

Quantum repeaters based on entanglement purification

W. Dür,¹ H.-J. Briegel,^{1,2,*} J. I. Cirac,¹ and P. Zoller¹

¹*Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*

²*Departamento de Física, Universidad de Castilla-La Mancha, 13071 Ciudad Real, Spain*

(Received 31 August 1998)

We study the use of entanglement purification for quantum communication over long distances. For distances much longer than the coherence length of a corresponding noisy quantum channel, the fidelity of transmission is usually so low that standard purification methods are not applicable. It is possible, however, to divide the channel into shorter segments that are purified separately and then connected by the method of entanglement swapping. This method can be much more efficient than schemes based on quantum error correction, as it makes explicit use of two-way classical communication. An important question is how the noise, introduced by imperfect local operations (that constitute the protocols of purification and the entanglement swapping), accumulates in such a compound channel, and how it can be kept below a certain noise level. To treat this problem, we first study the applicability and the efficiency of entanglement purification protocols in the situation of imperfect local operations. We then present a scheme that allows entanglement purification over arbitrary long channels and tolerates errors on the percent level. It requires a polynomial overhead in time, and an overhead in local resources that grows only logarithmically with the length of the channel. [S1050-2947(99)09801-7]

PACS number(s): 03.67.Hk, 03.65.Bz, 42.50.-p

I. INTRODUCTION

In quantum communication, quantum bits (qubits) [1] are sent across quantum channels that connect distant nodes of a quantum network. In general, these quantum channels are noisy and therefore limit the fidelity of the transmission. A bottleneck for quantum communication is the scaling of the probability of transmission errors with the length of the channels connecting the nodes. Different from classical (digital) communication, the “signals” in quantum communication consist of single qubits which may be entangled. Owing to fundamental principles, these qubits cannot be cloned [2,3] nor amplified [4] without destroying the essential quantum feature. This fact limits the maximum distance between the nodes to a few multiples of the absorption length (or the coherence length) of the channel, and poses a severe restriction on any practical application. For example, in recent experiments on quantum cryptography [5], single photons are sent through optical fibers with a given absorption and depolarization length. This has two effects: (i) to transmit a photon without absorption, the number of trials scales exponentially with l ; (ii) even when a photon arrives, the fidelity of the transmitted state decreases exponentially with l . In the experiment, the distance between the nodes is therefore presently limited by a few multiples of the absorption length of the fiber [6].

In the context of fault-tolerant quantum computing [7], Knill and Laflamme [8] have discussed an important scheme that allows us, in principle, to transmit a qubit over arbitrarily long distances with a polynomial overhead in the resources. Their method requires us to encode a single qubit into a concatenated quantum code (i.e., an entangled state of

a large number of qubits) and to operate on this code repeatedly while it is propagated through the channel. The tolerable error probabilities for transmission are less than 10^{-2} , whereas for local operations they are less than 5×10^{-5} . This seems to be outside the range of any practical implementation in the near future. A crucial figure for any experiment will be the number of particles that can be manipulated locally in a coherent fashion, together with the precision with which such local manipulations can be realized. For instance, even when the number of particles scales only polynomially with the length of the channel, a polynomially large number may still be far too large for any practical implementation.

A central tool in the theory of quantum information, specifically for quantum communication, is entanglement purification [9–12]. It allows us, in principle, to create maximally entangled states of particles at different locations even if the channel that connects those locations is noisy [1]. These entangled particles can then be used for faithful teleportation [13] or secure quantum cryptography [12,14]. It seems natural therefore to use this method as an ingredient for a quantum repeater. Furthermore, it allows highly efficient two-way protocols which cannot be realized with quantum error correction procedures. If a noisy quantum channel is much longer than its coherence length, one cannot directly employ standard purification schemes. These schemes first create an ensemble of low-fidelity Einstein-Podolsky-Rosen (EPR) pairs across the channel, and then purify/distill a few perfect EPR pairs out of the ensemble. This, however, requires a minimum fidelity F_{\min} of the initial pairs to operate with, which cannot be achieved as the length l of the channel increases.

In this paper, we treat the problem of a quantum repeater based on the method of entanglement purification. The idea of such a repeater is to divide a long quantum channel into shorter segments, which are purified separately, before they are connected. Connecting two segments of a channel means

*Permanent address: Institut für Theoretische Physik, Universität München, Theresienstrasse 37, D-80333 München, Germany.

here to build up quantum correlations across the compound channel from correlations that exist across the individual segments. This can be done by entanglement swapping, or teleportation of entanglement. A quantum repeater must therefore combine the methods of entanglement purification and teleportation.

Although the combination of these methods should, in principle, allow us to create entanglement over arbitrary distances, it is another question how much this “costs” in terms of resources needed for purification. Resources means here the number of low-fidelity EPR pairs that have to be provided for purification of each channel segment. This quantity is related to the number of particles that have to be manipulated locally (at the connection points between the segments) in a coherent fashion. If the resources grow too fast with the length of the channel, not much will be gained by the whole procedure. A further important quantity is the error tolerance for the local operations. In every real situation, the local operations applied to one or more particles will bear some imperfections. Since such operations are the building blocks for any entanglement purification protocol, their imperfections will limit the maximum attainable fidelity for an EPR pair and the efficiency of the protocol. In the context of the quantum repeater, a maximum fidelity $F < 1$ corresponds to a residual amount of noise for each segment. When the segments are connected, this noise accumulates.

To give a realistic treatment of the quantum repeater, we will therefore first study the applicability and the efficiency of entanglement purification protocols in the situation of imperfect local operations. The general conditions under which standard purification protocols can be used in the presence of errors have been studied by Giedke *et al.* [15]. This includes, in particular, thresholds and lower bounds for the attainable fidelities. For a generic class of stochastic errors, one can give explicit representations of the imperfect operations in terms of completely positive maps (POVMs) [16]. In terms of these maps, we derive recursion formulas for the fidelities, which generalize the results given by Bennett *et al.* [9] and by Deutsch *et al.* [12]. From these results, we estimate that, for a generic class of errors, standard entanglement purification protocols work even for error probabilities of the order of a few percent. In the context of long distance communication, we develop a purification procedure that combines the standard protocols with quantum teleportation in a certain way to be specified. This purification procedure allows quantum communication via noisy channels of arbitrary length. Since it explicitly exploits two-way classical communication [10], our procedure is much more efficient for quantum communication than protocols based on quantum error correction [8]. Specifically, this solution of the quantum repeater tolerates errors on the percent level; it requires a polynomial overhead in time and an overhead in local resources that grows only logarithmically with the length of the channel.

The paper is organized as follows. In Sec. II we introduce a generic error model to describe imperfect local operations such as noisy one-bit and two-bit operations and imperfect measurements. With the aid of these models, we revisit in Sec. III the basic elements of quantum communication—purification and teleportation. This discussion includes results for the maximum attainable fidelities and the working

conditions of the standard protocols under the condition of noisy local operations. After this discussion, in Sec. IV, we are ready to attack the quantum repeater problem itself. Our solution combines the methods of entanglement purification and entanglement swapping into a single (meta)protocol, which we call nested entanglement purification. This protocol allows to distribute entanglement with a given fidelity across arbitrary long distances, even when local operations are imperfect. It requires an overhead in local resources that grows polynomially with the length of the channel. A modification of this protocol works with resources that grow only logarithmically with the length of the channel (while the build-up time grows polynomially).

II. IMPERFECT LOCAL OPERATIONS AND MEASUREMENTS

Imperfections of local operations can have various origins. An example for an imperfect one-qubit operation is a unitary “overrotation” [17], as it would be realized by a laser pulse that effects a Bloch rotation around an angle that slightly deviates from the ideal (intended) one. If the laser is well stabilized but the pulse area tuned incorrectly, say, the deviation of the real from the intended (unitary) rotation will be the same when we repeat the operation, representing an example of a systematic error. If, on the other hand, the angle of the rotations fluctuates randomly around a certain mean value, every pulse introduces a certain amount of noise into the system, and the resulting operation would be described by a nonunitary map. In the present paper, we concentrate on this latter situation, that is, we assume only stochastic errors and neglect systematic errors.

To give a precise description of a noisy one-bit or two-bit operation, one needs to know the exact form of the error mechanisms, which in turn depend on the specific physical implementation. In general, we have only limited knowledge of these details. A generic model for a noisy channel is the so-called (symmetric) depolarizing channel. It transforms a qubit with initial state ρ as

$$\rho \rightarrow p\rho + \frac{1-p}{2}I, \quad (1)$$

where I is the identity operator and $0 \leq p \leq 1$ depends on the time for which the qubit is subjected to the channel. The action of the channel thus results in admixing a completely depolarized state $I/2$ to the initial density operator. The limit $p \rightarrow 0$ corresponds to a very noisy channel, while $p \rightarrow 1$ describes a channel with very little noise (“ideal storage”).

One can easily generalize Eq. (1) to the case where the ideal operation is some arbitrary unitary (one-bit) operation U ,

$$\rho \rightarrow pU\rho U^\dagger + \frac{1-p}{2}I. \quad (2)$$

In this situation, the ideal operation is accompanied by the action of the depolarizing channel. The whole map becomes nonunitary. It describes an imperfect one-bit operation, which for $p \rightarrow 1$ becomes identical to the ideal unitary map. We call p the *reliability* of the imperfect operation, which represents a lower bound to the probability that its result

corresponds to the ideal one. For a parametrization $U = U_{\vec{\alpha}} = \exp(-i\vec{\alpha} \cdot \vec{\sigma})$, an imperfect (noisy) rotation may explicitly be defined by the map

$$\rho \rightarrow R_{\vec{\alpha}} \rho = \int d\vec{\beta} \nu(\vec{\beta}) U_{\vec{\alpha} + \vec{\beta}} \rho U_{\vec{\alpha} + \vec{\beta}}^{\dagger}, \quad (3)$$

where the noise function $\nu(\vec{\beta})$ is normalized to unity and describes the fluctuations $\delta\vec{\alpha} = \vec{\beta}$ of the (generalized) Bloch vector α . One can easily show that for ‘‘isotropic noise,’’ $\nu(\vec{\beta}) = \bar{\nu}(|\vec{\beta}|)$, the integral reduces to

$$R_{\vec{\alpha}} \rho = p U_{\vec{\alpha}} \rho U_{\vec{\alpha}}^{\dagger} + \frac{1-p}{2} I = p R_{\vec{\alpha}}^{\text{ideal}} \rho + \frac{1-p}{2} I, \quad (4)$$

wherein $R_{\vec{\alpha}}^{\text{ideal}} \rho \equiv U_{\vec{\alpha}} \rho U_{\vec{\alpha}}^{\dagger}$ describes the ideal rotation.

Motivated by these observations, we generalize this model to arbitrary one-qubit and two-qubit gates [18] acting on an entangled state ρ of several qubits. We thereby require that errors introduced by local operations may only affect the local qubits on which the ideal operation acts (locality condition). Let ρ be a state of q qubits, labeled by $1, 2, \dots, q$. An imperfect one-qubit operation acting on the first qubit, say, is then described by the map

$$O_1 \rho = p_1 O_1^{\text{ideal}} \rho + \frac{1-p_1}{2} \text{tr}_1\{\rho\} \otimes I_1 \quad (5)$$

whereas an imperfect two-qubit operation acting on qubits 1 and 2 is described by

$$O_{12} \rho = p_2 O_{12}^{\text{ideal}} \rho + \frac{1-p_2}{4} \text{tr}_{12}\{\rho\} \otimes I_{12}. \quad (6)$$

In these expressions, O^{ideal} is the ideal (perfect) operation and I_1 and I_{12} denote unit operators on the subspace where the ideal operation acts, corresponding to totally depolarized one- and two-qubit states. The states of the other particles are described by the partial traces $\text{tr}_1\{\rho\}$ and $\text{tr}_{12}\{\rho\}$, respectively, of the initial density operator over these subspaces. The quantities p_1 and p_2 measure the *reliability* of the operations, where perfect operations correspond to $p_j = 1$. Technically speaking, an imperfect operation is modeled by the corresponding ideal operation accompanied/ followed by a depolarizing channel that acts (only) on the same subspace as the ideal operation.

Note that the maps (5) and (6) are linear and trace conserving, albeit nonunitary. For any state ρ which is diagonal in the Bell basis defined by any two of the particles (all states we deal with in this paper are of this form), the model is self-consistent in the sense that $O_1 \otimes O_2$ (two single-qubit operations, each described by an error parameter p_1) can be written as a certain two-qubit operation O_{12} described by an error parameter $p_2 = p_1^2$. Generally, any sequence of local operations can be written as a single joint operation within this model [21]. The resulting error parameter (i.e., reliability) describing the joint operation is obtained by multiplying the error parameters of the single operations.

We will use these maps to estimate the role of imperfect operations in standard protocols for entanglement purification and for teleportation. Although the model is simple, it is

generic at the same time. We just mention here that similar maps may be derived from a Jaynes-type principle, insofar as their resulting states maximize the entropy of the resulting state with respect to variations that are trace conserving and keep the average fidelity of the operation constant.

We finally describe an *imperfect measurement* on a single qubit (in the computational basis) by a POVM [20] corresponding to the ‘‘imperfect projectors’’

$$\begin{aligned} P_0^{\eta} &= \eta |0\rangle\langle 0| + (1-\eta) |1\rangle\langle 1|, \\ P_1^{\eta} &= \eta |1\rangle\langle 1| + (1-\eta) |0\rangle\langle 0|. \end{aligned} \quad (7)$$

The parameter η is a measure for the quality of the projection onto the basis states. Assume the qubit to be measured is in the state $\rho = |0\rangle\langle 0|$ and we are trying to measure its state with the aid of a measurement apparatus described by Eq. (7). The expectation values $\langle P_0^{\eta} \rangle = \eta$ and $\langle P_1^{\eta} \rangle = 1 - \eta$ simply mean that the apparatus will give us the wrong result (‘‘1’’) with probability $1 - \eta \geq 0$. That is, the result is not completely reliable. An ideal measurement, in contrast, is described by $\eta = 1$. It is clear that the effect of the measurement on the measured qubit is not fully specified by the POVM (7). In the present context, however, this description is sufficient as all measured particles are removed from the system, i.e., we trace over their degrees of freedom after the measurement.

The operations (5) and (6) together with single-qubit measurements (7) are sufficient to describe all operations occurring in the context of teleportation and entanglement purification. For example, a Bell measurement (the measurement of a projector in the Bell basis) on two particles, say 1 and 2, can be realized by a two-qubit operation $O_{12} \equiv \text{CNOT}_{1 \rightarrow 2}^{\text{imperf}}$ (controlled NOT operation) followed by a Hadamard rotation of particle 1 and two single-qubit measurements $P_{0(1)}^1, P_{0(1)}^2$ on particles 1 and 2 [25]. Instead of performing the Hadamard transformation one can also measure particle 1 in a rotated basis. In summary, an imperfect Bell measurement is described by an imperfect two-qubit operation followed by two imperfect single-qubit measurements, effecting, e.g., $|0\rangle|0\rangle \pm |1\rangle|1\rangle \rightarrow (|0\rangle \pm |1\rangle)|0\rangle$.

III. PURIFICATION AND TELEPORTATION WITH IMPERFECT MEANS

In this section we reconsider the basic elements of quantum communication, which are teleportation and purification, in the presence of local errors.

A. Entanglement purification

Purification is the distillation of few ‘‘perfect’’ EPR pairs out of many imperfect pairs. In the following, we will generalize two different purification protocols that have been

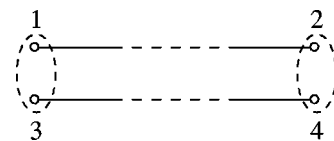


FIG. 1. Particles required for purification in standard recurrence schemes.

treated in the literature, by introducing imperfect gate and measurement operations. In Sec. III A 3, we then discuss a modified version of these schemes which, generally speaking, has less favorable convergence properties but works with a smaller and constant number of *physical resources*.

1. Scheme of Bennett et al. (scheme A)

This purification scheme was introduced by Bennett *et al.* [9,10]. In short, the scheme takes two pairs (1-2 and 3-4) as in Fig. 1, both in a Werner state

$$\rho = F|\Phi^+\rangle\langle\Phi^+| + \left(\frac{1-F}{3}\right)(|\psi^-\rangle\langle\psi^-| + |\psi^+\rangle\langle\psi^+| + |\Phi^-\rangle\langle\Phi^-|) \quad (8)$$

with fidelity $F = \langle\phi^+|\rho|\phi^+\rangle$. Then it performs local (1- and 2-bit) operations on the particles at the same ends of the

pairs. Writing $\rho_{12} \otimes \rho_{34} = \rho_{1234}$, this essentially involves two CNOT operations, $\text{CNOT}_{13}^{\text{imperf}}$ and $\text{CNOT}_{34}^{\text{imperf}}$, acting on the state ρ_{1234} , followed by a simple measurement $P_{0(1)}^3, P_{0(1)}^4$ of the particles 3 and 4. If the particles are found in the same state (00 or 11), the remaining pair, described by the state ρ'_{12} , is kept, otherwise it is discarded. To obtain a recursive mapping between Werner states, a nonunitary depolarization operation (twirl) is applied to the resulting state before it is used for the next purification step. The original treatment of this protocol [9,10] assumes that all operations and measurements of the protocol are perfect.

To estimate the effect of local errors, we evaluate the protocol with the aid of the imperfect operations (5)–(7). The calculation of the fidelity F' of the new pair ρ'_{12} is somewhat lengthy but straightforward, and the result can be given in analytic form. The result of this calculation is summarized in the formula

$$F' = \frac{p_2^2 \left[F^2 + \left(\frac{1-F}{3}\right)^2 \right] [\eta^2 + (1-\eta)^2] + p_2^2 \left[F \left(\frac{1-F}{3}\right) + \left(\frac{1-F}{3}\right)^2 \right] [2\eta(1-\eta)] + \left(\frac{1-p_2^2}{8}\right)}{p_2^2 \left[F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2 \right] [\eta^2 + (1-\eta)^2] + p_2^2 \left[F \left(\frac{1-F}{3}\right) + \left(\frac{1-F}{3}\right)^2 \right] [8\eta(1-\eta)] + \left(\frac{1-p_2^2}{2}\right)}, \quad (9)$$

which reduces to the formula given in Ref. [9] in the limiting case $\eta=1$ and $p_2=1$ (perfect operations). Although ρ'_{12} is no longer a Werner state, it can again be brought to Werner form using (noisy) depolarization [19]. If one starts with an ensemble of pairs with fidelity F , F' gives the fidelity of the remaining pairs that are left after one purification step. This defines a fraction of $2/p_{\text{even}}$ of the initial ensemble of pairs, where p_{even} denotes the probability for finding the particles 3 and 4 in the state 00 or 11, and is given by the denominator in Eq. (9). The factor 2 arises since the pair originally composed of particles 3 and 4 is lost due to the measurement.

Each (iterated) application of Eq. (9) corresponds to a purification step. For each purification step, two identical pairs (which both result from previous successful purification steps) are used. The *purification resources* are defined by the

average number M of pairs needed to perform k_{max} successful purification steps, and are given by

$$M = \prod_k^{k_{\text{max}}} \frac{2}{p_{\text{even}}^{(k)}}, \quad (10)$$

where the probabilities $p_{\text{even}}^{(k)}$ depend on the purification step k . The *physical resources*, defined by the total number of particles at A or B that are used to store the pairs needed for the purification process, are for this scheme equal to the purification resources, since all pairs are created at the beginning and have to be stored as can be seen in Fig. 2.

When calculating the fixed points of Eq. (9), one finds that one fixed point is always $F = \frac{1}{4}$, independent of the error parameters p_2 and η . The other two fixed points F_{min} and F_{max} (see Fig. 12) are given by the expression

$$F_{\text{max,min}} = \frac{8\eta(\eta-1) + 3 \pm \sqrt{10 - 9/p_2^2 + 64\eta^4 - 128\eta^3 + 116\eta^2 - 52\eta - 36\eta(\eta-1)/p_2^2}}{16\eta(\eta-1) + 4}. \quad (11)$$

They depend on the error parameters and give the borders of the interval within which purification is possible. If $F \in (F_{\text{min}}, F_{\text{max}})$, then $F' > F$. Since F_{max} is an attractor, iterative application of Eq. (9) leads to a resulting pair with fidelity $F \rightarrow F_{\text{max}}$. The value F_{min} thus gives the threshold for F where this purification scheme can be successfully applied,

while F_{max} gives the maximal reachable fidelity. For perfect local operations, $F_{\text{min}} = \frac{1}{2}$ and $F_{\text{max}} = 1$, meaning that all pairs with $F > \frac{1}{2}$ can be purified to $F = F_{\text{max}} = 1$. For imperfect local operations, $F_{\text{min}} > \frac{1}{2}$ and $F_{\text{max}} < 1$, i.e., no perfect EPR pairs can be created. If the error parameters become larger, these two fixed points approach each other and the region

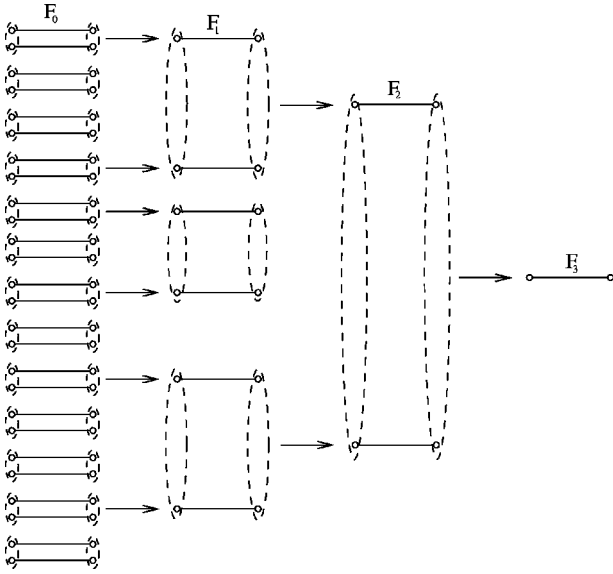


FIG. 2. Typical purification process. At each purification step, either both pairs are discarded (if the purification was not successful) or one pair is discarded (if the purification was successful). The leftover pairs are again used for purification at the next step.

where purification is possible shrinks to zero. The limiting situation $F_{\max} = F_{\min}$ defines the threshold for the applicability of the purification protocol. For all pairs (p_2, η) for which there is only one real fixed point (at $F = 1/4$), the imperfections of the local operations introduce more noise than one gains from the purification, so the scheme breaks down. For example for $\eta = 1$ (perfect measurements), Eq. (11) simplifies to

$$F_{\max, \min} = \frac{3}{4} \pm \frac{1}{4} \sqrt{10 - 9/p_2^2} \quad (12)$$

with the threshold at $p_2 = \sqrt{9/10} \approx 0.95$. That is, the CNOT gate must work with a reliability of at least 95%. The threshold gets tighter when the measurements are imperfect as well, i.e., for $\eta < 1$. In general, the threshold values for the error parameters p_2 and η are of the order of some percent as can be seen in Fig. 3. The fixed points as a function of the error parameters are plotted in Fig. 5, where we set $p_2 = \eta$ to get a two-dimensional plot.

2. Scheme of Deutsch *et al.* (scheme B)

A purification protocol that converges faster and involves fewer resources was proposed by Deutsch *et al.* [12]. Generally speaking, this scheme can be described as a mapping on states that are diagonal in the Bell basis, but need not necessarily be Werner states,

$$\rho_{12} = A|\phi^+\rangle\langle\phi^+| + B|\psi^-\rangle\langle\psi^-| + C|\psi^+\rangle\langle\psi^+| + D|\phi^-\rangle\langle\phi^-|, \quad (13)$$

where $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$ are the Bell states between particles 1 and 2 in the usual notation. In the notation of Eq. (13), the protocol corresponds to a mapping $R^4 \rightarrow R^4$ between the diagonal elements (A, B, C, D) . In particular, between two successive purification steps, the states are not depolarized. This

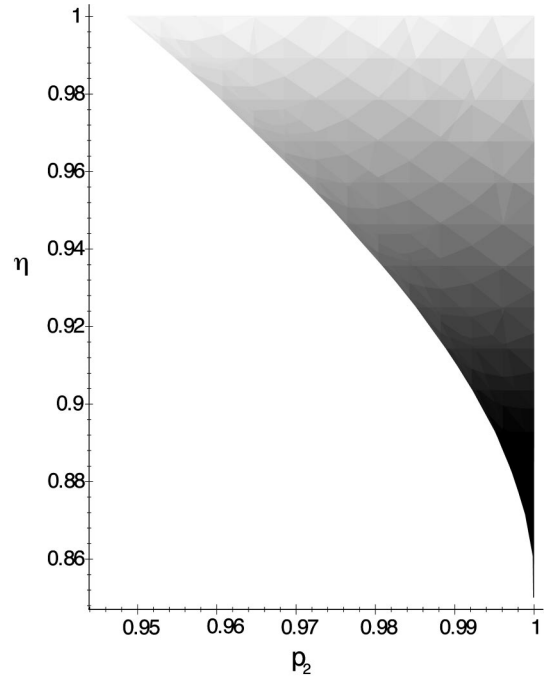


FIG. 3. Region for error parameters p_2 and η where purification is possible (scheme A).

feature, together with additional $\pi/2$ rotations that are applied to the qubits before the CNOT operations, makes scheme B a much faster converging protocol.

In the following analysis, we evaluate scheme B using the imperfect operations (5)–(7) instead of perfect ones. A $\pi/2$ rotation followed by a CNOT operation is thereby treated as a joint two-qubit operation with a single error parameter p_2 . The resulting map between the diagonal elements $R^4 \rightarrow R^4$ is described in [22]; it completely characterizes the action of this purification protocol. Successive purification steps are now described by iterated applications of this map. For each purification step, two identical pairs (which result from the previous step) are used. The resources can be calculated in a similar way as for scheme A.

The fixed points of this map are no longer described by a single parameter F but by a set of four numbers $(A_{\text{fix}}, B_{\text{fix}}, C_{\text{fix}}, D_{\text{fix}})$. The fidelity of such a diagonal Bell state is given by A , the $|\phi^+\rangle$ component, and, for simplicity, we shall continue to call this component the “fixed point” of scheme B, although the fixed point is not sufficiently described by this single parameter. For example, it may happen that a Werner state with a certain fidelity F_0 cannot be purified, while a binary state with the same fidelity F_0 that has only two nonzero components $|\phi^+\rangle$ and $|\psi^+\rangle$, say [in short: “binary state (A, C) ”], can be purified.

We have numerically compared schemes A and B, and found that scheme B converges much faster towards the upper fixed point F_{\max} if $F_0 > F_{\min}$, as can be seen in Fig. 4. Surprisingly, the upper fixed point for scheme B is above the one for scheme A for given error parameters and does not depend on the “shape” of the initial state. The lower fixed point F_{\min} is smaller for scheme B and therefore the interval within which purification is possible is *larger* for scheme B, and so is the maximal reachable fidelity. The fixed points as a function of the error parameters $p_2 = \eta$ are plotted in Fig.

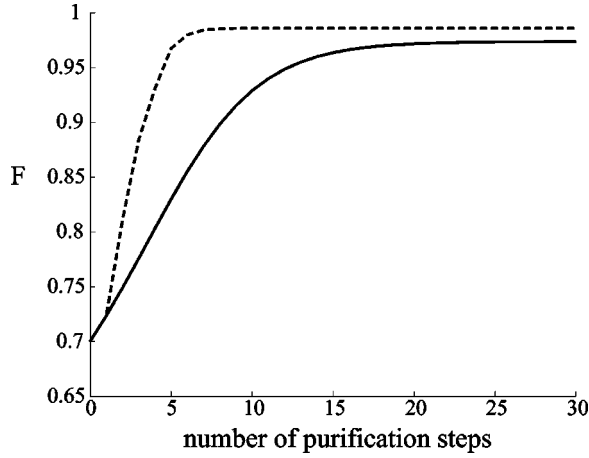


FIG. 4. Fidelity F plotted against the number of successful purification steps for scheme B (dashed line) and scheme A (solid line). Based on fixed error parameters $p_2 = \eta$ of 1% and initial fidelity $F_0 = 0.7$.

5. One can see that scheme B is significantly less sensitive to noisy local operations than scheme A .

3. A modified purification scheme (scheme C)

Both schemes (A and B) need many elementary pairs to start with, which have to be stored somewhere before the protocols are applied. The physical resources are thus quite large and grow with the number of necessary purification steps. In the following, we modify scheme B in a certain way, and call this scheme C .

Different from scheme B , we do not use two identical pairs at each purification step (which are left over from previous purification steps) but always purify one and the same pair with the help of an auxiliary pair π_0 with constant fidelity A_{π_0} . Apart from that, we employ the same protocol (that is, the sequence of local operations and measurements) as in scheme B . The resulting map is thus the same, the only difference being that ρ_{34} is a diagonal Bell state which is constant throughout the whole purification procedure and is given by $(A_{\pi_0}, B_{\pi_0}, C_{\pi_0}, D_{\pi_0})$. This auxiliary pair is repeatedly created before each purification step between two of the

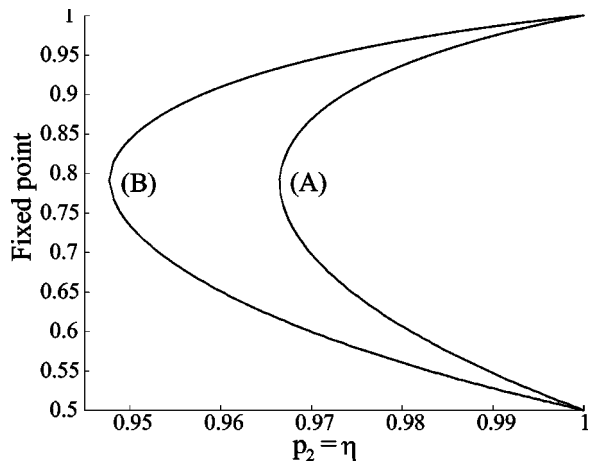


FIG. 5. Fixed point (F_{\min} and F_{\max}) of scheme (A) and scheme (B) plotted against error parameters $p_2 = \eta$.

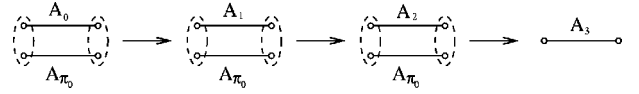


FIG. 6. Typical purification process. At each step, the same elementary pair π_0 is used. If one purification step is not successful, one has to start from the beginning.

four particles as visualized in Fig. 6. If a purification process is not successful, one has to start from the beginning (when both pairs 12 and 34 are put in the state π_0). Using this procedure, the fidelity converges towards a given fixed point $F(\pi_0)$ which is *not* equal to 1 [23]. The fixed point depends sensitively on both the initial fidelity *and* the shape (other diagonal elements in the Bell basis) of the state π_0 . The properties of the fixed point will be discussed in more detail later on.

For ideal operations, this method is generally less favorable as far as its convergence properties are concerned. However, for imperfect operations, the situation changes and the drawback that the reachable fixed point F_{π_0} is smaller than unity becomes less important. As we shall see later, for imperfect local operations the fixed point of scheme C may lie even *above* the fixed points of schemes A and B (see Fig. 8). The main advantage of this scheme is, however, that the *physical resources*, that is, the number of particles needed at A or B to store the pairs, are *constant* (namely two) and independent of the number of necessary purification steps. This fact makes scheme C particularly interesting for the repeater problem, where the accumulation of local particles at the connection points of a compound long channel plays an important role.

The *purification resources*, on the other hand, that is, the (average) number of how often an auxiliary pair has to be created in order to perform k_{\max} purification steps, now have to be calculated in a different way. Let $p_{\text{even}}(k)$ be the probability to succeed at the k th purification step. The total resources can be calculated using the iteration formula

$$M_{k+1} = (M_k + 1) \frac{1}{p_{\text{even}}(k+1)}. \quad (14)$$

To close this formula, note that $M_0 = 1$. This can be understood as follows: Starting at the elementary level, one needs two pairs for purification and has to repeat the procedure on average $1/p_{\text{even}}(1)$ times. Thus $M_1 = (1+1)/p_{\text{even}}(1)$. For the next purification step, one needs one additional elementary pair to perform the next purification step. This step has to be performed on average $1/p_{\text{even}}(2)$ times. The resources to perform the second purification step are thus given by $M_2 = (M_1 + 1)/p_{\text{even}}(2)$ and so on. To perform k_{\max} purification steps, one needs to create on average

$$M_{k_{\max}} = \sum_{i=1}^{k_{\max}} \left[\prod_{k=i}^{k_{\max}} \left(\frac{1 + \delta_{k1}}{p_{\text{even}}(k)} \right) \right] \quad (15)$$

times an auxiliary pair.

A related quantity is the average number of purification steps (including also those which fail). This is given by the iteration formula

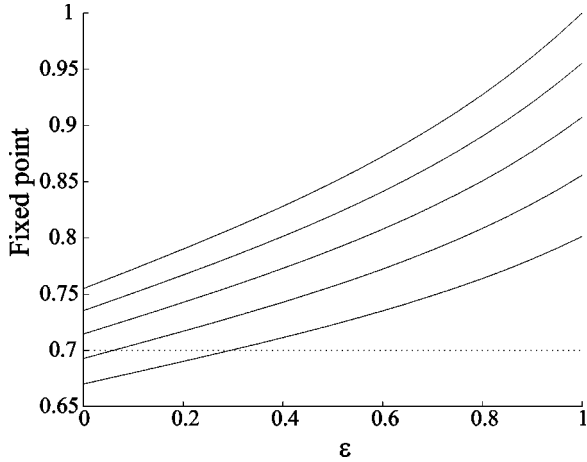


FIG. 7. Reachable fixed point plotted against parametrization parameter ϵ (shape of the state) for fixed initial fidelity $F_0=0.7$. Plots from bottom to top correspond to error parameters $p_2 = \eta$ of 4%, 3%, 2%, 1%, 0%.

$$S_{k+1} = (S_k + 1) \frac{1}{p_{\text{even}}(k+1)}, \quad (16)$$

where $S_0=0$ and k denotes the number of *successful* purification steps. If no purification is performed, the number of steps $S_0=0$. This is the only difference from the iteration formula (15) for the resources, since every time an elementary pair is created, one performs a purification step. Thus the average total number of purification steps performed (assuming that k_{max} steps were successful) is given by

$$S_{k_{\text{max}}} = \sum_{i=1}^{k_{\text{max}}} \left[\prod_{k=i}^{k_{\text{max}}} \left(\frac{1}{p_{\text{even}}(k)} \right) \right]. \quad (17)$$

The fixed point discussion for this purification protocol is more involved due to the many parameters, namely the fidelity A_{π_0} and the shape (other diagonal elements $B_{\pi_0}, C_{\pi_0}, D_{\pi_0}$) of the elementary pair, and the error parameters p_2 and η describing the noisy local operations. For this protocol, purification is possible if the reachable fidelity (fixed point) for a certain auxiliary pair lies above its initial fidelity. To illustrate first the shape dependence of the fixed point, we introduce the following parametrization of diagonal Bell states with constant fidelity F_0 . In the notation of Eq. (13) we write

$$\begin{aligned} A &= F_0, \\ B &= C = (1 - F_0)(1 - \epsilon)/2, \\ D &= (1 - F_0)\epsilon, \end{aligned} \quad (18)$$

where $0 \leq \epsilon \leq 1$. A Werner state thereby described by $\epsilon = \frac{1}{3}$ and a binary state (A, D) is obtained for $\epsilon = 1$. Figure 7 shows the dependence of the fixed point as a function of ϵ for different error parameters.

For the manifold of states covered by this parametrization, one sees that the ‘‘optimum shape’’ of the elementary pair is a binary state (A, D) , meaning that the reachable fixed point for a given initial fidelity is the largest for this shape.

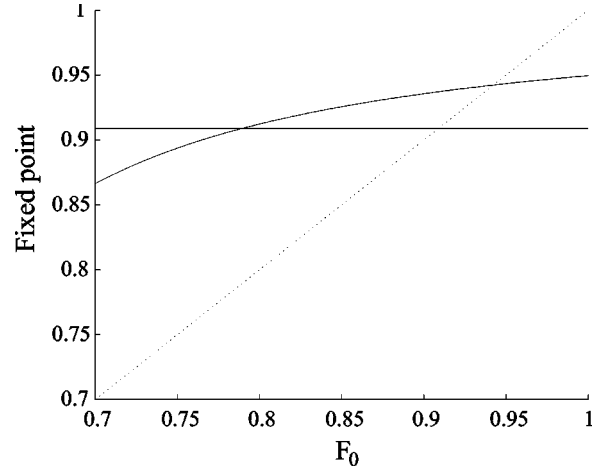


FIG. 8. Reachable fixed point plotted against initial fidelity F_0 for scheme B (constant function) and scheme C . Based on fixed error parameters $p_2 = \eta$ of 4% and binary pairs (A, C) .

Figure 8 demonstrates two different things. First, it shows that the fixed point (maximally reachable fidelity) depends on the initial fidelity of the elementary pair even if the other components are kept constant. Second, it demonstrates that the reachable fidelity using this purification scheme may lie above the reachable fidelity using schemes A or B . [The upper fixed point for scheme A is not plotted here, but as we already know (see Fig. 5) it always lies below the fixed point for scheme B .] One should mention, however, that this is only the case if the shape of the elementary pair is close to the optimal configuration (A, D) . This can be understood as follows: Scheme B always picks two pairs that result from a previous purification step and the shape of such a pair converges towards a ‘‘working state’’ which no longer depends on the initial shape but only on the error parameters. Scheme C , on the other hand, always uses the same auxiliary pair for each purification step which has *not* been influenced by noisy local operations in previous steps. As we have pointed out earlier, in general one can only increase the fidelity by a certain amount.

B. Teleportation

In the context of the quantum repeater, teleportation comes into play when two (purified) segments of a channel are connected. The channel segments are represented by EPR pairs between particles 1-2 and 3-4 that have been created across the corresponding segments, see Fig. 9. In general, to teleport the state of particle 2 to particle 4, a Bell measurement has to be made on particles 2 and 3 (and the result of this measurement communicated particle 4). If particle 2 is itself entangled to some other particle, say particle 1 as in Fig. 9, the effect of the teleportation is to transfer this entanglement to an entanglement between particles 1 and 4. This process has also been termed ‘‘entanglement swapping’’ [24].

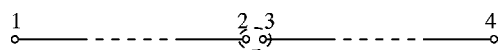


FIG. 9. Particles involved in the connection process. Particle 1 is located at A , particles 2 and 3 at C_1 , and particle 4 at B .

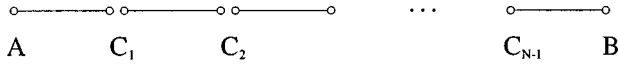


FIG. 10. Connection of a sequence of N EPR pairs.

As a result, one obtains an EPR pair between particles 1 and 4 which can be used as a single channel (again with the help of teleportation). In this sense, the segments of the compound channel have been connected. Put in different terms, the connection process creates quantum correlations across the compound channel from correlations that exist across the individual segments.

We will study this process first for the particular case where the involved pairs (1-2 and 3-4) are not maximally entangled but are both in a Werner state (8) with fidelity F . To connect the pairs (1-2) and (3-4), we make a Bell measurement on particles 2 and 3, which is realized by a (imperfect) CNOT operation followed by two (imperfect) single-particle measurements, as described in the last paragraph of Sec. II. Depending on the outcome of this measurement, a one-particle operation O_4 is performed on particle 4, as in the teleportation scheme [13]. The measurement outcome needs therefore to be sent to particle 4 using classical communication. The result of this sequence of operations, followed by a subsequent (imperfect) depolarization, is a Werner state between particle 1 and 4 with a smaller fidelity F_2 , which is independent of the outcome of the measurement.

More generally, imagine that we have not only two pairs but a whole string of N pairs as visualized in Fig. 10. Each of the pairs $(A - C_1), (C_1 - C_2), \dots, (C_{N-1} - B)$ is assumed to be in a Werner state with fidelity F . Connecting these N pairs using the procedure described above leads to a pair $(A - B)$ with fidelity F_N given by the formula

$$F_N = \frac{1}{4} \left\{ 1 + 3(p_1^2 p_2)^{N-1} \left(\frac{4\eta^2 - 1}{3} \right)^{N-1} \left(\frac{4F - 1}{3} \right)^N \right\}. \quad (19)$$

The parameters η , p_1 , and p_2 appearing in this formula quantify the amount of noise that is introduced by the connection processes. The connection therefore leads to an exponential decrease of the resulting fidelity, unless both the elementary pairs and all the operations involved have unity fidelity.

The connection can be performed in two different ways, which both lead to the same resulting state with fidelity F_N but involve a different temporal ordering of the operations. The first way is to connect the pairs *sequentially*, i.e., first connect at C_1 , then at C_2 , and so on, each time only connecting one additional pair. This involves a sequence of $N - 1$ connection procedures. The second way is to connect the pairs in *parallel*. To achieve this, first connect simultaneously the neighboring pairs at C_1, C_3, \dots, C_{N-1} . This leaves us with longer pairs $(A - C_2), (C_2 - C_4), \dots, (C_{N-2} - B)$. Then connect simultaneously these longer pairs at C_2, C_6, \dots, C_{N-2} , and so on, until we get a final pair between A and B . To have at each step pairs of equal length and fidelity, N should be some power of 2, $N = 2^n$, although this is not an essential requirement. This method is much faster as it requires *fewer* iteration steps, namely $\log_2 N = n$

instead of $N - 1$, although the number of local connections to be made is, of course, the same.

The elementary pairs that are connected need not be in a Werner state. For example, for Bell diagonal states one can derive a map $R^4 \rightarrow R^4$ that relates the elements (A, B, C, D) of the corresponding states before and after the connection. That is, Bell diagonal states are mapped to Bell diagonal states under connection. All other remarks about the connection procedure for a string of pairs apply here as well. The parallel way of connecting the pairs is preferable not only because it can be done faster, but also because, after each connection step, one deals with an ensemble of *identical* pairs. Further details are given in [22].

IV. QUANTUM COMMUNICATION OVER LONG DISTANCES

A. Concept of the quantum repeater: Nested entanglement purification

We have now all necessary tools available to introduce the concept of the quantum repeater. Our goal is to create an EPR pair of high fidelity between two distant locations. Since nonlocal entanglement between distant particles cannot be created using only local operations, this involves the usage of a quantum channel, which is noisy in general. The bottleneck for communication over large distances is the scaling of the error probability with the length of the channel. When using, for example, optical fibers and single photons as a quantum channel, both the absorption losses and the depolarization errors scale *exponentially* with the length of the channel. The state of the photon or the photon itself will therefore be destroyed with almost certainty if the channel is longer than a few half-lengths of the fiber.

To overcome this limitation, we divide the long channel into N smaller segments and create less distant EPR pairs across each segment as visualized in Fig. 10. The number of segments N is thereby chosen in such a way that it is possible to create EPR pairs with sufficiently high initial fidelity $F > F_{\min}$ over the distance of such a segment. In a next step, we connect these “elementary” pairs as described in Sec. III B. This leaves us with a pair between A and B with reduced fidelity F_N as given in Eq. (19). In principle, one could now create many pairs between A and B in a similar way and then use this ensemble of pairs for purification. But purification is only possible if the fidelity of the initial pairs is above a certain threshold value F_{\min} as we have seen in Sec. III A. This limits the number of pairs one can connect before purification becomes impossible. We therefore connect a smaller number $L \ll N$ of pairs so that the resulting fidelity F_L stays above the threshold value for purification ($F_L \geq F_{\min}$) and purification is possible.

The general strategy will be to design an alternating sequence connection and (re)purification procedures in such a way that the number of resources needed remains as small as possible, and in particular does not grow exponentially with N and thus with l . In the remainder of this section we describe a *nested purification protocol* which consists of connecting and purifying certain groups of pairs simultaneously in the following sense (see Fig. 11). For simplicity, assume that $N = L^n$ for some integer n . On the first level, we simultaneously connect the pairs (initial fidelity F_1) at all the

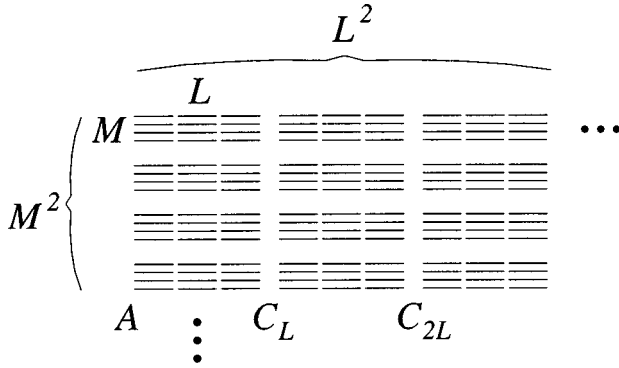


FIG. 11. Nested purification with an array of elementary EPR pairs.

checkpoints except at $C_L, C_{2L}, \dots, C_{N-L}$. As a result, we have N/L pairs of length L (and fidelity F_L) between A and C_L , C_L and C_{2L} , and so on.

To purify these pairs, we need a certain number M of copies that we construct in parallel fashion. (For keeping track of the resources, it is convenient to arrange them in the form of an array of elementary pairs as is done in Fig. 11 for $L=3$ and $M=4$.) We then use these copies on the segments A and C_L , C_L and C_{2L} , etc., to purify and obtain one pair of fidelity $\geq F_1$ on each segment. This last condition determines the (average) number of copies M that we need, which will depend on the initial fidelity, the degradation of the fidelity under connections, and the efficiency of the purification protocol. The total number of elementary pairs we used up to this point is LM . On the second level, we connect L of these larger pairs at every checkpoint C_{kL} ($k=1,2,\dots$) except at $C_{L^2}, C_{2L^2}, \dots, C_{N-L^2}$. As a result, we have N/L^2 pairs of length L^2 between A and C_{L^2} , C_{L^2} and C_{2L^2} , and so on, of fidelity $\geq F_L$. Again, we need M parallel copies of these long pairs to repurify up to a fidelity $\geq F_1$. The total number of elementary pairs involved up to this point is $(LM)^2$. We iterate the procedure to higher and higher levels, until we reach the n th level. As a result, we have obtained a final pair between A and B of length N and fidelity $\geq F_1$. In this way, the total number R of elementary pairs will be $(LM)^n$ (where M^n alone gives the number of required ‘‘parallel channels’’ in Fig. 11). We can reexpress this result in the form

$$R = N^{\log_L M + 1} \quad (20)$$

which shows that the resources grow *polynomially* with the distance N .

The central feature of this nested purification protocol is the two-step process connection-purification on each nesting level. This purification loop is visualized in Fig. 12. The curves shown in this figure are described by the formulas (9) for purification (upper curve), and (19) for connection (lower curve, with N replaced by L), respectively. Let us consider a given nesting level k , where we have N/L^{k-1} pairs of fidelity F each. Starting from F , the fidelity F_L after connecting L pairs can be read off from the curve below the diagonal. Reflecting this value back to the diagonal line, as indicated by the arrows in Fig. 12, sets the starting value for the purification curve. If F_L lies within the purification interval (F_{\min}, F_{\max}) , then the purification curve lies above the diag-

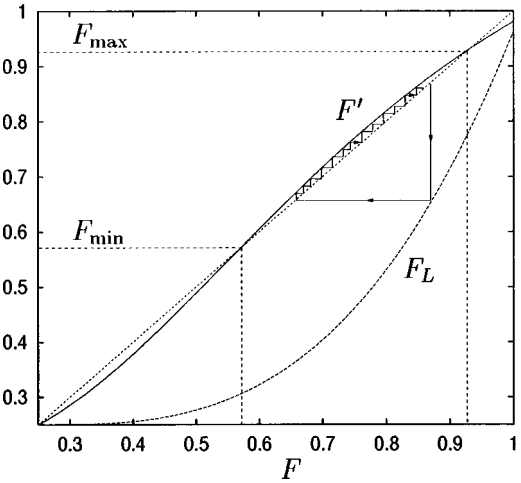


FIG. 12. ‘‘Purification loop’’ for connecting and purifying EPR pairs. The parameters are $L=3$, $\eta=p_1=1$, and $p_2=0.97$. The (upper) purification curve corresponds to scheme A, Eq. (9). The (lower) connection curve is described by Eq. (19) with $N=3$.

onal, $F'(F_L) > F_L$, and iterative application of Eq. (9) leads back to a fidelity larger than or equal to the initial value F . Each step in the ‘‘staircase’’ of Fig. 12 corresponds to a successful purification step, and with the help of the total number of necessary steps k_{\max} needed to recover one can calculate the needed resources M as described in Sec. III A. Once the initial value F of the fidelity is reobtained, we have N/L^k pairs and we can start with the next level $k+1$. In summary, each level in the protocol corresponds to one cycle in Fig. 12.

There are two conditions that have to be fulfilled to realize a closed loop. First, the fidelity after the connection has to be larger than the minimum value for purification (lower fixed point), $F_L > F_{\min}$. If $F_L \leq F_{\min}$, then repurification is impossible. Second, the fidelity F one starts with and wants to reach again has to be smaller than the maximal reachable fidelity (upper fixed point), $F < F_{\max}$. These two conditions determine both a threshold value for the error tolerances of the local operations and they limit the value L (the number of pairs which can be connected before purification becomes necessary). Please note that, being polynomial in L , the lower curve gets steeper and steeper near $F=1$ for higher and higher values of L . From this one can see that, for a given initial fidelity F , there is a maximum number of pairs one can connect before repurification becomes impossible.

The threshold value for the nested purification scheme, i.e., the repeater, is tighter than the threshold for simple purification on a single segment. Consider, as an example, the situation in Fig. 12. The chosen value $p_2=0.97$ of the error parameter (with $\eta=1$) lies above the purification threshold of 0.95 that we have found after Eq. (12). On the other hand, for $p_2=0.95$, the purification interval in Fig. 12 would shrink essentially to a point at $F_{\min}=F_{\max}=0.75$. Clearly, in this situation no loop can be realized; even if we start initially at $F=0.75$, the purification ‘‘interval’’ is left after the first connection process and the fidelity would subsequently converge towards the trivial fixed point $F=0.25$.

When we employ the protocols A or B in the purification part of the nested scheme, we find error thresholds that are typically in the percent region. For scheme C, the situation is

similar, *as long as* we do not use depolarization after each purification step (i.e., keep all involved pairs during the purification process in the Werner form). If we do use depolarization, thus realizing a modified version of protocol *A*, the loop cannot be closed. In other words, for Werner states, the fidelity that is lost by the connection process can never be regained by purification with this scheme. For this to be true, the repurification condition $F_{\max}(F_L(F)) \geq F$ must be fulfilled, where the upper fixed point F_{\max} is a function of the fidelity of the auxiliary L pair. It can be shown analytically that this is not possible for scheme *C* with Werner states. This underlines the fact that the purification scheme *C* is not a trivial variant of either of the schemes *A* and *B*.

Note that both connection and purification are not smooth processes. This means that one can only perform whole steps and not parts of a step. Due to this fact, one will not get an exactly closed purification loop, in general, but the final fidelity after the purification (this is the value at which the ladder in Fig. 12 ends) may be slightly larger than the initial fidelity; second, the final fidelity may be different at each nesting level, but it is always larger than or equal to the fidelity of the elementary pairs.

B. Physical resources

The length of a segment is limited by the transmission errors, and the number of segments N one splits up the total channel should be varied in order to find out the optimal configuration. The quantum repeater can be characterized by two quantities, which depend on the used connection and purification protocol: (i) The total *physical resources per segment* needed to build up the EPR pair—this gives the number of necessary “parallel channels” between two checkpoints; (ii) the *total time* which is needed to build up the EPR pair. The way to calculate these quantities is similar for schemes *A* and *B*, while the properties of scheme *C* are totally different.

C. Physical resources per segment

The number of physical resources (per segment), R_{segment} , is given by the number of required connection lines between two checkpoints. At the end points (at *A* and *B*), R_{segment} is also equal to the number of particles to be stored, while at each checkpoint C_i , the number of particles to be stored is $2R_{\text{segment}}$, since there are connections in both directions.

For schemes *A* and *B*, R_{segment} (vertical axis in Fig. 11) is completely determined by the resources M needed for each purification loop and is given by $R_{\text{segment}} = M^n$, where $n = \log_L N$ is the number of nesting levels. The resources M needed for purification can be calculated as described in Sec. III A. Figure 13 shows the resources M needed for a single purification loop, where it is assumed that $L=2$, i.e., only two pairs are connected before repurification takes place. M is plotted against a “working fidelity,” which is the fidelity one starts with before connection and one ends up with after repurification. Although the difference between schemes *A* and *B* does not look very dramatic, note that M has to be taken to the n th power to calculate the resources per segment, where for long range communication $n \approx 10$ (see Sec. IV E). One can see that there exists an optimal working region, which can be understood as follows: For small working

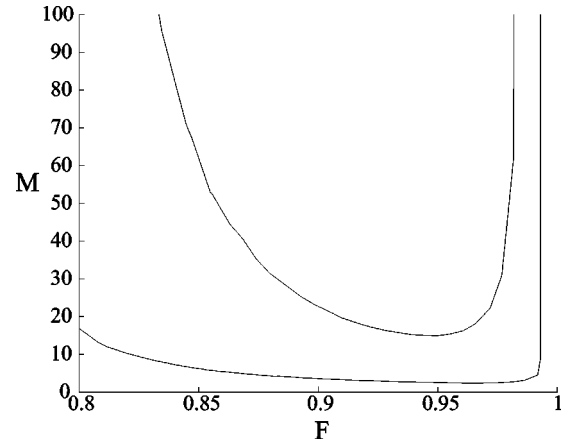


FIG. 13. Resources M for purification versus working fidelity F for scheme *A* (upper curve) and scheme *B* (lower curve). The errors of all operations are 0.5%, and $L=2$.

fidelities F , due to the polynomial law for the connection, the fidelity decreases strongly. Second, purification becomes less effective near the lower fixed point F_{\min} (the gain per purification step gets smaller). For both reasons, many purification steps are needed to recover and thus the needed resources are large. For working fidelities F close to the maximal reachable fidelity (upper fixed point F_{\max}), one does not lose much due to the connection, but purification is less effective—the gain per purification step is smaller. Therefore, the number of necessary steps is again quite large and so are the needed resources. In between there exists a region which is optimal in the sense that the needed resources are minimized. Here a working fidelity $F \approx 0.95$ turns out to be optimal for the chosen error parameters.

The error dependence of the resources is shown in Fig. 14. For smaller error probabilities (larger error parameters), two things happen: the optimal working fidelity gets larger and the needed resources M decrease. For imperfect local operations, the needed resources increase to infinity if one really wants to reach the maximal achievable fidelity F_{\max} , only for perfect operations and $F=1$ this is not true because one starts with perfect pairs and does not lose due to connection. Therefore no purification is necessary and $M=1$.

Using scheme *C* for purification, the situation is different. The vertical axis of Fig. 11 (which corresponds to the resources) is translated into a “temporal axis.” Instead of creating all needed pairs at the beginning and operating parallelly on ensembles of pairs at each checkpoint (as in scheme *A* and *B*), one creates the pairs needed for purification every time one needs one and operates sequentially on the pairs. To perform the purification process, only two pairs are involved every time. One is needed to store the purified state and the other one is repeatedly created to purify the first pair as visualized in Fig. 6. The number of *physical resources* required for purification is thus only two, but every time the purification is not successful one has to start from the very beginning. Using scheme *A* or *B* one obtains a purified pair after k_{\max} successful purification steps, which is in this case also the number of actually performed purification steps. Looking at Fig. 2, one sees that a purification step which was not successful eliminates one branch of the tree, but after four steps (in this example) one ends up with a purified pair.

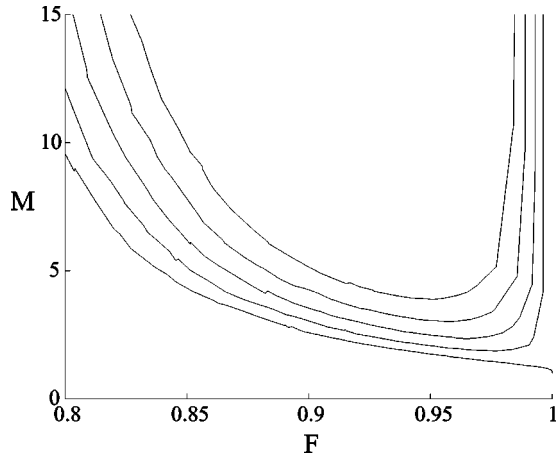


FIG. 14. Resources M versus working fidelity F for different error parameters (scheme B with $L=2$). The curves from bottom to top correspond to error probabilities of 0%, 0.25%, 0.5%, 0.75%, and 1%. The center curve correspond to the lower curve in Fig. 13.

In scheme C , on the other hand, one does not follow all branches parallel but follows the branches sequentially (and using always the same elementary pair for each purification step). This limits the number of involved particles, but increases the required time.

Looking now at the nested algorithm, it turns out that the required number of physical resources for scheme C grows linearly with the number of nesting levels and thus logarithmically with the number of segments (and the distance). This is because one additional pair is needed for storage purposes at each nesting level. One can understand this by inspecting Fig. 15. First, three elementary pairs are connected (line 4) and used to purify the pair at line 3, which now is the ‘‘elementary pair’’ for the next nesting level. Second, three of these repurified pairs (line 3) are connected and used to purify the pair at line 2. Since one has to create such a pair repeatedly and all particles at lines 3 and 4 are involved, it is necessary to store the pair to be purified (here in line 2). Therefore one needs one additional particle to store the pair at each new nesting level (see Fig. 16). This particle is not needed in all checkpoints, but only in those which lie on the *borders* of the corresponding nesting levels. That is why the maximum number of additional particles (physical resources) is required at the outermost places (A and B), while, e.g., at checkpoint C_1 , no additional particle is needed. The *maximal* number of additional particles (physical resources) grows only linearly with the number of nesting levels and

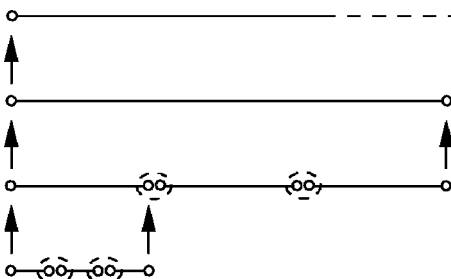


FIG. 15. The nested purification algorithm using the Innsbruck protocol. At each nesting level, one additional particle at the borders of this nesting level is needed to store the pair.

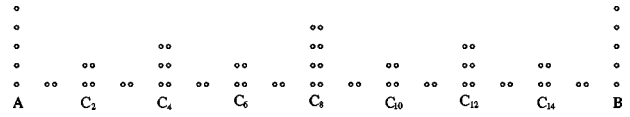


FIG. 16. Additional particles needed at each checkpoint for the Innsbruck protocol. The number of segments $N=2^4=16$, $L=2$ pairs are connected at each nesting level, and the number of nesting levels is $n=4$.

therefore logarithmically with the number of segments in contrast to the polynomially growing resources when using scheme A or B . The maximal resources per segment (in this case particles needed to store the pair) can be calculated by

$$R_{\text{segment}} = 1 + \log_L N = 1 + n. \tag{21}$$

D. Temporal resources

Here we will discuss the total time needed to create an EPR pair. This involves at least three parameters, as follows.

(i) The typical time τ_{op} needed to perform local operations (single qubit, two qubit, and measurements).

(ii) The typical time τ_{pair} to create an elementary pair. Using optical fibers and the model of the absorption free channel (AFC) [26,27], τ_{pair} can be expressed in terms of the other two parameters and is given by

$$\tau_{\text{pair}} = \tau_{\text{AFC}} = (5\tau_{\text{op}} + 2\tau_{\text{class}})e^{(l_{\text{segment}}/l_0)}, \tag{22}$$

where l_0 is the coherence length of the fiber and l_{segment} is the length of a segment. This just reflects the fact that for a single use of the AFC, altogether five operations and two classical communications (in this case the transmission of a photon) are necessary. The exponential function gives the average number of repetitions which are necessary due to absorption losses.

(iii) The time τ_{class} needed for classical communication to broadcast the result of the measurement. τ_{class} is determined by the length of the segment and the speed of light c and is given by

$$\tau_{\text{class}} = \frac{l_{\text{segment}}}{c}. \tag{23}$$

To simplify the discussion, we will assume that the number of pairs L which are connected at each nesting level is some power of 2, $L=2^l$, because in this case the connection process can be performed in parallel. For each connection process, three elementary operations (CNOT, measurement, operation depending on the outcome of the measurement) and classical communication over the distance of one segment are needed. For purification, also three elementary operations (e.g., for scheme A depolarization, bilateral CNOT, and bilateral measurement) and classical communication of the result are necessary.

Using scheme A or B , the time needed to perform a *purification loop* (the connection of $L=2^l$ pairs and repurification, where k_{max} successful purification steps are necessary) at nesting level m is given by

$$t_{\text{loop}}(m) = 3l\tau_{\text{op}} + f(m)(2^l - 1)\tau_{\text{class}} + k_{\text{max}}[3\tau_{\text{op}} + f(m)2^l\tau_{\text{class}}], \quad (24)$$

where $f(m) = (2^l)^m$ gives the length dependence of the elementary pair on the nesting level. The first two terms give the time required to perform the connection process in parallel fashion, where l connections and classical communication over the distance of $(2^l - 1)$ times the length of an elementary pair is needed. The purification process involves k_{max} purification steps and for each purification step classical communication over the distance of 2^l times the length of an elementary pair (since $L = 2^l$ pairs were connected before). One only has to take into account the successful purification steps, since one runs through the whole purification tree (see Fig. 2) in a parallel fashion. To calculate the total time needed to perform the nested algorithm, one can use the iteration formula

$$t_{\text{tot}}(m) = t_{\text{tot}}(m-1) + t_{\text{loop}}(m), \quad (25)$$

where m corresponds to the m th nesting level and $t_{\text{tot}}(n)$ gives the total time needed for the creation of an EPR pair between A and B . To complete this iteration formula, note that $t_{\text{tot}}(0) = \tau_{\text{pair}}$, which is just the time needed to create an elementary pair at the beginning. The total time if one has $N = L^n$ segments and $L = 2^l$ is thus

$$t_{\text{tot}}^{A,B} = n(3l + 3k_{\text{max}})\tau_{\text{op}} + \left[2^l - 1 + k_{\text{max}}2^l \left(\frac{(2^l)^n - 1}{2^l - 1} \right) \right] \tau_{\text{class}} + \tau_{\text{pair}}. \quad (26)$$

The main contribution is given by the classical communication if τ_{op} is not too large and is just $t_{\text{tot}} \approx (2k_{\text{max}} + 1)N\tau_{\text{class}}$.

Using scheme C for purification, the time needed to perform a purification loop on nesting level m is given by

$$t_{\text{loop}}(m) = [\max\{t_{\text{loop}}(m-1)\} + 3l\tau_{\text{op}} + f(m)(2^l - 1)\tau_{\text{class}}]M + S(3\tau_{\text{op}} + f(m)2^l\tau_{\text{class}}), \quad (27)$$

where the first term is the time needed to create a pair for purification [by building up 2^l pairs at nesting level $(m-1)$ and connecting them], which must be done *sequentially* M times. The second term gives the time needed for purification (operations and classical communication over the distance of 2^l times the length of an elementary pair), where S purification steps have to be performed. The function $f(m) = (2^l)^m$ reflects the length dependence of the elementary pair on the nesting level and the time needed to create an elementary pair at the lowest nesting level $\tau_{\text{pair}} = t_{\text{loop}}(0)$, which completes this iteration formula. The maximum appearing in this expression is taken over all 2^l segments on nesting level $(m-1)$, which is necessary because all 2^l new elementary pairs have to be built up before the next connection process can start. Therefore one has to wait for the slowest one. Note that the time for purification is fixed for schemes A and B (obtaining bad results in this case corresponds to the elimination of a branch in Fig. 2), while for scheme C the purifi-

TABLE I. Resources and time needed for creating a distant EPR pair via optical fibers. See text for more details.

	Continental scale		Intercontinental scale	
	Resources	Time	Resources	Time
A	1.58×10^9	3.88×10^{-2}	9.01×10^{12}	0.298
B	329	1.34×10^{-2}	4118	0.103
C	7	0.77	10	15.69

cation process has to be started from the very beginning when obtaining a bad result. This results in the fact that the performed purification steps S and the used purification resources M (and therefore the required time) might vary from case to case. This formula is sufficient to calculate the total time needed to perform the nested algorithm up to nesting level m and $t_{\text{tot}}(n) = t_{\text{loop}}(n)$ gives the total time needed to build up an EPR pair between A and B .

A rough estimation of the total time can be obtained when using Eqs. (15) and (17) to calculate the *average* number of purification resources M and purification steps S . In this case, one can write down a closed expression for the total time, which is polynomially growing with the number of segments N and thus with the distance. Comparing this time with the results obtained from a simulation of the whole process, it turns out to be smaller by a factor of ≈ 3 . In some sense, the vertical axis (physical resources) in Fig. 11 is translated into a temporal axis.

E. Comparison of the three schemes

We will give some typical numbers to quantify the properties of the nested purification protocol if the purification loop is performed with the help of scheme A , B , or C . Table I is based on error parameters of $\frac{1}{2}\%$ ($p_1 = p_2 = \eta = 0.995$) and a working fidelity $F = 0.96$, the fidelity one starts with at the lowest nesting level and one ends up after each purification loop. The length of a segment is assumed to be on the order of the coherence length of an optical fiber, $l_{\text{segment}} \approx 10$ km. In this case, the number of segments is proportional to the distance between two locations. If the number of segments is on the order of $N = 2^7 = 128$, this will be called the ‘‘Continental scale’’ (distance of ≈ 1000 km), while $N = 2^{10} = 1024$ is called the ‘‘Intercontinental scale’’ (distance of ≈ 10000 km), since one can create an EPR pair between two international cities. It is assumed that the connection is performed in parallel. The columns from left to right have the following meaning: (i) *resources*: gives the *physical* resources per segment R_{segment} ; (ii) *time*: gives the total time in seconds needed to create an EPR pair. The number is based on the application of the AFC to create elementary pairs ($\tau_{\text{pair}} = \tau_{\text{AFC}} = 3.2 \times 10^{-4}$ s). The coherence length of the fiber is considered to be 10 km, which is also the length of the elementary segment ($\tau_{\text{class}} = 0.33 \times 10^{-4}$ s). All operations (single-qubit, two-qubit, measurement) are considered to be performed in $\tau_{\text{op}} = 10^{-5}$ s. The time is calculated using a simulation of the nested entanglement purification process, averaging over a few hundred runs.

In Table I one sees that the physical resources needed when using scheme C are some orders of magnitude smaller, while the time needed is larger. For a practical implementa-

tion, the achievable bit rates are not very impressive, but note that all numbers get much better if the local operations can be performed better (error parameters closer to 1) as can be seen in Fig. 14.

So the reachable fidelity is larger and at the same time the required resources are smaller when using better local operations. Note that the total time needed is on the order of the time for classical communication over this distance, which is just $t_{\text{class}} = 10\,240 \text{ km}/3 \times 10^5 \text{ km/s} = 0.034 \text{ s}$.

V. SUMMARY

We have shown that it is possible to create EPR pairs via a noisy channel, with an overhead in physical resources that grows only logarithmically with the length of the channel,

while the time needed for the creation grows polynomially. The central idea is to use a nested purification protocol for connecting a sequence of EPR pairs at certain “connection points” within the channel, whose roles are reminiscent of classical repeaters. Different from the classical situation, the concept of the quantum repeater is not a local amplifier, but it involves both the local checkpoints and global purification protocol. Our scheme tolerates errors for local operations and measurements that are in the percent region.

ACKNOWLEDGMENTS

This work was supported in part by the Österreichischer Fonds zur Förderung der wissenschaftlichen Forschung, and by the European TMR network ERB-FMRX-CT96-0087.

-
- [1] B. Schumacher, *Phys. Rev. A* **54**, 2614 (1996); B. Schumacher and M. D. Westmoreland, *ibid.* **56**, 131 (1997).
 - [2] W. K. Wootters and W. H. Zurek, *Nature (London)* **299**, 802 (1982).
 - [3] D. Dieks, *Phys. Lett.* **92A**, 271 (1982).
 - [4] R. J. Glauber, in *Frontiers in Quantum Optics*, edited by E. R. Pike and S. Sarkar (Adam Hilger, Bristol, 1986), pp. 534–582.
 - [5] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin, Los Alamos Report quant-ph/9707042 (unpublished).
 - [6] For optical fibers, this length is typically 10 km; see, e.g., [5].
 - [7] P. Shor, e-print quant-ph/9605011 (unpublished); A. M. Steane, *Phys. Rev. Lett.* **78**, 2252 (1997); D. Gottesman, quant-ph/9702029 (unpublished); for a review see, e.g., J. Preskill, e-print quant-ph/9712048 (unpublished).
 - [8] E. Knill and R. Laflamme, e-print quant-ph/9608012 (unpublished); see also D. Aharonov and M. Ben-Or, e-print quant-ph/9611025 (unpublished); C. Zalka, e-print quant-ph/9612028 (unpublished).
 - [9] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).
 - [10] C. H. Bennett, D. V. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
 - [11] N. Gisin, *Phys. Lett. A* **210**, 151 (1996).
 - [12] D. Deutsch, A. Ekert, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).
 - [13] C. H. Bennett, C. H. Brassard, C. Crepeau, R. Josza, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
 - [14] A. K. Ekert, *Phys. Rev. Lett.* **70**, 661 (1991).
 - [15] G. Giedke *et al.*, e-print quant-ph/9809043 (unpublished).
 - [16] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* (to be published).
 - [17] C. Miquel, J. P. Paz, and W. H. Zurek, *Phys. Rev. Lett.* **78**, 3971 (1997).
 - [18] A similar form as in Eq. (4) may be obtained for two-bit rotations with a corresponding isotropic noise function, although the calculation is more complicated. In particular, we have not yet been successful in giving proof in terms of a manifest *parametrization-independent average* over the invariant group manifold of SU(4). Isotropic noise in this case means that the depolarizing channel does not distinguish between the two qubits and acts on them in a symmetric way.
 - [19] The twirl is realized by (random) one-qubit operations described by the error parameter p_1 . Since one can perform instead of the twirl followed by a \mathcal{C} operation a *joined two-qubit operation*, which is described by a single error parameter p_2 , the error parameter p_1 does not appear in formula (9), although the (noisy) depolarization is already included.
 - [20] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Associate Press, London, 1976).
 - [21] Any sequence of operations at the same node, e.g., two single qubit operations $O_1 \otimes O_2$ followed by a \mathcal{C} operation, will be described by a single two-qubit operation O_{12} and consequently with only a single error parameter.
 - [22] W. Dür, Master thesis, available under <http://www.uibk.ac.at/c7/c705/staff/wd.html>
 - [23] See also N. Lütkenhaus (unpublished).
 - [24] A. Zeilinger *et al.*, *Phys. Rev. Lett.* **78**, 3031 (1997). In their scheme, however, a three-particle entangled state is obtained rather than a distant EPR pair.
 - [25] This procedure is not necessary, but to have a consistent model for both connection and purification, we want to describe all operations in terms of Eqs. (6) and (7).
 - [26] S. J. van Enk, J. I. Cirac, and P. Zoller, *Science* **279**, 205 (1998).
 - [27] S. J. van Enk, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **78**, 4293 (1997).