho_A \log_2 \rho_A) = -\operatorname{Tr}(\rho_B \log_2 \rho_B), \tag{6}$$

where ρ_A and ρ_B are the reduced density matrices of the subsystems,

$$\rho_A = \operatorname{Tr}_B(|X\rangle_{AB}\langle X|_{AB}), \tag{7}$$

$$\rho_B = \operatorname{Tr}_A(|X\rangle_{AB}\langle X|_{AB}). \tag{8}$$

Since we assume $m\geq n$, therefore,

$$E_{AB} \leq n. \tag{9}$$

Consider first the case

$$E_{AB} = n \tag{10}$$

so that the entanglement between the two subsystems is maximal. Then we must have

$$\rho_B = I_B/2^n, \tag{11}$$

where I_B is the $2^n\times 2^n$ identity matrix in Bob's Hilbert space H_B. Now consider another situation in which Alice and Bob share n pairs of Bell states, and in addition Alice owns an arbitrary pure state $|\mathcal{O}\rangle$ of $(m-n)$ qubits. The combined $(m+n)$-qubit state is

$$|\Lambda\rangle_{AB} = \left(\prod_{i=1}^{n} |\phi^1\rangle_{A_iB_i}\right)|\mathcal{O}\rangle_{A_{n+1}\ldots A_m}, \tag{12}$$

where $|\phi^1\rangle_{A_iB_i}$ is the singlet Bell state defined in Eq. (1). Although the properties of $|\mathcal{O}\rangle_{A_{n+1}\ldots A_m}$ are irrelevant, for definiteness and without loss of generality, we may take

$$|\mathcal{O}\rangle_{A_{n+1}\ldots A_m} = \prod_{j=n+1}^{m} |0\rangle_{A_j}. \tag{13}$$

The reduced density matrix on Bob's side is given by

$$\bar{\rho}_B = \operatorname{Tr}_A(|\Lambda\rangle_{AB}\langle\Lambda|_{AB}) = I_B/2^n, \tag{14}$$

which is the same as ρ_B given in Eq. (11). Hence, by a theorem of Hughston *et al.* [17], these two pure states are related by a unitary transformation on Alice's side. In other words, Alice can transform $|X\rangle_{AB}$ into $|\Lambda\rangle_{AB}$ by applying a local unitary operation $\mathcal{U}_A$ on her qubits:

$$|\Lambda\rangle_{AB} = \mathcal{U}_A|X\rangle_{AB}, \tag{15}$$

where $\mathcal{U}_A$ is explicitly constructed in the Appendix. It is important to note that Alice can carry out this transformation by herself and there is no need for Bob to do anything. However, if $m<n$, then maximal entanglement means $E_{AB}=m$ and Bob must carry out the corresponding n-qubit transformation $\mathcal{U}_B$. And if $m=n$, either party can do it.

Equation (15) essentially establishes that, for any arbitrary bipartite state $|X\rangle_{A_1\ldots A_m B_1\ldots B_n}$, if the von Neumann entropy of either of the subsystems is $n(\leq m)$, then it can be used to teleport faithfully an arbitrary n-qubit state. Conversely, by applying arbitrary unitary operators $\mathcal{U}_A$ to the state $|\Lambda\rangle_{AB}$ given in Eq. (12), one can generate any number of states which can support n-qubit teleportation. Indeed, all of the special channels proposed in the literature can be obtained this way [8–14].

Next we consider the nonmaximally entangled case

$$E_{AB} < n. \tag{16}$$

In this case, perfect teleportation of an arbitrary n-qubit state is obviously impossible. Nevertheless it may still be used to teleport a state of $d(<n)$ qubits. Let

$$|X'\rangle_{AB} = \mathcal{U}_B|X\rangle_{AB}, \tag{17}$$

where is $\mathcal{U}_B$ is a unitary operator in H_B which maximizes the value of $d(\leq E_{AB})$ in the following expression:

$$\rho_B' = \operatorname{Tr}_A|X'\rangle_{AB}\langle X'|_{AB} = \eta_{B'}\frac{1}{2^d}\prod_{i=1}^{d} I_{B_i}, \tag{18}$$

where I_{B_i} is the 2×2 identity operator for qubit B_i and $\eta_{B'}$ is the density matrix of the qubits in $B'=\{B_{d+1},\ldots,B_n\}$. It is easy to see that d is the number of qubits in H_B which are maximally entangled with those in H_A; it may be called the "maximally entangled number." Explicit construction of $\mathcal{U}_B$ is given in the Appendix.

Let

$$|\lambda\rangle_{AB} = \left(\prod_{i=1}^{d} |\phi^1\rangle_{A_iB_i}\right)|\varphi\rangle_{A'B'}, \tag{19}$$

where $|\phi^1\rangle$ is the singlet Bell state, $A'=\{A_{d+1},\ldots,A_m\}$, and $|\varphi\rangle_{A'B'}$ is any bipartite state satisfying

$$\operatorname{Tr}_{A'}|\varphi\rangle_{A'B'}\langle\varphi|_{A'B'} = \eta_{B'}. \tag{20}$$

It follows that

$$\operatorname{Tr}_A|X'\rangle_{AB}\langle X'|_{AB} = \operatorname{Tr}_A|\lambda\rangle_{AB}\langle\lambda|_{AB} \tag{21}$$

by construction. Then, as before, Alice can transform $|X'\rangle_{AB}$ into $|\lambda\rangle_{AB}$ [17],

$$|\lambda\rangle_{AB} = \mathcal{U}_A|X'\rangle_{AB}, \tag{22}$$

where the operator $\mathcal{U}_A$ is explicitly constructed in the Appendix. Therefore finally we have

$$|\lambda\rangle_{AB} = \mathcal{U}_A\mathcal{U}_B|X\rangle_{AB}, \tag{23}$$

and Alice can employ the d shared Bell states in $|\lambda\rangle_{AB}$ to teleport an arbitrary d-qubit state to Bob. Note that as long as

$E_{AB}<n$, we may have $d=0$; if so, then not even a singlet qubit can be teleported perfectly.

In the maximally entangled case ($E_{AB}=n$), we have $\mathcal{U}_B=I$, and $d=n$ in Eq. (18). So the general condition for faithful teleportation can be stated as follows. If there exists a unitary operator $\mathcal{U}_B$ such that $d\neq 0$ in Eq. (18), then $|X\rangle_{AB}$ can be used to teleport faithfully an arbitrary state containing d qubits. This condition is clearly also necessary. The following general protocol works for any arbitrary channel state $|X\rangle_{AB}$ satisfying Eq. (18): (1) Bob calculates $\mathcal{U}_B$ which determines the maximum number (d) of qubits that can be teleported and Alice calculates $\mathcal{U}_A$. (2) Alice and Bob apply $\mathcal{U}_A$ and $\mathcal{U}_B$, respectively, to the qubits in their control. (3) Then Alice can use the resulting d shared Bell states to teleport an arbitrary d-qubit state to Bob as usual [1].

Note that, if $E_{AB}=n$, then Alice is required to perform one m-qubit operation and n Bell state measurements and Bob is required to make n single qubit operations at most. On the other hand, if $E_{AB}<n$, then Bob may be required to perform a n-qubit operation $\mathcal{U}_B$ as well. The generalization to $m<n$ should be straightforward by now. In other protocols proposed for multiqubit teleportation, more complex operations are involved. For example, in [8,9,11–13], Alice is required to perform a joint operation involving $(m+n)$ qubits.

Using similar arguments, one can show that teleportation could also be performed without making Bell state measurements. For simplicity, we will show how it works for teleporting a one-qubit state $|\Psi\rangle_1$. The original procedure corresponds to Eq. (5) with $N=1$. Let us replace the four Bell states $\{|\phi^1\rangle,|\phi^2\rangle,|\phi^3\rangle,|\phi^4\rangle\}$ by the four orthogonal product states $\{|\chi^i\rangle\}=\{|11\rangle,|10\rangle,|01\rangle,|00\rangle\}$, respectively. The result is

$$|\xi\rangle_{1ab}=-\frac{1}{2}\left(\sum_{i=1}^{4}|\chi^i\rangle_{1a}U_b^i\right)|\Psi\rangle_b. \tag{24}$$

The reduced density matrix on Bob's side is

$$\mathrm{Tr}_{1a}(|\xi\rangle_{1ab}\langle\xi|_{1ab})=I_b/2, \tag{25}$$

which is the same as that of the joint initial state $|\Psi\rangle_1|\phi^1\rangle_{ab}$. Therefore, again by the theorem of Hughston *et al.* [17], $|\xi\rangle_{1ab}$ is related to $|\Psi\rangle_1|\phi^1\rangle_{ab}$ by a unitary transformation $\mathcal{U}_{1a}$ on Alice's side,

$$|\xi\rangle_{1ab}=\mathcal{U}_{1a}(|\Psi\rangle_1|\phi^1\rangle_{ab}). \tag{26}$$

It can be shown that (apart from an unimportant phase)

$$\mathcal{U}_{1a}=H_aC_1^a, \tag{27}$$

where H_a is the Hadamard operator and C_1^a is the controlled-not operator with qubit 1 as the target. Hence the Bell measurement in the original protocol [1] can be replaced by the unitary operation U_{1a} plus two single-qubit measurements. It turns out that this is equivalent to the mysterious looking quantum computing circuit devised by Brassard *et al.* [18].

Finally, as a simple demonstration, let us take the channel state to be the N-qubit Greenberger-Horne-Zeilinger (GHZ) state

$$|\mathrm{GHZ}\rangle_{1\ldots N}=\frac{1}{\sqrt{2}}(|0\ldots 0\rangle_{1\ldots N}+|1\ldots 1\rangle_{1\ldots N}). \tag{28}$$

No matter how the qubits are partitioned between Alice and Bob (provided that each party gets at least one qubit), the entropy of entanglement $E_{AB}=1$, so it can be used to teleport a one-qubit state at most. If Alice holds qubits $\{1,\ldots,N-1\}$ and Bob holds the last qubit N, then the entanglement between the two subsystems is maximal. It follows from Eq. (15) that there exists a unitary operator $\mathcal{U}_A$ such that

$$\mathcal{U}_A|\mathrm{GHZ}\rangle_{1\ldots N}=|\phi^4\rangle_{1N}\prod_{i=2}^{N-1}|0\rangle_i. \tag{29}$$

It is easy to show that $\mathcal{U}_A$ is just a series of controlled-not operators C_i^1:

$$\mathcal{U}_A=\prod_{i=2}^{N-1}C_i^1. \tag{30}$$

In this special case, Alice alone can transform $|\mathrm{GHZ}\rangle_{1\ldots N}$ into the desired form given in Eq. (12). In general, if Alice holds qubits $\{1,\ldots,m\}$ and Bob holds qubits $\{m+1,\ldots,N\}$, the two subsystems are not maximally entangled. Then according to Eq. (23), both $\mathcal{U}_A$ and $\mathcal{U}_B$ are required, i.e.,

$$\mathcal{U}_A\mathcal{U}_B|\mathrm{GHZ}\rangle_{1\ldots N}=|\phi^4\rangle_{1N}\prod_{i=2}^{N-1}|0\rangle_i, \tag{31}$$

where

$$\mathcal{U}_A=\prod_{i=2}^{m}C_i^1, \tag{32}$$

$$\mathcal{U}_B=\prod_{i=m+1}^{N-1}C_i^N. \tag{33}$$

In both cases, Alice and Bob share one Bell state, so the given channel can be used to teleport a single-qubit state only.

III. SUMMARY

In summary, we have considered issues related to faithful teleportation when the available channel is an arbitrary N-qubit state $|X\rangle_{AB}$ partitioned between Alice and Bob in any given manner. A general criterion, Eq. (18), is presented which allows one to decide the maximum number of qubits it can faithfully teleport. The general multiparticle teleportation protocol proposed here is applicable for any channel states, whereas the other protocols proposed in the literature are applicable only for quantum channels of certain specific forms.

ACKNOWLEDGMENTS

This work is supported by the program for New Century Excellent Talents at the University of China under Grant No. NCET-06-0554, the National Natural Science Foundation of

China under Grant No. 60677001, the science-technology fund of Anhui province for outstanding youth under Grant No. 06042087, the key fund of the ministry of education of China under Grant No. 206063, and the general fund of the educational committee of Anhui province under Grant No. 2006KJ260B.

APPENDIX

In this appendix, we show how to find the unitary operators $\mathcal{U}_A$ and $\mathcal{U}_B$ which are required to transform $|X\rangle_{AB}$ into $|\lambda\rangle_{AB}$ in Eq. (23). Recall that $|X\rangle_{AB}$ is any bipartite state of $m+n$ qubits, of which m qubits belong to Alice and n to Bob. We assume $m \geq n$ and generalization to $m < n$ is obvious. Using singular value decomposition, we can always express $|X\rangle_{AB}$ in the Schmidt form,

$$|X\rangle_{AB} = \sum_{k=1}^{2^n} \sqrt{p^k}|e^k\rangle_A|f^k\rangle_B, \tag{A1}$$

where $\Sigma p^k = 1$, and $\{|e^k\rangle_A\}$ and $\{|f^k\rangle_B\}$ are orthonormal bases in H_A and H_B, respectively. If the entanglement between Alice and Bob's qubits is not maximal [see Eq. (16)], then we need to find the maximally entangled number d as defined in Eq. (18). To find out if any qubit B_i in H_B is maximally entangled with those in H_A, we can proceed as follows. Let U_B^0 be a unitary operator in H_B such that

$$|\widetilde{X}\rangle_{AB} = U_B^0|X\rangle_{AB}, \tag{A2}$$

$$= \sum_{k=1}^{2^n} \sqrt{p^k}|e^k\rangle_A|\widetilde{f}^k\rangle_B, \tag{A3}$$

where the new basis states

$$|\widetilde{f}^k\rangle_B = U_B^0|f^k\rangle_B \tag{A4}$$

are all product states. For example, for $n=2$, $\{|\widetilde{f}^k\rangle\} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Explicitly,

$$U_B^0 = \sum_{k=1}^{2^n} |\widetilde{f}^k\rangle_B\langle f^k|_B. \tag{A5}$$

It follows that the new reduced density matrix,

$$\widetilde{\rho}_B = \mathrm{Tr}_A(|\widetilde{X}\rangle_{AB}\langle\widetilde{X}|_{AB}), \tag{A6}$$

can be written as

$$\widetilde{\rho}_B = \frac{1}{2}(|0\rangle_{B_i}\langle 0|_{B_i}\eta_{B-i} + |1\rangle_{B_i}\langle 1|_{B_i}\xi_{B-i}), \tag{A7}$$

where the subscript "$B-i$" denotes all particles in H_B except B_i, and η_{B-i} and ξ_{B-i} are diagonal matrices in H_{B-i}. If η_{B-i} and ξ_{B-i} have identical matrix elements (when arranged in descending order), then they are related by a change in bases. Namely,

$$\eta_{B-i} = u_{B-i}\xi_{B-i}u_{B-i}^{\dagger}, \tag{A8}$$

where u_{B-i} is a unitary operator which can be easily constructed as in Eq. (A5). Define

$$U_B^i = |0\rangle_{B_i}\langle 0|_{B_i}I_{B-i} + |1\rangle_{B_i}\langle 1|_{B_i}u_{B-i}, \tag{A9}$$

where I is the identity operator, and let

$$|\widetilde{X}'\rangle_{AB} = U_B^i|\widetilde{X}\rangle_{AB}, \tag{A10}$$

then the new reduced density matrix in H_B is given by

$$\widetilde{\rho}'_B = \mathrm{Tr}_A(|\widetilde{X}'\rangle_{AB}\langle\widetilde{X}'|_{AB}), \tag{A11}$$

$$= \frac{1}{2}I_{B_i}\eta_{B-i}. \tag{A12}$$

Similarly one can check if any other qubit $B_j(\neq B_i)$ is maximally entangled with those in H_A. If so, then as before we can construct an operator

$$U_B^j = I_{B_i}(|0\rangle_{B_j}\langle 0|_{B_j}I_{B-i-j} + |1\rangle_{B_j}\langle 1|_{B_j}u_{B-i-j}), \tag{A13}$$

such that if

$$|\widetilde{X}''\rangle_{AB} = U_B^jU_B^i|\widetilde{X}\rangle_{AB}, \tag{A14}$$

then the new reduced density matrix

$$\widetilde{\rho}''_B = \mathrm{Tr}_A(|\widetilde{X}''\rangle_{AB}\langle\widetilde{X}''|_{AB}), \tag{A15}$$

$$= \frac{1}{2^2}I_{B_i}I_{B_j}\eta_{B-i-j}, \tag{A16}$$

where η_{B-i-j} is the diagonal density matrix of all the qubits in H_B except B_i and B_j. Suppose in the end we find d such qubits, each corresponds to a U_B^i, then the transformation $\mathcal{U}_B$ defined in Eq. (17) is given by

$$\mathcal{U}_B = \prod_{i=1}^{d} U_B^i, \tag{A17}$$

where some relabeling of the qubits may be required.

To find $\mathcal{U}_A$, we can proceed as follows. First of all,

$$|X'\rangle_{AB} = \mathcal{U}_B|X\rangle_{AB}, \tag{A18}$$

$$= \sum_{k=1}^{2^n} \sqrt{p^k}|e^k\rangle_A|f'^k\rangle_B, \tag{A19}$$

where

$$|f'^k\rangle_B = \mathcal{U}_B|f^k\rangle_B. \tag{A20}$$

By construction, we have

$$\rho'_B = \mathrm{Tr}_A(|X'\rangle_{AB}\langle X'|_{AB}) = \sum_{k=1}^{2^n} p^k|f'^k\rangle_B\langle f'^k|_B, \tag{A21}$$

$$= \eta_{B'}\frac{1}{2^d}\prod_{i=1}^{d} I_{B_i}, \tag{A22}$$

where the density matrix $\eta_{B'}$ so obtained is automatically diagonal. Let

$$\eta_{B'} = \sum_{k=1}^{2^{n-d}} q^k|\beta^k\rangle_{B'}\langle\beta^k|_{B'}, \tag{A23}$$

where $\Sigma q^k=1$, and $\{|\beta^k\rangle_{B'}\}$ are orthonormal states in $H_{B'}$. Furthermore, let

$$|\varphi\rangle_{A'B'} = \sum_{k=1}^{2^{n-d}} \sqrt{q^k}|\alpha^k\rangle_{A'}|\beta^k\rangle_{B'} \tag{A24}$$

be a purification of $\eta_{B'}$ to $H_{A'}\otimes H_{B'}$, where $\{|\alpha^k\rangle_{A'}\}$ is any set of orthonormal states in $H_{A'}$. For simplicity, we can take the $|\alpha^k\rangle_{A'}$'s to be product states. Then the pure state $|\lambda\rangle_{AB}$ as defined in Eq. (19),

$$|\lambda\rangle_{AB} = \left(\prod_{i=1}^{d} |\phi^k\rangle_{A_iB_i}\right)|\varphi\rangle_{A'B'}, \tag{A25}$$

is already in the diagonal Schmidt form. From the fact that

$$\mathrm{Tr}_A(|X'\rangle_{AB}\langle X'|_{AB}) = \mathrm{Tr}_A(|\lambda\rangle_{AB}\langle\lambda|_{AB}), \tag{A26}$$

we must have

$$|\lambda\rangle_{AB} = \sum_{k=1}^{2^n} \sqrt{p^k}|e'^k\rangle_A|f'^k\rangle_B, \tag{A27}$$

where $\{e'^k_A\}$ is another set of orthonormal basis in H_A. Finally, comparing Eqs. (A19) and (A27), we conclude that $\mathcal{U}_A$ is simply the operator connecting the two bases sets $\{|e^k\rangle_A\}$ and $\{|e'^k\rangle_A\}$:

$$|e'^k\rangle_A = \mathcal{U}_A|e^k\rangle_A, \tag{A28}$$

or explicitly,

$$\mathcal{U}_A = \sum_{k=1}^{2^m} |e'^k\rangle_A\langle e^k|_A. \tag{A29}$$

As mentioned in Sec. II, in the special case of maximal entanglement between Alice and Bob's qubits [see Eq. (10)], we have $d=n$ and hence $\mathcal{U}_B=I$. Thus we see that the most basic ingredients in the above construction are unitary transformations connecting one orthonormal basis to another. In general $\mathcal{U}_A$ and $\mathcal{U}_B$ are operators involving m and n qubits, respectively. Of course, by the universality of two-level unitary gates [7], one can always decompose them into a product of elementary operations involving one or two qubits. In the special case specified below, they involve exclusively single-qubit operations. Let $\{|0\rangle_i,|1\rangle_i\}$ and $\{|0'\rangle_i,|1'\rangle_i\}$ be two single-qubit bases. One can readily check that, if and only if the effect of a transformation is a simple substitution of $\{|0\rangle_i,|1\rangle_i\}$ by $\{|0'\rangle_i,|1'\rangle_i\}$ (for all qubits), then it can be decomposed into a product of single-qubit operations $u_i=|0'\rangle_i\langle 0|_i+|1'\rangle_i\langle 1|_i$.

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature (London) **421**, 509 (2003).
[3] M. Riebe, H. Hffner, C. F. Roos, W. Hnsel, J. Benhelm, G. P. T. Lancaster, T. W. Krber, C. Becher, F. S. Kaler, D. F. V. James, and R. Blatt, Nature (London) **429**, 734 (2004).
[4] M. D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D. J. Wineland, Nature (London) **429**, 737 (2004).
[5] Z. Zhao, Y. A. Chen, A. N. Zhang, T. Yang, H. J. Briegel, and J. W. Pan, Nature (London) **430**, 54 (2004).
[6] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and Z. Zeilinger, Nature (London) **430**, 849 (2004).
[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[8] Y. Yeo and W. K. Chua, Phys. Rev. Lett. **96**, 060502 (2006).
[9] P. X. Chen, S. Y. Zhao, and G. C. Guo, Phys. Rev. A **74**, 032324 (2006).
[10] J. Lee, H. Min, and S. D. Oh, Phys. Rev. A **66**, 052318 (2002).
[11] G. Rigolin, Phys. Rev. A **71**, 032303 (2005).
[12] P. Agrawal and A. Pati, Phys. Rev. A **74**, 062320 (2006).
[13] S. Muralidharan and P. K. Panigrahi, Phys. Rev. A **77**, 032321 (2008).
[14] X. W. Zha and H. Y. Song, Phys. Lett. A **369**, 377 (2007).
[15] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[16] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).
[17] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. A **183**, 14 (1993).
[18] G. Brassard, S. Braunstein, and R. Cleve, Physica D **120**, 43 (1998); e-print arXiv:quant-ph/9605035.