

## Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication

H.-J. Briegel,<sup>1,2,\*</sup> W. Dür,<sup>1</sup> J. I. Cirac,<sup>1,2</sup> and P. Zoller<sup>1</sup>

<sup>1</sup>*Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*

<sup>2</sup>*Departamento de Física, Universidad de Castilla-La Mancha, 13071 Ciudad Real, Spain*

(Received 20 March 1998)

In quantum communication via noisy channels, the error probability scales exponentially with the length of the channel. We present a scheme of a quantum repeater that overcomes this limitation. The central idea is to connect a string of (imperfect) entangled pairs of particles by using a novel nested purification protocol, thereby creating a single distant pair of high fidelity. Our scheme tolerates general errors on the percent level, it works with a polynomial overhead in time and a logarithmic overhead in the number of particles that need to be controlled locally. [S0031-9007(98)08063-6]

PACS numbers: 03.67.Hk, 03.65.Bz, 42.50.-p

Quantum communication deals with the transmission and exchange of quantum information between distant nodes of a network. Remarkable experimental progress has been reported recently, for example, on secret key distribution for quantum cryptography [1,2], teleportation of the polarization state of a single photon [3,4], and the creation of entanglement between different atoms [5]. On the other hand, first steps towards the implementation of quantum logical operations, which are the building blocks of quantum computing, have been demonstrated [6]. In view of this progress, it is not farfetched to expect the creation of small quantum networks in the near future. Such networks will involve nodes, where qubits are stored and locally manipulated, and which are connected by quantum channels over which communication takes place by sending qubits. This will open the possibility for more complex activities such as multiparty communication and distributed quantum computing [7].

The bottleneck for communication between distant nodes is the scaling of the error probability with the length of the channel connecting the nodes. For channels such as an optical fiber, the probability for both absorption and depolarization of a photon (i.e., the qubit) grows exponentially with the length  $l$  of the fiber. 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  $l$ . One may think that this last problem can be circumvented by standard purification schemes [8–10]. However, purification schemes require a certain minimum fidelity  $F_{\min}$  to operate, which cannot be achieved as  $l$  increases. Furthermore, in any realistic situation, the operations that are part of the purification protocol are themselves imperfect, and this defines a maximum attainable fidelity  $F_{\max}$  and limits the efficiency of the scheme. For this reason, it is not obvious, first, what the allowed error tolerances of local operations are for entanglement purification to be applicable at all and, second, how the resources that are needed for purification grow with the length of the channel. In the experiments,

the distance between the nodes is presently limited by (a few times) the absorption length of the fiber [11].

The theory of fault-tolerant quantum computing [12] implies that any computation can be performed with polylogarithmic cost in time and space [13], if the error probability for each gate operation can be made sufficiently small. A special case of a computation is the transmission of information, for which these fault-tolerant methods must therefore have the same (or a better) asymptotic complexity. An explicit scheme for quantum transmission has been discussed by Knill and Laflamme, using concatenated quantum codes [14]. Their method requires one to encode a single qubit into an entangled state of a polynomially large number of qubits, and to operate on this code repeatedly during the transmission process. The tolerable error probabilities for transmission are less than  $10^{-2}$ , whereas for local operations they are less than  $5 \times 10^{-5}$ . 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.

In this Letter, we present a model of a *quantum repeater* that allows the creation of an entangled (EPR) pair of particles over arbitrary large distances with a tolerability of errors in the percent region. Once an EPR pair is created, it can be employed to teleport any quantum information [15,16]. Our solution of this problem comprises three novel elements: (i) entanglement *purification with imperfect means*, including analytic results for the range and the working conditions of standard protocols; (ii) a method for creation of entanglement between particles at distant nodes that uses auxiliary particles at intermediate “connection points” and a *nested purification protocol*; (iii) a scheme for which the time needed for entanglement creation scales polynomially whereas the required material resources per connection point grow only *logarithmically* with the distance. Since our model is based on two-way classical communication, it is qualitatively different from

quantum error correction. By exploiting this property we will obtain a higher efficiency and significantly more favorable error tolerances.

In classical communication, the problem of exponential attenuation can be overcome by using repeaters at certain points in the channel, which amplify the signal and restore it to its original shape. Guided by these ideas, for quantum communication, we divide the channel into  $N$  segments with connection points (i.e., auxiliary nodes) in between. We then create  $N$  elementary EPR pairs of fidelity  $F_1$  between the nodes  $A$  and  $C_1$ ,  $C_1$  and  $C_2, \dots, C_{N-1}$  and  $B$ , as in Fig. 1(a). The number  $N$  is chosen such that  $F_{\min} < F_1 \leq F_{\max}$ . Subsequently, we connect these pairs by making Bell measurements at the nodes  $C_i$  and classically communicating the results between the nodes as in the schemes for teleportation [15] and entanglement swapping [15,17]. Unfortunately, with every connection, the fidelity  $F'$  of the resulting pair will decrease: on the one hand, the connection process involves imperfect operations which introduce noise; on the other hand, even for perfect connections, the fidelity decreases. Both effects lead to an exponential decrease of the fidelity  $F_N$  with  $N$  of the final pair shared between  $A$  and  $B$ . Eventually, the value of  $F_N$  drops below  $F_{\min}$ , and therefore it will not be possible to increase the fidelity by purification. The number of pairs  $L \ll N$  that may be connected by this method seems therefore to be restricted by the condition  $F_L > F_{\min}$ .

Our proposal, the *nested purification protocol*, combines the methods of entanglement swapping and purification into a single (meta) protocol that circumvents this restriction. 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 of the 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. 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

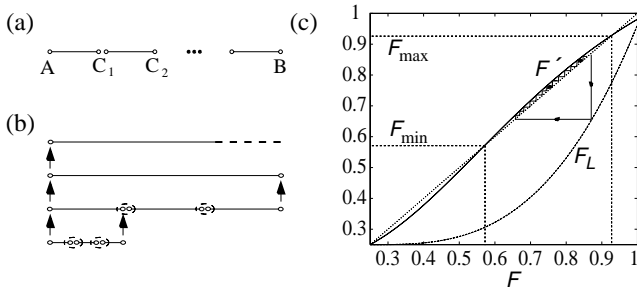


FIG. 1. (a) Connection of a sequence of  $N$  EPR pairs; (b) nested purification with repeated creation of auxiliary pairs; (c) "purification loop" for connecting and purifying EPR pairs. Parameters are  $L = 3$ ,  $\eta = p_1 = 1$ , and  $p_2 = 0.97$ .

on the initial fidelity, the degradation of the fidelity under connections, and the efficiency of the purification protocol. The total number of elementary pairs involved in constructing one of the more distant pairs of length  $L$  is  $LM$ . On the second level, we connect  $L$  of these more distant 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 the fidelity  $\geq F_1$ . The total number of elementary pairs involved in constructing one pair of length  $L^2$  is thus  $(LM)^2$ . 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  $(LM)^n$ . We can reexpress this result in the form

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

which shows that the resources grow polynomially with the distance  $N$ . A similar formula was obtained in [14] for the overhead required in propagating the concatenated quantum code. Note that  $R$  depends only on  $L$  and  $M$ . In order to evaluate  $M$ , we need to know the specific form of the error mechanisms involved in the purification and connections, which in turn depend on the specific physical implementation of the quantum network. In general, we have only limited knowledge of these details. In order to estimate  $M$ , we will choose a generic error model for imperfect operations and measurements.

We define *imperfect operations* on states of one or more qubits by the following maps:

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

$$\rho \rightarrow O_{12} \rho = p_2 O_{12}^{\text{ideal}} \rho + \frac{1-p_2}{4} \text{tr}_{12}\{\rho\} \otimes I_{12}, \quad (3)$$

the first of which describes an imperfect one-qubit operation on particle 1, and the second an imperfect two-qubit operation on particles 1 and 2. In these expressions,  $O^{\text{ideal}}$  is the *ideal* operation, and  $I_1$  and  $I_{12}$  denote unit operators on the subspace where the ideal operation acts. The quantities  $p_1$  and  $p_2$  measure the *reliability* of the operations. The expressions (2) and (3) describe a situation where we have no knowledge about the result of an error occurring during some operation ("depolarization"), except that it happens with a certain probability  $(1 - p_j)$ . Any sequence of two one-qubit operations on the same qubit is equivalent to a single one-qubit operation, and is therefore described by a single parameter  $p_1$ . Similarly, a sequence of a two- and a one-qubit operation counts as a single two-qubit operation and is thus described by  $p_2$ . An *imperfect measurement* on a single qubit in the computational basis is described by a POVM (positive-operator-valued measure) corresponding to

$$P_0^\eta = \eta |0\rangle\langle 0| + (1 - \eta) |1\rangle\langle 1|, \quad (4)$$

$$P_1^\eta = \eta |1\rangle\langle 1| + (1 - \eta) |0\rangle\langle 0|.$$

The parameter  $\eta$  is a measure for the quality of the projection onto the basis states. For example, for the state  $\rho = |0\rangle\langle 0|$  the measuring apparatus will give the wrong result (“1”) with probability  $1 - \eta \geq 0$ . A detailed discussion of this and more general models for imperfect operations will be given elsewhere [18]. With these error models, we have a toolbox to analyze all of the processes involved in the connection and purification procedures. For example, the Bell measurement required in the connection can be decomposed into a controlled-NOT (CNOT) operation, effecting, e.g.,  $|0\rangle|0\rangle \pm |1\rangle|1\rangle \rightarrow (|0\rangle \pm |1\rangle)|0\rangle$ , followed by two single-qubit measurements.

The basic elements of the nested purification protocol are (i) pair connections and (ii) purification. In the following we analyze these elements using the error models introduced above. Assume now that all of the pairs in Fig. 1(a) are in Werner states (see [8]). These states can be produced using depolarization (as in Ref. [8]) after each connection and purification process. This depolarization

works even in the presence of errors which we take into account. Connecting  $L$  neighboring pairs as explained earlier, one obtains a new “ $L$  pair” with fidelity

$$F_L = \frac{1}{4} + \frac{3}{4} \left( \frac{p_1^2 p_2 (4\eta^2 - 1)}{3} \right)^{L-1} \left( \frac{4F - 1}{3} \right)^L. \quad (5)$$

This formula describes an exponential decrease of the resulting fidelity, unless both the elementary pairs and all of the operations involved in the connection process are perfect. There are several possibilities to do the purification, and we first analyze the scheme introduced by Bennett *et al.* [8] in the case of imperfect gate and measurement operations. In short, the scheme takes two adjacent  $L$  pairs of fidelity  $F$ , performs local (1-bit and 2-bit) operations on the particles at the same ends of the pairs, and obtains with a certain probability  $p_{\text{succ}}$  a new pair of fidelity

$$F' = \frac{[F^2 + (\frac{1-F}{3})^2][\eta^2 + (1-\eta)^2] + [F(\frac{1-F}{3}) + (\frac{1-F}{3})^2][2\eta(1-\eta)] + (\frac{1-p_2^2}{8p_2^2})}{[F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2][\eta^2 + (1-\eta)^2] + [F(\frac{1-F}{3}) + (\frac{1-F}{3})^2][8\eta(1-\eta)] + 4(\frac{1-p_2^2}{8p_2^2})}. \quad (6)$$

The value of  $p_{\text{succ}}$  is given by  $p_2^2$  times the denominator of this expression. For perfect operations,  $\eta = 1$  and  $p_2 = 1$ , (6) reduces to the formula given in Ref. [8].

Figure 1(c) shows the curves for connection (5) and purification (6) for a certain set of parameters. The purification curve has three intersection points with the diagonal, which are the real fixpoints of the map (6). In addition to the trivial point at  $F = 1/4$ , there are two nontrivial fixpoints. The upper point,  $F_{\text{max}} < 1$ , is an attractor and gives the maximum value of the fidelity beyond which no pair can be purified. Note also the existence of the minimum value  $F_{\text{min}} > 1/2$ . Together, they define the interval within which purification is possible. The limiting situation  $F_{\text{max}} = F_{\text{min}}$  defines the threshold for the applicability of the purification protocol. For all pairs  $(p_2, \eta)$  for which there is only one real fixpoint (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  $\eta = 1$  the threshold is at  $p_2 \approx 0.95$ ; that is, the CNOT gate must work with a reliability of 95%, at least. Please note that the fixpoints and the threshold condition can all be given analytically from (6). The connection curve, which looks like a simple power in Fig. 1(c), stays below the diagonal for all values of  $F$  between  $1/4$  and  $1$ . The offset of this curve at  $F = 1$  from the ideal value  $F' = 1$  quantifies the amount of noise that is introduced through imperfect operations in the connection process.

With the above results, we can now analyze the nested purification protocol. Let us consider a given level  $k$  in this protocol, where we have  $N/L^{k-1}$  pairs of fidelity  $F$  each. The two-step process connection-purification can now be visualized as follows [see Fig. 1(c)]. 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. 1(c), sets the starting value for the purification curve. If  $F_L$  lies within the purification interval, then iterated application of (6) leads back to the initial value  $F$  (staircase). Once the initial value  $F$  is reobtained, we have  $N/L^k$  pairs and we can start with the level  $k + 1$ . In summary, each level in the protocol corresponds to one cycle in Fig. 1(c). Note that if, in the loop,  $F_L \leq F_{\text{min}}$  then purification is not possible. Being polynomial in  $F$ , the lower curve gets steeper and steeper near  $F = 1$  for higher values of  $L$ . From this, one sees that for a given starting fidelity  $F$ , there is a maximum number of pairs one can connect before purification becomes impossible.

For the resources we obtain  $M = \prod_m^{m_{\text{max}}} 2/p_{\text{succ}}^{(m)}$ , where  $p_{\text{succ}}^{(m)}$  is the probability of obtaining the required outcome (00 or 11) in the measurement at the  $m$ th purification step. The total number of steps,  $m_{\text{max}}$ , is the same as in the staircase of Fig. 1(c).

In Fig. 2(a),  $M$  is plotted against the working fidelity  $F$ . Because of the discrete nature of the purification process, the fidelity of the repurified pairs need not be exactly the same on each nesting level. The working fidelity is thus defined as the fidelity maintained *on average* when going through different nesting levels. The error parameters for this plot are  $\eta = p_1 = p_2 = 0.995$ . One can see that there exists an optimum working fidelity of about 0.94 which requires a minimum number of about 15 resources.

A purification protocol that converges faster and therefore involves less parallel channels was proposed by Deutsch *et al.* [9]. We have employed this protocol,

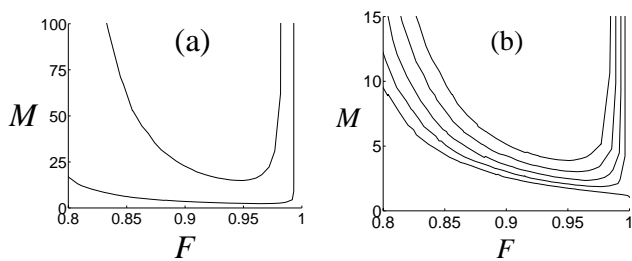


FIG. 2.  $M$  (see text) versus working fidelity  $F$ . (a) Realization of the repeater with the aid of the purification schemes of Refs. [8] (upper curve) and [9] (lower curve). The error probabilities of all operations are 0.5% (error parameters 0.995), and  $L = 2$ . (b) Lower curve in (a) for different error probabilities. From bottom to top: 0%, 0.25%, 0.5%, 0.75%, 1%.

using imperfect operations (2)–(4). As is demonstrated in Fig. 2(a),  $M$  can be reduced by a factor of the order of 10. Since this number has to be taken to the  $n$ th power, this reduces the number of total resources that are required at each connection point by many orders of magnitude. In Fig. 2(b),  $M$  is plotted versus the working fidelity for different error parameters. One can see that for errors in the one percent region, a working fidelity can be maintained with, on average, five  $L$  pairs on each nesting level. We note that the procedure also works for error probabilities up to about 3%, but the number of purification resources gets larger.

In the remainder of this paper, we propose a method for which the resources grow only logarithmically with the distance, whereas the total *time* needed for building the pair scales polynomially. Imagine that we purify a pair not with the help of  $M$  copies, but instead with one auxiliary pair of constant fidelity  $\pi_0$  that is repeatedly created at each purification step. The purification with the help of such a pair leads to a maximum achievable fidelity  $F_{\max}(\pi_0)$  that depends on the value of  $\pi_0$  and, more generally, on the state of the auxiliary pair. This purification method is different from the standard schemes [8,9], and the purification limit  $F_{\max}$  is usually smaller than for the distillation method. In the context of the repeater protocol, it is therefore not *a priori* clear whether the fidelity that is lost by the connection process can be regained with this method.

When connecting  $L$  pairs of fidelity  $F$  as in Fig. 1(b), we obtain a resulting  $L$  pair of fidelity  $\pi_0 \equiv F_L$ . In the first step, this pair is swapped to two auxiliary particles at the ends of the  $L$  pair, as indicated by the arrows in Fig. 1(b). In the next step, an  $L$ -pair of fidelity  $\pi_0$  is again created by using the same string of particles as before, which is now used to purify the pair stored between the auxiliary particles. This procedure can be iterated and thus the stored pair be purified back to the fidelity  $F$  given that the nesting condition  $F_{\max}(F_L) > F$  is satisfied. If this is the case, then the same procedure can be applied at higher levels, thereby purifying correlations between more and more distant particles as indicated in

Fig. 1(b). Here, the dependence of the fixpoint on the form of the auxiliary pair becomes quite important: When we use our method together with the recurrence protocol of Ref. [8], which is based on Werner states, the fixpoint  $F(\pi_0)$  is too small and the nesting condition cannot be satisfied for any  $L \geq 2$ . On the other hand, the nesting condition can be satisfied if we adopt a similar sequence of local operations as in Ref. [9], which does not involve a depolarization to Werner states.

Using this method, the vertical axes in Fig. 2 are essentially translated into temporal resources [18]. On the other hand, the number of particles at each node [see Fig. 1(b)] increases by unity with every additional nesting level, and thus depends only logarithmically on the distance between the initial and the final node. In the context of a quantum optical implementation [19], for example, this would correspond to the number of ions that need to be controlled in a cavity at each node [20]. Note, however, that this method requires perfect memory during the process. In this particular implementation, the storage decoherence time is orders of magnitude longer than the estimated duration of the process [20].

This work was supported in part by the Austrian Science Foundation, and by the TMR network ERB-FMRX-CT96-0087.

\*On leave from Institut für Theoretische Physik, Universität München, Theresienstrasse 37, D-80333 München, Germany.

- [1] W. Tittel *et al.*, Phys. Rev. Lett. **81**, 3563 (1998).
- [2] W. T. Buttler *et al.*, Phys. Rev. Lett. **81**, 3283 (1998).
- [3] D. Bouwmeester *et al.*, Nature (London) **390**, 575 (1997).
- [4] D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).
- [5] E. Hagley *et al.*, Phys. Rev. Lett. **79**, 1 (1997).
- [6] C. Monroe *et al.*, Phys. Rev. Lett. **75**, 4714 (1995); Q. A. Turchette *et al.*, *ibid.* **75**, 4710 (1995).
- [7] L. K. Grover, quant-ph/9704012.
- [8] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).
- [9] D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996).
- [10] N. Gisin, Phys. Lett. A **210**, 151 (1996).
- [11] For optical fibers, this length is typically 10 km (see [1]).
- [12] P. Shor, quant-ph/9605011; A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997).
- [13] E. Knill, R. Laflamme, and W. Zurek, Science **279**, 342 (1998); D. Aharonov and M. Ben-Or, quant-ph/9611025; A. Yu. Kitaev, Russ. Math. Surv. **52**, 1191 (1997).
- [14] E. Knill and R. Laflamme, quant-ph-9608012.
- [15] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
- [16] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
- [17] M. Zukowski *et al.*, Phys. Rev. Lett. **71**, 4287 (1993).
- [18] W. Dür *et al.*, quant-ph/9808065; G. Giedke *et al.*, quant-ph/9809043.
- [19] S. J. van Enk *et al.*, Phys. Rev. Lett. **78**, 4293 (1997); Science **279**, 205 (1998).
- [20] For a distance of 1280 km and a local node every 10 km [11], this amounts to, e.g.,  $7 = \log_2(128)$  particles per node and an estimated purification time of less than 1 s [18].