PHYSICAL REVIEW A

ATOMIC, MOLECULAR, AND OPTICAL PHYSICS

THIRD SERIES, VOLUME 57, NUMBER 6 JUNE 1998

RAPID COMMUNICATIONS

The Rapid Communications section is intended for the accelerated publication of important new results. Since manuscripts submitted to this section are given priority treatment both in the editorial office and in production, authors should explain in their submittal letter why the work justifies this special handling. A Rapid Communication should be no longer than 4 printed pages and must be accompanied by an abstract. Page proofs are sent to authors.

Multiparticle entanglement purification protocols

M. Murao,[1] M. B. Plenio,[1] S. Popescu,[2,3] V. Vedral,[1] and P. L. Knight[1]

[1]*Optics Section, Blackett Laboratory, Imperial College, London SW7 2BZ, United Kingdom*
[2]*Isaac Newton Institute for Mathematical Sciences, Cambridge CB3 0EH, United Kingdom*
[3]*BRIMS, Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, United Kingdom*

(Received 18 December 1997)

Purification schemes for multiparticle entangled states cannot be treated as straightforward extensions of those two-particle ones because of the lack of symmetry they possess. We propose purification protocols for a wide range of mixed entangled states of many particles. These are useful for understanding entanglement, and could be of practical significance in multiuser cryptographic schemes or distributed quantum computation and communication. We show that operating locally on multiparticle entangled states directly is more efficient than relying on two-particle purification. [S1050-2947(98)50906-7]

PACS number(s): 03.67.Hk

Entanglement is of central importance for quantum computation [1], quantum teleportation [2], and certain types of quantum cryptography [3]. Without entangled states, quantum computation and communication would be no more efficient than their classical counterparts. For two particles, the maximally entangled states are the Bell diagonal states $|\phi^{\pm}\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$, $|\psi^{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$, and all other locally unitarily equivalent ones, where the state for each particle is written in the quantum bit (qubit) ($|0\rangle$, $|1\rangle$) basis. For many spin-1/2 particles, the maximally entangled states are

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle \pm |11\cdots 1\rangle), \tag{1}$$

as well as those that are locally unitarily equivalent; for three particles, these are called Greenberg-Horne-Zeilinger (GHZ) states [4]. Unfortunately entangled states turn into mixed states due to the dissipative effects of the environment, and this is one of the main obstacles for the practical realization of quantum computation and entanglement based quantum cryptography. The environment does not always destroy entanglement completely. Mixed states resulting from interaction with the environment may still contain some residual entanglement [5]. The task is then to ''purify'' this residual entanglement with the aim of obtaining maximally entangled states. These purification procedures use only local operations and classical communication [6–8]. Related to this, various quantitative measures of entanglement for mixed states have been proposed [5,9–11]. Popescu and Rohrlich [12] have proven, using arguments based on purification procedures [6–8], that the von Neumann entropy is a unique measure of entanglement for pure bipartite states.

These measures can give upper bounds on the efficiency with which one can purify an initial ensemble of partially entangled states. Disentangled states, which for two particles, are of the form $\Sigma p_i \rho_i^1 \otimes \rho_i^2$ where ρ^1 and ρ^2 are the local-density matrices [13], cannot be purified. For many particles the generalization is not unique. One can define disentangled states as those being of the form $\Sigma p_i \rho_i^1 \otimes \cdots \otimes \rho_i^N$ or as those states from which one cannot purify using local operations a maximally entangled state of N particles [e.g., the state $(|01\rangle + |10\rangle)|0\rangle$ is disentangled according to this definition] [9–11]. The latter definition also gives the investigation of multiparticle purification procedures a fundamental importance in the understanding of entanglement.

Several protocols have been proposed [6–8] for the purification of two-particle entangled states. For two particles, the singlet state ($|\phi^-\rangle$), which is totally antisymmetric, is

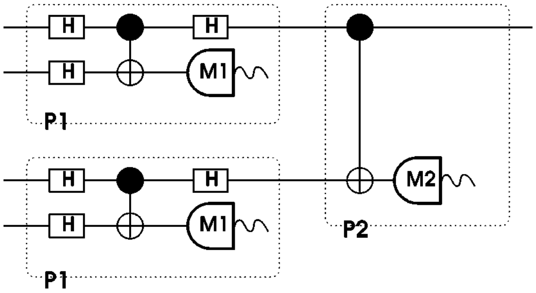

FIG. 1. Purification protocol P1+P2. H is a Hadamard transformation; M1 and M2 are local measurement and classical communication. This diagram shows four particles belonging to Alice. Bob and others apply exactly the same procedure.

invariant under any bilateral rotations. This plays a role in the original purification scheme [6], in which arbitrary density matrices are first mapped into a Werner state $x|\psi^-\rangle\langle\psi^-|+[(1-x)/4]\mathbf{1}$ [14] without changing the weight of the singlet state $f=(1+3x)/4$ (x is a real number) by bilateral random rotations. The Werner state is diagonal in the Bell-state basis and with equal weight for all the elements except the singlet state. Subsequently, Alice and Bob apply bilateral CNOT (Control NOT) operations and local measurements. By communicating the results and selecting a subensemble of the original ensemble of pairs they can distill a number of singlets.

However, for three (many) particles, there is no maximally entangled state that is invariant under trilateral (multilateral) rotations (for a classification of entangled states based on invariance under local unitary transformations, see [15]). This makes it more difficult to transform an arbitrary state into Werner states. This is why we cannot treat multiparticle entanglement purification protocols as straightforward extensions of the two-particle case.

Here, we propose *direct* purification protocols for a wide range of mixed diagonal states having N-particle entanglement. Our aim is to investigate the fidelity limits and efficiency for purification and to make a first step towards a protocol that purifies general mixed states. Our procedures may have important implications for the understanding of multiparticle entanglement and important practical applications, e.g., in quantum communications. A central result is that purifying multiparticle entangled states directly is more efficient than relying on two-particle purification.

Although there is no maximally entangled state invariant under random bilateral rotations for $N\geqslant 3$ (N is the number of entangled particles), we call the state

$$\rho_W=x|\phi^+\rangle\langle\phi^+|+\frac{1-x}{2^N}\mathbf{1} \tag{2}$$

a ''Werner-type state'' because of the similarity to the two-particle case. Note that we write $|\phi^+\rangle$ instead of $|\psi^-\rangle$ for convenience. The aim of purification is the distillation of a subensemble in the state $|\phi^+\rangle$. The fidelity, i.e., $\langle\phi^+|\rho_W|\phi^+\rangle$, of the Werner-type state is $f=x+(1-x)/2^N$. The Werner-type states can occur when we try to transmit N entangled particles to N different parties via noisy channels.

Now, we present a protocol (P1+P2 in Fig. 1), which can purify a Werner-type state, provided the fidelity of the initial mixed state is higher than a certain critical value. The advantage of this is that Werner-type states for *any number of particles* can be *directly* purified.

In the protocol P1+P2, each party (Alice, Bob, and others) performs iterations of the operations P1 followed by P2 on the particles belonging to them. The operation P1 consists of a local Hadamard transformation that maps $|0\rangle\rightarrow(|0\rangle+|1\rangle)/\sqrt{2}$, $|1\rangle\rightarrow(|0\rangle-|1\rangle)/\sqrt{2}$, a local CNOT (Control NOT) operation and a measurement M1, and another local Hadamard transformation. In M1, we keep the control qubits if an even number of target qubits are measured to be in the state $|1\rangle$; otherwise the control qubits are discarded. For example, when purifying for three particles, we only keep $|000\rangle$, $|011\rangle$, $|101\rangle$, $|110\rangle$. The operation P2 consists of a local CNOT operation and a measurement M2 in which we keep the control qubits if all target bits are measured to be in the same state; otherwise the control qubits are discarded. For example, when purifying three particles, we only keep $|000\rangle$ and $|111\rangle$. In this operation, the diagonal and off-diagonal elements of the density matrix are independent of each other, so that the off-diagonal elements do not affect the purification.

Our purification scheme is, however, not restricted to Werner states. When the state to be purified is $|\phi^+\rangle$, we call the state $|\phi^-\rangle$ the pairing state of $|\phi^+\rangle$. If the initial mixed state does not have any weight on the pairing state and weights on other states are equal or some perhaps be zero, iterations of the operation P2 only are sufficient to purify the initial ensemble to the $|\phi^+\rangle$ state. This purification procedure fails if the weight of $|\phi^-\rangle$ is not exactly zero, because even a very small weight of $|\phi^-\rangle$ in the initial mixed state results in an even distribution of $|\phi^+\rangle$ and $|\phi^-\rangle$ after iteration and destroys entanglement.

When the initial state has weight only on the pairing states, that is, when we have states of the form

$$\rho=f|\phi^+\rangle\langle\phi^+|+(1-f\ )|\phi^-\rangle\langle\phi^-|, \tag{3}$$

then these can be purified only by the iteration of the operation P1. P1 maps the state, Eq. (3), into a state of the same form as Eq. (3) but new fidelity $f'=f^2/(2f^2-2f+1)$. That is, the states with initial fidelity f can be purified to $|\phi^+\rangle$ if $f>1/2$ from the condition $f'-f>0$. For $f<1/2$, P1 purifies into $|\phi^-\rangle$. When $f=1/2$, the resulting state is disentangled and therefore cannot be purified by local operations and classical communications.

In our protocols, we purify many-particle entangled states *directly*. This is necessary for a fundamental investigation of characteristic multiparticle entanglement. However, one could imagine schemes that purify many-particle entanglement via two-particle purification: one of these schemes for three particles (of Alice, Bob, and Claire) uses the fact that we know how to purify two particles. So this scheme converts three-particle states into two-particle states, then purifies these two-particle states, and finally reconverts them to three-particle entangled states. This involves the following: (i) We divide an ensemble of the state for three particles into equal amount of two subensembles. (ii) Bob measures his particle from one subensemble in the state $|\chi^{\pm}\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ and Claire measures her particle from another

TABLE I. A, observed fidelity limit of initial states to be purified for N particles of the Werner-type states by the protocol P1+P2; B, theoretical fidelity limit of the purification scheme via two-particle purification; and C, the theoretical minimum sufficient fidelity for purification.

N	A	B	C
2	$f\geqslant 0.5395$	$f>1/2=0.5$	$f>1/2$
3	$f\geqslant 0.4073$	$f>5/12\approx 0.4167$	unknown
4	$f\geqslant 0.313$	$f>3/8=0.375$	unknown
5	$f\geqslant 0.245$	$f>17/48\approx 0.3542$	unknown
6	$f\geqslant 0.20$	$f>11/32\approx 0.3438$	unknown

subensemble in the same state $|\chi^{\pm}\rangle$. If Bob or Claire project onto $|\chi^{-}\rangle$, then they alert Alice to perform the σ_z operation, so that the final two-particle ensemble is in the same state as after a projection onto $|\chi^{+}\rangle$, after which Alice does nothing. Then we have two reduced two-particle entangled states (one pair shared by Alice and Bob and another pair shared by Alice and Claire). (iii) We perform the purification protocol [6,8] with each of the entangled states of two particles. Then we get maximally entangled two particles shared between Alice and Bob, and between Alice and Claire. (iv) Alice chooses one entangled pair from each subensemble and then performs a CNOT operation on her two particles. Then she projects the target particle onto $|0\rangle$ or $|1\rangle$. If Alice obtains a successful projection onto $|1\rangle$, she instructs Claire to perform the σ_x operation on her particle, and otherwise, to do nothing. Then we obtain a subensemble containing the maximally entangled GHZ state [16].

We next analyze this scheme and compare it to our direct purification schemes. Any efficient direct three-particle purification scheme *should* perform better than this indirect method via two particles because one obtains *one* maximally entangled state of three particles from *two* maximally entangled states of two particles. For purification of N-particle entangled states, we get one maximally entangled state from $N-1$ maximally entangled states of two particles. In addition, the number of two-qubit CNOT operations, each of which is difficult to carry out practically to high accuracy, is higher than in our direct scheme. These ''inefficiencies'' are the main practical disadvantage of the two-particle scheme. In the following, we investigate the fidelity limit and efficiency of purification and show that direct multiparticle purification is indeed the more efficient method.

For two-particle entanglement, an initial fidelity $f>1/2$ is sufficient for successful purification if we have no knowledge of this initial state [6,8]. However, the sufficiency condition is not as simple for more than three particles. We have found several different criteria, depending on the type of mixed states.

For the Werner-type states of the form $\rho_W=x|\phi^{+}\rangle\langle\phi^{+}|+[(1-x)/2^N]\mathbf{1}$, and purification by the protocol P1+P2, we obtain numerically the results shown in Table I. The theoretical fidelity limit for the Werner-type states ρ_W of the purification scheme via two-particle purification is determined by the condition that the fidelity f_r of the reduced two-particle states should be $f_r>1/2$. For example, for three particles, the Werner state having initial fidelity $f=x+(1-x)/8$ is reduced to a two-particle state after the measurement of Bob or Claire $\rho_r=x|\phi^{+}\rangle\langle\phi^{+}|+[(1-x)/4]\mathbf{1}$. The fidelity of the reduced two-particle state is now $f_r=(1+6f)/7$. For four particles, we have $f_r=(1+4f)/5$, for five particles, $f_r=(7+24f)/31$, for six particles, $f_r=(5+16f)/21$, and so on. The general formula for the fidelity limit of purification scheme via two-particle purification is $f>(2^{N-1}+1)/(3\times 2^{N-1})$ where N is the number of particles, which tends to 1/3 as N tends to infinity.

We see from Table I, that the protocol P1+P2 is not optimal for two particles. So it may not be optimal for $N>2$. However, for more than three particles, our observed fidelity limit is lower than that obtained via two-particle purification. In general, the fidelity limit decreases as the number of particles increases. We can say that any Werner-type state whose fidelity satisfies the bounds in column A is entangled. In fact, any state that can be *locally* converted into a Werner-type state satisfying column A is also entangled. However, the final boundary separating entangled and disentangled states is still unknown. For the states having no weight on $|\phi^{-}\rangle\langle\phi^{-}|$ and equal weight on all other states except $|\phi^{+}\rangle\langle\phi^{+}|$, the fidelity limit of purification by the protocol P2 is $f>2^{-(N-1)}$. The fidelity limit obtained by the purification scheme via two-particle purification is $2/5=0.4$ for the three-particle case, $65/23\approx 0.358\,46$ for the four-particle case, $125/377\approx 0.328\,912$ for the five-particle case, and so on, i.e., worse than that in our protocols.

We have seen that direct many-particle purification can purify states that *cannot* be purified via the two-particle purification scheme described before. This already suggests that multiparticle purification is also more efficient in terms of the number of maximally entangled states one obtains. We define the asymptotic efficiency of our protocol by the product of the survival probability of the control qubit P_J after J iterations of the protocol and $1/2^J$, which originates from the fact that the entanglement of the target qubits is destroyed. The product of the normalization for each iteration gives the probability P_J that we keep the entangled state after J iterations of the purification procedure. The number of iterations J is chosen such that the fidelity reaches unity with some *a priori* chosen accuracy (this is why it is called ''asymptotic'' efficiency).

The protocol P1 also purifies an ensemble of a pure state $|\Phi\rangle=a|00\cdots 0\rangle+b|11\cdots 1\rangle$, where $b=\sqrt{1-a^2}$, into a subensemble of the maximally entangled pure state $|\phi^{+}\rangle$, that is, the state with $a=b=1/\sqrt{2}$ (we assume $a\leqslant b$ for convenience). The asymptotic efficiency of the purification protocol P1 for the pure state $|\Phi\rangle$ is *invariant* for entangled states of any number of particles and coincides with the asymptotic efficiency of the purification scheme of Deutsch *et al.* [8] for a two-particle pure state. The asymptotic efficiency of our protocol for the N-particle pure entangled state is $N-1$ times better than that of the scheme via two-particle purification [6,8].

We compare the asymptotic efficiency of our purification protocol for the Werner-type states and that of the purification scheme via two-particle purification using the ''normalized'' asymptotic efficiency. The normalized asymptotic efficiency is the product of survival probability P_J of the control qubit for our protocol, but is $P_J/(N-1)$ for the purification scheme via two-particle purification. The factor

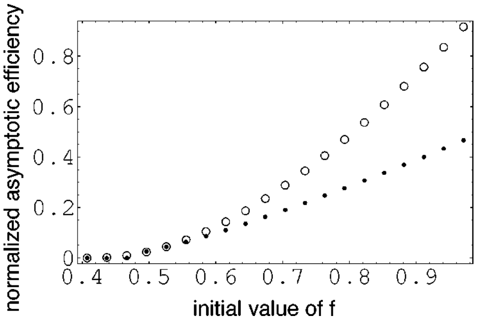

FIG. 2. Normalized asymptotic efficiency of purification of the Werner-type states for three particles against the initial value of fidelity f. The circles are obtained numerically by our purification protocol P1 with a choice of accuracy 10^{-7}. The dots are obtained by the purification scheme via two-particle purification with the same choice of accuracy.

$1/(N-1)$ originates from the fact that one N-particle maximally entangled state is obtained from $N-1$ two-particle maximally entangled states. In Fig. 2, we show the numerical result for the normalized asymptotic efficiency of the two purification procedures for three particles against the initial fidelity f. Our direct purification scheme performs better for all fidelities. We have made the same comparison for four-particle and higher-order entanglement and note that the direct purification scheme is always more efficient than the scheme via two-particle purification. In fact, the difference in normalized asymptotic efficiency between the two schemes becomes even larger for higher-order entanglement. This is an important result because it shows that it is more advantageous both in terms of resources (number of CNOT operations) and normalized asymptotic efficiency (number of maximally entangled states obtained) to perform direct purification of our type than to rely on the two-particle purification schemes.

Next we present an important example of a common noisy quantum communication channel that gives rise to Werner-type states and where our direct purification schemes can be successfully applied. We show that the mixed entangled states that we have treated in this Rapid Communication can be useful in practical applications. The mixed entangled states are likely to appear when one has an ensemble of initially maximally entangled states (for example, $|\phi^{+}\rangle$) of N particles and then transmits the N particles to N different parties via noisy channels. Let us consider the effect of a channel whose action on each particle can be expressed by random rotations about random directions. When each noisy channel causes random rotations (about a random direction and by a random angle) with probability $1-p$, while it leaves the particle unaffected with probability p, the state after transmission becomes the Werner-type state as in Eq. (2). If we consider a noisy channel causing random rotations with a small but random probability depending on the state, purification of states of high fidelity and small random weights on other diagonal states will also be significant. These states are similar to Werner-type states but with additional random weights on the diagonal elements. When the ratio of the additional random weight to fidelity is small; that is, the weight difference among other diagonal elements is much smaller than the fidelity, we have checked that the protocol P1+P2 is successful. However, the final criterion for purification is not yet understood, as the success of purification depends on the distribution of the diagonal elements.

We have found that combinations of the protocols P1 and P2 can directly purify a wide range of mixed states of many particles. The advantage of the protocols proposed in this Rapid Communication is that they can *directly* purify some practically important states (Werner-type states, states having no weight on the pairing state, etc.) of *any number of particles*. We have investigated the fidelity limit and asymptotic efficiency of the purification protocol and have shown that our direct purification protocols are more efficient than two-particle schemes. The fidelity limit of the initial states that are purifiable depends on the distribution of the weight on other diagonal states. This is a condition of different character from the case of two particles [8]. For two particles, the distribution of the weight on other diagonal elements was irrelevant for purification, since any distribution of weights on the other diagonal can be transformed into an even distribution by local random rotations of both particles without changing the amount of entanglement. This suggests that there may be some additional structure to entangled mixed states for many particles, which does not exist for mixed entangled states of two particles.

This work was supported in part by the Japan Society for the Promotion of Science and the U.K. Engineering and Physical Sciences Research Council, the Knight Trust, the European Community, and the Alexander von Humboldt Foundation.

[1] A. Barenco, Contemp. Phys. **37**, 375 (1996).
[2] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] D. M. Greenberger *et al.*, Am. J. Phys. **58**, 1131 (1990).
[5] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
[6] C. H. Bennett *et al.*, Phys. Rev. A **53**, 2046 (1996); Phys. Rev. Lett. **76**, 722 (1996).
[7] N. Gisin, Phys. Lett. A **210**, 151 (1996).
[8] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).
[9] V. Vedral *et al.*, Phys. Rev. Lett. **78**, 2275 (1997).
[10] V. Vedral *et al.*, Phys. Rev. A **56**, 4452 (1997).
[11] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[12] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).
[13] M. Horodecki *et al.*, Phys. Rev. Lett. **78**, 574 (1997).
[14] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[15] N. Linden and S. Popescu, e-print quant-ph/9711016.
[16] A. Zeilinger *et al.*, Phys. Rev. Lett. **78**, 3031 (1997).