Entanglement purification protocol for a mixture of a pure entangled state and a pure product state

Mikołaj Czechlewski,[1] Andrzej Grudka,[1,2,3] Satoshi Ishizaka,[4,5] and Antoni Wójcik[1]

[1]*Faculty of Physics, Adam Mickiewicz University, Umultowska 85, 61-614 Poznań, Poland*
[2]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, Wita Stwosza 57, 80-952 Gdańsk, Poland*
[3]*National Quantum Information Centre of Gdańsk, Władysława Andersa 27, 81-824 Sopot, Poland*
[4]*Nano Electronics Research Laboratories, NEC Corporation, 34 Miyukigaoka, Tsukuba 305-8501, Japan*
[5]*INQIE, The University of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Japan*

We present an entanglement purification protocol for a mixture of a pure entangled state and a pure product state, which are orthogonal to each other. The protocol is a combination of bisection method and one-way hashing protocol. We give recursive formula for the rate of the protocol for different states, i.e., the number of maximally entangled two-qubit pairs obtained with the protocol per a single copy of the initial state. We also calculate numerically the rate for some states.

Entanglement is a resource in quantum information. Maximally entangled states are a basic ingredient of fundamental quantum information protocols such as, e.g., quantum teleportation [1], dense coding [2], or Ekert's quantum cryptographic protocol [3]. In these protocols the maximally entangled pair is shared by two parties and used to perform a certain task. However, in the real world the parties share noisy entangled pairs. Bennett *et al.* have shown that many pairs in mixed entangled states can be distilled to a smaller number of pairs in nearly maximally entangled states [4,5]. In particular, they presented purification protocols that can be realized by means of local operations and classical communication. Let us suppose that the parties share n pairs of qubits, each of which is in the state ρ. If in using a particular protocol the parties can obtain m pairs of qubits, each of which is in the maximal entangled state, from n pairs of qubits, each of which is in state ρ, then the protocol has the rate $\frac{m}{n}$ for the state ρ. Different protocols have different rates and moreover one needs different protocols for different states. The maximal rate for state ρ, i.e., the rate of the optimal protocol for state ρ, is called distillable entanglement. Distillable entanglement of mixed states is usually difficult to calculate, and it is only known for bound entangled states, maximally correlated states, and some other specific mixed states [6–11]. For bound entangled states it is equal to zero [6] while for maximally correlated states it is equal to the relative entropy of entanglement [11–14] and can be distilled by the one-way hashing protocol [15,16]. However, for many states only upper and lower bounds on distillable entanglement are known. Lower bounds are usually given by the rates of particular protocols. Upper bounds are given by entanglement measures known to be greater or equal to distillable entanglement, e.g., the relative entropy of entanglement.

In this Brief Report we present an entanglement purification protocol for a mixture of a pure entangled state and a pure product state that are orthogonal to each other. The very first protocol for these states was presented in [5]. Our protocol is a combination of Procrustean method of entanglement concentration [17], bisection method, and one-way hashing protocol [15,16].

We assume that Alice and Bob share many copies of the state

$$\rho = p|\psi^+\rangle\langle\psi^+| + (1-p)|00\rangle\langle00|, \qquad (1)$$

where

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \qquad (2)$$

is the maximal entangled state. State ρ is a mixture of the maximal entangled state and a product state. The product state is orthogonal to the maximal entangled state. Let Alice and Bob group these states in blocks of n copies, where n is the power of two. It is convenient to write $\rho^{\otimes n}$ in the following way

$$\rho^{\otimes n} = p^n|\psi^+\rangle\langle\psi^+|^{\otimes n} + p^{n-1}(1-p)[|\psi^+\rangle\langle\psi^+|^{\otimes(n-1)}|00\rangle\langle00| + \cdots]$$
$$+ p^{n-2}(1-p)^2[|\psi^+\rangle\langle\psi^+|^{\otimes(n-2)}|00\rangle\langle00|^{\otimes 2} + \cdots] \cdots$$
$$+ (1-p)^n|00\rangle\langle00|^{\otimes n}, \qquad (3)$$

where "$\cdots$" in each square bracket stands for all permutations of the first term in the square bracket.

Let each party project her/his part of the state on a subspace spanned by vectors with the definite number of ones and definite number of zeros, i.e., Alice and Bob perform von Neumann measurements given by the sets of projectors

$$\left\{P_a^n = \sum_{[x]=n,|x|=a} |x\rangle\langle x|\right\}, \qquad (4)$$

and

$$\left\{P_b^n = \sum_{[x]=n,|x|=b} |x\rangle\langle x|\right\}, \qquad (5)$$

respectively, where $|x|$ denotes the Hamming weight of the string x of $[x]=n$ qubits and $a,b \in \{0,1,\ldots,n\}$. If Alice obtains P_a^n as a result of her measurement and Bob obtains P_b^n as a result of his measurement, then all terms in the expansion of $\rho^{\otimes n}$ except the term with $a+b$ $|\psi^+\rangle$'s and $n-a-b$ $|00\rangle$'s are annihilated, i.e., the post measurement state is

$$\rho(n,a,b) = \frac{1}{p(n,a,b)} P_a^n P_b^n [|\psi^+\rangle\langle\psi^+|^{\otimes(a+b)}|00\rangle\langle00|^{\otimes n-a-b}$$
$$+ \cdots] P_a^n P_b^n, \quad (6)$$

where

$$p(n,a,b) = \binom{n}{a+b}\binom{a+b}{a}2^{-(a+b)}. \quad (7)$$

The probability of this event is

$$P(n,a,b) = p^{a+b}(1-p)^{n-a-b}p(n,a,b). \quad (8)$$

The factor $p^{a+b}(1-p)^{n-a-b}\binom{n}{a+b}$ is the probability that Alice and Bob share the state $|\psi^+\rangle\langle\psi^+|^{\otimes(a+b)}|00\rangle\langle00|^{\otimes n-a-b}$ or any permutation of it and $\binom{a+b}{a}2^{-(a+b)}$ $= \mathrm{Tr}[P_a^n P_b^n|\psi^+\rangle\langle\psi^+|^{\otimes(a+b)}|00\rangle\langle00|^{\otimes n-a-b}P_a^n P_b^n]$.

If $a+b=n$, then Alice and Bob share the maximal entangled state of the rank $r(n,a)$, where

$$r(n,a) = \binom{n}{a}, \quad (9)$$

i.e., they share $\log_2 r(n,a)$ maximally entangled pairs of qubits. If one of the equalities: $a=0$, $a=n$, $b=0$, or $b=n$ holds, then Alice and Bob share a separable state.

In the remaining cases Alice and Bob share a mixed entangled state. In order to distill entanglement from it, they can proceed in two ways. First, if Alice and Bob share a large number of blocks of qubits in identical post measurement states, then they can apply the one-way hashing protocol [15] and distill entanglement at the rates

$$I_c(A > B) = S(B) - S(AB), \quad (10)$$

if Alice classically communicates to Bob or

$$I_c(B > A) = S(A) - S(AB), \quad (11)$$

if Bob classically communicates to Alice. $S(A)$ and $S(B)$ are von Neumann entropies of Alice's and Bob's subsystems, respectively, and $S(AB)$ is von Neumann entropy of the whole system. They are given by the following formulas:

$$S(A) = \log_2\binom{n}{a} \quad (12)$$

because the state of Alice's subsystem is an equal mixture of all sequences of length n with the Hamming weight equal to a,

$$S(B) = \log_2\binom{n}{b} \quad (13)$$

because the state of Bob's subsystem is an equal mixture of all sequences of length n with the Hamming weight equal to b, and

$$S(AB) = \log_2\binom{n}{a+b} \quad (14)$$

because the state of the whole system is an equal mixture of $\binom{n}{a+b}$ pure orthogonal states. Hence, the optimal rate of the one-way hashing protocol is

$$I_c(n,a,b) = \log_2\left[\max\left\{\binom{n}{a},\binom{n}{b}\right\}\right] - \log_2\binom{n}{n-a-b}. \quad (15)$$

Second, Alice and Bob can divide the pairs of qubits into two blocks of equal length (the first block consists of the first $n/2$ pairs and the second block consists of the last $n/2$ pairs) and repeat the measurements on each block separately. If Alice obtains $P_{a'}^{n/2} \otimes P_{a''}^{n/2}$ as the result of her measurement and Bob obtains $P_{b'}^{n/2} \otimes P_{b''}^{n/2}$ as the result of his measurement, then the post measurement state is

$$\rho(n/2,a',b') \otimes \rho(n/2,a'',b''), \quad (16)$$

where $a'+a''=a$ and $b'+b''=b$. In derivation we used the identity

$$(P_{x'}^{n/2} \otimes P_{x''}^{n/2})P_x^n = (P_{x'}^{n/2} \otimes P_{x''}^{n/2})\delta_{x'+x'',x}. \quad (17)$$

The probability of this event is

$$p(a',b';a'',b''|n,a,b) = \frac{p(n/2,a',b')p(n/2,a'',b'')}{p(n,a,b)}. \quad (18)$$

If $a'+b'=n/2$ ($a''+b''=n/2$), then the first (second) block of pairs is in the maximal entangled state of the rank $r(n/2,a')$ ($r(n/2,a'')$). If $a'+b' \neq n/2$ ($a''+b'' \neq n/2$), then Alice and Bob can choose if they want to apply the one-way hashing protocol or to divide the pairs in the first (second) block into two blocks and repeat the measurement on each block separately. For different choices Alice and Bob obtain different rates. The rates achievable with the optimal choices are given by the following recursive formula:

$$R(n,a,b) = \max\left\{ I_c(n,a,b), \sum_{a'=a'_{\min}}^{a'_{\max}} \sum_{b'=b'_{\min}}^{b'_{\max}} p(a',b';a-a',b-b'|n,a,b)[R(n/2,a',b') + R(n/2,a-a',b-b')] \right\}, \quad (19)$$

where the summation limits are

$$a'_{\min} = \max\left\{0, a - \frac{n}{2}\right\},$$

$$a'_{\max} = \min\left\{a, \frac{n}{2}\right\},$$

$$b'_{\min} = \max\left\{0, a + b - a' - \frac{n}{2}\right\},$$

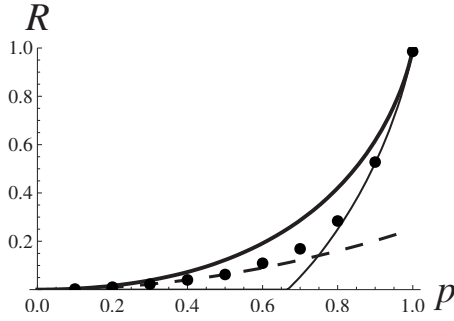$$b'_{\max} = \min\left\{b, \frac{n}{2} - a'\right\}. \quad (20)$$

FIG. 1. Relation between coherent information (thin solid line), relative entropy of entanglement (thick solid line), the rate of the protocol of Bennett *et al.* (dashed line), and our protocol for n =64 (dots) for different values of the parameter p.

If we use only the bisection method (without the one-way hashing protocol), then we obtain the following expression for the rate of such a protocol for state ρ:

$$R(\rho) = \sum_{l=1}^{m} p^{(2^l)}[Y(2^l) - Y(2^{l-1})], \qquad (21)$$

where $n=2^m$ and

$$Y(x) \equiv \frac{1}{x2^x} \sum_{k=0}^{x} \binom{x}{k} \log_2 \binom{x}{k}. \qquad (22)$$

In Fig. 1 we present the rates of the protocol based on the bisection method and the one-way hashing protocol for different initial states ρ of Eq. (1) that depend on the parameter p. The first measurement was performed on a block of 64 pairs of qubits. For comparison, we also present the rates of the protocol from [5] and the one-way hashing protocol as well as an upper bound for distillable entanglement given by the relative entropy of entanglement. One can see that our protocol performs better than the other two protocols.

In Table I we present the rates of the protocol for different sizes of blocks of pairs of qubits on which the first measurement was performed. For comparison, we present also the rates of the protocol based only on the bisection method (without the one-way hashing protocol). One can see that the one-way hashing protocol causes an increase in the rate.

TABLE I. Results for $p=\frac{2}{3}$. n is the size of the block of pairs of qubits on which the first measurement is performed. R is the rate of the protocol based on bisection method and one-way hashing protocol. R' is the rate of the protocol based only on bisection method.

n	R	R'
2	0.111111	0.111111
4	0.158981	0.158981
8	0.173419	0.16638
16	0.175076	0.166574
32	0.175129	0.166575
64	0.175129	0.166575

Let us also point out that our protocol applies to a mixture of an arbitrary pure entangled state and a pure product state orthogonal to it, i.e.,

$$\rho = p|\psi\rangle\langle\psi| + (1-p)|00\rangle\langle00|, \qquad (23)$$

where

$$|\psi\rangle = \alpha|10\rangle + \beta|01\rangle. \qquad (24)$$

One can see it by noting that the first measurement projects n copies of the initial state on a state given in Eq. (6) with probability

$$P'(n,a,b) = p^{a+b}(1-p)^{n-a-b}\binom{n}{a+b}\binom{a+b}{a}|\alpha|^{2a}|\beta|^{2b}. \qquad (25)$$

Because the states given in Eq. (23) can be obtained by sending half of the state

$$|\psi'\rangle = \alpha'|10\rangle + \beta'|01\rangle) \qquad (26)$$

through the amplitude damping channel N_{AD}, given by Kraus operators

$$E_0 = |0\rangle\langle0| + \sqrt{1 - \gamma^2}|1\rangle\langle1|,$$

$$E_1 = \gamma|0\rangle\langle1|, \qquad (27)$$

we can obtain the lower bound on quantum capacity of the amplitude damping channel assisted by two-way classical communication Q_2. In such a case, the best lower bound on Q_2 is given by the following expression

$$R_{\max} = \max_{\psi'} R(N_{AD}(\psi')). \qquad (28)$$

Our protocol requires collective measurements on large blocks of pairs of qubits while the protocol presented in [5] requires only measurements on two pairs of qubits. We will show how one can improve the two-copy protocol. Let Alice and Bob perform von Neumann measurements given by projectors

$$P_0 = |00\rangle\langle00| + |11\rangle\langle11|,$$

$$P_1 = |01\rangle\langle01| + |10\rangle\langle10|, \qquad (29)$$

on the state $\rho^{\otimes2}$. If both obtain one as the results of their measurements, then the post measurement state is equivalent to the maximal entangled state $|\psi^+\rangle$. The probability of this event is equal to $\frac{p^2}{2}$. If both obtain zero as the results of their measurements, then the post measurement state is equivalent to

$$\rho' = p'|\psi^+\rangle\langle\psi^+| + (1-p')|00\rangle\langle00|, \qquad (30)$$

where $p' = \frac{p^2}{p^2 + 2(1-p)^2}$. The probability of this event is equal to $\frac{p^2}{2} + (1-p)^2$. Two such states can be used in another measurement and hence there is a chance to obtain from them the maximal entangled state. In particular, if $p=2/3$ then p' =2/3 and the rate is equal to 2/15 for improved protocol instead of 1/9 for the original protocol.

In conclusion, we presented the entanglement purification

protocol for a mixture of a pure entangled state and a pure product state, orthogonal to each other. We also discussed how one can obtain the lower bound on quantum capacity of the amplitude damping channel assisted by two-way classical communication.

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

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

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[5] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[6] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[7] E. M. Rains, e-print arXiv:quant-ph/9707002.

[8] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens, Phys. Rev. Lett. **84**, 1611 (2000).

[9] Y.-X. Chen and D. Yang, Phys. Rev. A **66**, 014303 (2002).

[10] S. Hamieh and H. Zaraket, J. Phys. A **36**, L387 (2003).

[11] T. Hiroshima and M. Hayashi, Phys. Rev. A **70**, 030302(R) (2004).

[12] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

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

[14] E. M. Rains, IEEE Trans. Inf. Theory **47**, 2921 (2001).

[15] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).

[16] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[17] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).