Role of memory errors in quantum repeaters

L. Hartmann,[1] B. Kraus,[1] H.-J. Briegel,[1,2] and W. Dür[1,2]
[1]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria*
[2]*Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften, Innsbruck, Austria*

(Received 17 November 2006; published 8 March 2007)

We investigate the influence of memory errors in the quantum repeater scheme for long-range quantum communication. We show that the communication distance is limited in standard operation mode due to memory errors resulting from unavoidable waiting times for classical signals. We show how to overcome these limitations by (i) improving local memory and (ii) introducing two operational modes of the quantum repeater. In both operational modes, the repeater is run blindly, i.e., without waiting for classical signals to arrive. In the first scheme, entanglement purification protocols based on one-way classical communication are used allowing to communicate over arbitrary distances. However, the error thresholds for noise in local control operations are very stringent. The second scheme makes use of entanglement purification protocols with two-way classical communication and inherits the favorable error thresholds of the repeater run in standard mode. One can increase the possible communication distance by an order of magnitude with reasonable overhead in physical resources. We outline the architecture of a quantum repeater that can possibly ensure intercontinental quantum communication.

DOI: 10.1103/PhysRevA.75.032310 PACS number(s): 03.67.Hk, 03.67.Mn

I. INTRODUCTION

From all fields of quantum information science, quantum communication is most likely to reach a commercial application first. For long-distance communication one faces the problem that quantum channels like optical fibers are noisy and lossy, and both the output and the fidelity of the quantum information sent decrease exponentially with distance. Since quantum information cannot be amplified, standard techniques from classical communication technology cannot directly be used to overcome this problem. In principle, quantum error correction techniques can protect the quantum information while it is sent through a channel [1]. However, the small tolerable error rates limit the length of the channel drastically before error correction must be applied. Hence, one would need a large number of segments to cover a certain distance. The requirements on the quality of measurements and local operations are also very stringent (10^{-4}), far below experimentally achievable accuracy today.

Entanglement can be a resource to overcome this problem. If party A holds one part of a maximally entangled pair of qubits, and party B the other part, quantum information can be transferred by teleportation [2]. When these parties are far away from each other, and channels and local operations are noisy, the problem arises how to distribute the entangled pairs among them.

The quantum repeater [3,4] (see also [5–11]) is a solution to this problem based on entanglement purification [12–19] and entanglement swapping [2,20]. The distance L between the parties A and B is divided into smaller segments such that one can send parts of maximally entangled pairs through the channel that do emerge with sufficiently high fidelity for entanglement purification. Noisy local operations and measurements do not allow to purify one single maximally entangled pair from several copies, but the fidelity can be increased for remarkably high errors in the local operations and measurements on the order of percent [4]. Via entanglement swapping, segments are connected, establishing entangled pairs over larger distances. Observe that the connection process again decreases the fidelity such that one may connect only a few segments before the entanglement can no longer be increased by purification. The key ingredient of the quantum repeater is to use the combination of purification and entanglement swapping in a nested scheme, i.e., on different repeater levels. After few connections are made, the resulting pair is again purified by several copies obtained in the same way. Then the sequence "connection and repurification" is repeated until one has reached the desired distance between the parties. Most importantly, the physical and temporal resources needed for the quantum repeater scale only polynomially with the distance between parties A and B. The details naturally depend on the errors, the specific purification protocol, and the repeater metaprotocol, i.e., the distribution and number of repeater stations and their individual setup. The repeater protocols range from the standard protocol [12,13], where all pairs needed in the process are created initially as an ensemble (maximal physical, minimal temporal resources), over the "Innsbruck protocol" [4] (physical resources scale logarithmically with the distance) to the "Harvard protocol" [5] with minimal physical resources (two qubits per repeater station) but maximal temporal resources. For practical purposes minimal physical resources are desirable since it is hard to control or even establish a large number of interacting quantum systems. In this light, one would tend to prefer the last two of the protocols above.

While in previous investigations the influence of noise in channels and in local control operations has been extensively studied, memory errors have not been included in the analysis so far. It was implicitly assumed that (almost perfect) local memory is available by some means. If this assumption is valid, as can, e.g., be ensured by using local encoding to actively maintain quantum information, one obtains a scalable scheme that allows for quantum communication over arbitrary distances with polynomial overhead. However, all repeater schemes require the storage of pairs before they are further processed, and the influence of imperfect memory needs to be studied. In particular, at high repeater levels when long-distance pairs are processed, the waiting times can be significant. Estimated times to establish an entangled pair over, say, intercontinental distances are of the order of the decoherence times of the best known memory systems today, making the consideration of memory errors a necessity. In this paper we address the problem of memory errors in quantum repeaters. Specifically we investigate (i) the limits of the quantum repeater with memory errors when run in standard mode (error detection mode), where we show that memory errors lead to a limited communication distance; (ii) ways to reduce or overcome memory errors by using decoherence free subspaces or local encoding for storage; (iii) an operational mode for the quantum repeater, the error correction mode, which in principle allows one to overcome the limitations of memory errors, however, suffers from low error thresholds; (iv) a blind operation mode and hybrid architectures that allow one to increase the possible communication distance by an order of magnitude, without changing favorable error thresholds.

The paper is organized as follows. In the next section we briefly describe the building blocks of a quantum repeater, entanglement purification, and swapping. We sketch different repeater protocols and present the error model we will use. In Sec. III we apply the error model, especially memory errors, to the quantum repeater. We derive the limits for communication distance when no memory-enhancing techniques are used and discuss error thresholds. As a possible way to overcome the limitations due to memory errors, a direct solution is to reduce or even eliminate them, which we discuss in Sec. IV. If no perfect quantum memory is available, we show in Sec. V that blind mode is an alternative way to relax the limitations of the quantum repeater. We then outline possible architectures for a quantum repeater in Sec. VI, and summarize our results in Sec. VII.

II. BASIC PRINCIPLES

We start with some notations, present purification protocols, entanglement swapping and repeater protocols for both a repeater in error detection as well as in error correction mode [21], and introduce the error model we are going to use.

A. Notation

Throughout the paper we will speak of two spatially separated parties A and B, who share certain entangled pairs of qubits between them. We denote these pairs by $A_1B_1,\ldots,A_NB_N$, i.e., A holds the qubits $A_1,\ldots,A_N$, while B holds $B_1,\ldots,B_N$. Whenever it is not clear from the context on which system an operator is acting, we specify it with a sub or superscript. An operation is called local if it acts only on A's or only on B's qubits, e.g., $U_{\text{CNOT}}^{A_1\to A_2}$ is a local controlled-NOT (CNOT) operation with qubit A_1 as control and A_2 as target [22]. By P_Φ we denote a projector onto the states $|\Phi\rangle$. Furthermore, σ_i denote the Pauli operators, explicitly, $\sigma_0=\mathbb{1}$, $\sigma_1=\sigma_x$, $\sigma_2=\sigma_y$, $\sigma_3=\sigma_z$. The Bell states are denoted by $|\Phi_j\rangle=\mathbb{1}\otimes\sigma_j|\Phi^+\rangle$ with $|\Phi^+\rangle=1/\sqrt{2}(|00\rangle+|11\rangle)$.

Instead of the usual Bell states we often take their graph state equivalents [23], which we call graph Bell states. The graph state basis for two qubits defined in the basis $|0\rangle_z$, $|1\rangle_z$ (eigenbasis of the Pauli σ_z operator) and in the basis $|0\rangle_x$, $|1\rangle_x$ (eigenbasis of the Pauli σ_x operator) is

$$|00\rangle_G \coloneqq 2^{-1/2}(|00\rangle_{zx}+|11\rangle_{zx}),$$

$$|01\rangle_G \coloneqq 2^{-1/2}(|01\rangle_{zx}+|10\rangle_{zx}),$$

$$|10\rangle_G \coloneqq 2^{-1/2}(|00\rangle_{zx}-|11\rangle_{zx}),$$

$$|11\rangle_G \coloneqq 2^{-1/2}(|01\rangle_{zx}-|10\rangle_{zx}).$$

Expressions like $|00\rangle_{zx}$ mean $|0\rangle_z\otimes|0\rangle_x$. The graph state basis is related to the standard Bell basis $|k_1,k_2\rangle_B$ by a Hadamard operation in B. When the basis is clear from the context we will omit the label G. If such a state is, for example, the first pair shared between A and B we write $|00\rangle_G^{A_1B_1}$.

We will consider density matrices that are diagonal in the graph state basis,

$$\rho=\sum_{k_1,k_2=0}^{1}\lambda_{k_1,k_2}|k_1,k_2\rangle\langle k_1,k_2|,$$

and we will sometimes write $\rho=\Sigma_{k_1}^{1},k_2=0\ \lambda_{k_1,k_2}P_{k_1,k_2}$ with a projector

$$P_{k_1,k_2}\coloneqq|k_1,k_2\rangle\langle k_1,k_2|.$$

We denote by (m_1,m_2) a possible shift of the basis, i.e. a permutation of the basis vectors. That is,

$$\rho=\sum_{k_1,k_2}\lambda_{k_1,k_2}|k_1\oplus m_1,k_2\oplus m_2\rangle\langle k_1\oplus m_1,k_2\oplus m_2|,$$

where $\oplus$ will always mean addition modulo 2. We remark that, without loss of generality, any density matrix can be brought to a graph-diagonal form without changing the diagonal coefficients by applying appropriate sequences of (probabilistic) local operations. To be precise, these operations correspond to the stabilizing operators of the given graph, in our case $K_1,K_2,K_1K_2,\mathbb{1}$ with $K_1=\sigma_x\otimes\sigma_z$, $K_2=\sigma_z\otimes\sigma_x$ [24]. Permutations of basis vectors can be achieved by local unitary operations of the form $\sigma_z^{m_1}\sigma_z^{m_2}$. Note that the state ρ results from sending one part of a graph state $|k_1,k_2\rangle$ through a Pauli-diagonal channel

$$\mathcal{E}_1(\rho)=\sum_{i=0}^{3}p_i\sigma_i\rho\sigma_i,$$

with $p_0=\lambda_{00}$, $p_1=\lambda_{10}$, $p_2=\lambda_{11}$, and $p_3=\lambda_{01}$.

Later, we will use the Werner states [25]

$$\begin{aligned}\rho_W(x)&\coloneqq x|00\rangle_G\langle 00|+(1-x)/4\mathbb{1}\\&\coloneqq F|00\rangle_G\langle 00|+(1-F)/3\sum_{i,j\neq 0,0}|ij\rangle_G\langle ij|\end{aligned}\qquad(1)$$

with $F=(3x+1)/4$, which are uniquely defined by the quantity F, the fidelity, whereas more general graph diagonal states are usually only fully specified by all diagonal coefficients. We call the largest of these the fidelity, and we will often omit the other coefficients in the discussion. This simplification is justified since the purification protocol we will use produces states close to particular graph diagonal states, so called binary mixtures $\lambda_{00}|00\rangle_G\langle 00| + \lambda_{10}|10\rangle_G\langle 10|$. Here, $\lambda_{10}=1-\lambda_{00}$ such that binary mixtures are also specified by only one coefficient.

B. Entanglement purification

Entanglement purification allows one to produce from several noisy copies of an entangled state a few copies with high fidelity by means of local operations and classical communication. For perfect operations, the fidelity can, in principle, be brought arbitrarily close to unity. However, many purification steps are required for nearly perfect pairs, so that, in practice, only some finite fidelity is achievable ("finite" meaning smaller than one). If the local operations required in the purification process are noisy themselves, then even in principle no perfect pairs can be obtained. At this stage, what matters to us is that in practice no protocol will produce perfect, maximally entangled pairs. Besides the maximal fidelity we can reach, there is also some minimal fidelity we need for the purification process. This minimal fidelity depends on the protocol we use for the purification, and it is called the purification threshold.

A number of different protocols exist, which differ in their purification range (i.e., the set of states they can purify), the efficiency, and the number of copies of the states they operate on [24]. We present two-way entanglement purification, i.e., a purification protocol using two-way classical communication, namely the DEJMPS protocol [13], and also one-way entanglement purification based on Calderbank-Shor-Steane codes.

1. Two-way entanglement purification

We take a recurrence protocol for purification, where we consider the DEJMPS protocol [13] since it has a very good efficiency in terms of convergence speed and robustness. Remarkably, the fidelity of states can be significantly increased even if errors in operations and measurements are on the order of percent. For the moment, however, we consider perfect operations and measurements, and generalize the formulas later when we will have introduced our error model. The protocol operates on two entangled pairs, and can be viewed as a generalization of the recurrence entanglement purification protocol introduced in [12]. We slightly modify the protocol as compared to the original work such that it purifies graph diagonal Bell states rather than Bell states. This corresponds, however, to a simple change of local basis which does not modify the protocol as such. The protocol consists of the following steps:

(i) depolarization of the density matrix to graph diagonal form; in fact this step need not be executed since off-diagonal elements do not influence the change in the diagonal elements and converge to zero upon iteration of the protocol;

(ii) local basis change $|0\rangle_z \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_z - i|1\rangle_z)$, $|1\rangle_z \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_z - i|0\rangle_z)$ in A and $|0\rangle_x \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_x + i|1\rangle_x)$, $|1\rangle_x \rightarrow \frac{1}{\sqrt{2}}(|1\rangle_x + i|0\rangle_x)$ in B; the effect of this basis change on two graph Bell states is, omitting an irrelevant phase factor,

$$|x_1,x_2\rangle|y_1,y_2\rangle \rightarrow |x_1,x_1 \oplus x_2\rangle|y_1,y_1 \oplus y_2\rangle;$$

(iii) application of bilateral local CNOT operations $U_{\text{CNOT}}^{A_1\rightarrow A_2} \otimes U_{\text{CNOT}}^{B_2\rightarrow B_1}$, such that

$$|x_1,x_2\rangle|y_1,y_2\rangle \rightarrow |x_1 \oplus y_1\rangle|x_2,y_1,x_2 \oplus y_2\rangle;$$

(iv) local measurement of qubit A_2 $[B_2]$ in the eigenbasis of σ_z $[\sigma_x]$ with corresponding result $(-1)^{\zeta_2}$ $[(-1)^{\xi_2}]$, where $\zeta_2, \xi_2 \in \{0,1\}$;

(v) decision: keep the state $\rho_{A_1B_1}$ if the measurement results indicate a successful purification round. This decision requires two-way classical communication between the parties A and B.

We let the protocol act on the tensor product of two graph diagonal states $\rho_{A_1B_1}$, $\rho_{A_2B_2}$ with coefficients λ_{k_1,k_2} and μ_{j_1,j_2} respectively, which have bases shifted by (m_1,m_2) and (n_1,n_2), respectively, i.e., on

$$\rho = \sum_{k_1,k_2,j_1,j_2=0}^{1} \lambda_{k_1,k_2}\mu_{j_1,j_2}P_{k_1\oplus m_1,k_2\oplus m_2,j_1\oplus n_1,j_2\oplus n_2}. \quad (2)$$

After steps (i)–(iv), qubits A_1 and B_1 will be in the state

$$\rho' = \sum_{k_1,k_2,j_1,j_2=0}^{1} \lambda_{k_1,k_2}\mu_{j_1,j_2}\delta_{\zeta_2\oplus\xi_2,k_1\oplus k_2\oplus j_1\oplus j_2\oplus m_1\oplus m_2\oplus n_1\oplus n_2} \times P_{k_1\oplus j_1\oplus m_1\oplus n_1,k_1\oplus k_2\oplus m_1\oplus m_2},$$

where δ is the Kronecker delta. The condition for a successful purification step relates the measurement outcomes ζ_2, ξ_2 and the basis shifts in the following way: $\zeta_2 \oplus \xi_2 = m_1 \oplus m_2 \oplus n_1 \oplus n_2$. In case this condition is fulfilled, we arrive at a simple expression for $(\rho')_{i_1,i_2} =: \lambda'_{i_1,i_2}$, namely,

$$\lambda'_{i_1\oplus m_1\oplus n_1,i_2\oplus m_1\oplus m_2} = \frac{1}{N}\sum_{k_1=0}^{1} \lambda_{k_1,k_1\oplus i_2}\mu_{k_1\oplus i_1,k_1\oplus i_1\oplus i_2}, \quad (3)$$

where $N=\Sigma_{i_1,i_2}\lambda'=(\lambda_{00}+\lambda_{11})(\mu_{00}+\mu_{11})+(\lambda_{01}+\lambda_{10})(\mu_{01}+\mu_{10})$ is a normalization constant that quantifies the probability to obtain the corresponding measurement results. The normalization is independent of the basis shifts. While the basis shifts do not play a role in the present discussion of the DEJMPS protocol, they will become crucial when running the repeater in a blind operational mode, Sec. V.

The DEJMPS map, after a successful step, always drives the states closer to a binary mixture like $\lambda_{00}|00\rangle\langle 00|_G + \lambda_{10}|10\rangle\langle 10|_G$. The map is also most effective on binary mixtures, and least effective on Werner states $\rho(x)=x|00\rangle\langle 00|_G + (1-x)/4\mathbb{1}$.

There are two distinct purification strategies for which we can use the DEJMPS protocol: regular entanglement purification and entanglement pumping.

a. Regular entanglement purification. First, we could imagine to an ensemble consisting of several copies of some elementary, noisy pair of qubits. Whenever we perform a successful purification step on two such pairs, the resulting pair of higher fidelity goes to the next purification round, otherwise it is discarded. In the DEJMPS map we have in this case $\lambda_{ik}^{(n)}=\mu_{ik}^{(n)}$ in every round n, and the (attractive) fixed point of the map is a perfect graph Bell state. In practice, we cannot do infinitely many steps to reach this fixed point, let alone that errors are present that prevent one to approach this fixed point even in principle. We call this purification strategy "regular entanglement purification." The drawback of this strategy are the many qubit pairs we need to prepare and keep ready-to-use during the process. The number of pairs is exponentially growing with the number of purification steps we wish to perform.

b. Entanglement pumping. Second, we can always use identical, elementary pairs in each round to further purify the pair we obtained from a previous successful step. If at any time we are not successful, the whole protocol must be restarted with two fresh elementary pairs. This strategy is called entanglement pumping [4]. The advantage clearly is that the physical resources (qubit pairs to be stored simultaneously) stay constant. We need not count elementary pairs because they do not have to be stored but are consumed at once. The elementary pairs can rather be recreated on demand. With entanglement pumping, we have $\lambda_{ik}^{(n)}\neq\mu_{ik}^{(n)}$, except in the first round, and the $\mu_{ik}^{(n)}$ are the same in every round n in the DEJMPS map (3). Even infinite iteration will not lead to maximally entangled pairs, but in practice (with errors in the operations), the fixed point of the map can even be closer to a maximally entangled pair than for the regular entanglement purification [4]. Because one saves physical resources at the expense of only a polynomial overhead in time, entanglement pumping was favored in the most recent designs of quantum repeaters [5,6]. The real drawback of using entanglement pumping in the quantum repeater shows up when we later include memory errors, where an—albeit polynomial—overhead in time becomes a problem.

We remark that this is also the reason why we do not consider nested entanglement pumping [26]. Nested entanglement pumping has the same fixed point of the purification map as regular entanglement purification. The number of pairs grows only linearly with the nesting level at the expense of a temporal overhead exponential in the number of purification steps one performs on each nesting level. Although the fixed point is (nearly) reached for about three nesting levels, the additional temporal overhead make this purification scheme unfavorable in the presence of memory errors.

2. One-way entanglement purification

In his Ph.D. thesis [21], Aschauer introduced a general scheme to construct entanglement purification protocols from quantum error correction codes. In particular, for each Calderbank-Shor-Steane (CSS) code that uses n physical qubits to protect k qubits, one can construct an entanglement purification protocol that operates on n initial copies of two-qubit states and produces k purified pairs as output. As described in [21], the purification protocols can either be run (i) in error correction mode or (ii) in error detection mode. In case of (i), output pairs are kept deterministically and measurements on remaining pairs are used to determine the required error correction operation. This operation mode only requires one-way classical communication. For (ii), the information gathered in the measurement of $(n-k)$ pairs is used to decide whether the remaining pairs should be kept or discarded. The ones that are kept have a higher fidelity than before. This operational mode is the standard mode for recurrence protocols as discussed above. Here, we will concentrate on (i), entanglement purification run in the error correction mode.

In the following we briefly review the work by Aschauer [21]. We consider the situation where the sender, Alice, wants to send quantum information to the receiver, Bob. To this aim, Alice might either send a system, A_0, prepared in an arbitrary state $|\Psi\rangle$ to Bob or she might prepare a maximally entangled state between two systems, send one to Bob and use the other to teleport the state $|\Psi\rangle$ to Bob. To protect the quantum information from the errors that occur during the transmission process, quantum error correction is used in the first and entanglement purification in the second scenario.

In a quantum error correction protocol (we consider here the case where the state of a single qubit is protected) Alice prepares n auxiliary systems (denoted by A) in a state $|a_1,\ldots,a_n\rangle_A$, with $a_i\in\{0,1\}$. Then she applies the encoding operation U_{A,A_0} to A and the system A_0, prepared in the state $|\Psi\rangle$ and carrying the quantum information, and sends all systems to Bob. In the simplest case, where no errors occur during the transmission, Bob receives the systems in the state $U_{B,B_0}|a_1,\ldots,a_n\rangle_B|\Psi\rangle_{B_0}$. He applies $U_{B,B_0}^{-1}=U_{B,B_0}^{\dagger}$ to decode the quantum information and measures the auxiliary systems in the computational basis. Finally, he will be left with a system in the state $|\Psi\rangle$.

Let us now consider an entanglement-based version of this protocol. We make use of the fact that $U_A\otimes\mathbb{1}_B|\Phi^+\rangle_{AB}=\mathbb{1}_A\otimes U_B^T|\Phi^+\rangle_{AB}$ for any operator U. The idea is that Alice prepares Bob's system at a distance using an entangled state. Suppose that Alice and Bob share $n+1$ maximally entangled states, $|\Phi^+\rangle_{AB}^{\otimes n}|\Phi^+\rangle_{A_0B_0}$, where A (B) denotes the first n systems of Alice (Bob), respectively, and A_0 (B_0) denotes the $(n+1)$th system of Alice (Bob). Alice applies U_{A,A_0}^T and teleports the state $|\Psi\rangle$ to Bob with the help of the $(n+1)$th pair. It is straightforward to verify that the remaining system is then described by the state $U_{B,B_0}|\Phi^+\rangle_{A,B}^{\otimes n}\sigma_j|\Psi\rangle_{B_0}$, where j depends on Alice‘s measurement outcome. Thus, if Alice measures her auxiliary systems in the computational basis and tells Bob the value of j, Bob can apply $\sigma_j^{B_0}$ to be left with exactly the same state as in the quantum error correction model.

In order to include the errors that occur during the transmission we describe the channel by the map $\mathcal{E}_1$ with $\mathcal{E}_1(\rho)=\sum_{i=0}^{3}p_i\sigma^i\rho\sigma^i$ where $\sum_i p_i=1, p_i\geq 0$ (see Sec. II A). We investigate the case where all the errors occur independently on each of the sent qubits. Thus, the map we consider is $\mathcal{E}=\mathcal{E}_1^{\otimes n}=\sum_{\mathbf{i}}p_{\mathbf{i}}\sigma^{\mathbf{i}}\rho\sigma^{\mathbf{i}}$, where $\mathbf{i}=(i_1,\ldots,i_n)$, with $i_j\in\{0,\ldots,3\}$ and $p_{\mathbf{i}}=p_{i_1},\ldots,p_{i_n}$. In the first scenario the encoded message is sent through this channel. Receiving the systems, Bob applies $U^{\dagger}$ and measures the auxiliary systems. Alice sends Bob the classical information about $\{a_i\}$ which allows Bob to determine the error syndrome with which he can correct the error. In the second scenario one qubit of each maximally entangled state is sent through the channel. Then the pairs are purified to one pair which is highly entangled. This pair is then used by Alice to teleport the state $|\psi\rangle$ to Bob. Considering the purification of the image of the map $\mathcal{E}$, i.e., $U_{\mathcal{E}}|\psi\rangle=\Sigma_{\mathbf{i}}\sqrt{p_{\mathbf{i}}}\sigma^{\mathbf{i}}|\psi\rangle|\mathbf{i}\rangle_R$, such that $\mathrm{tr}_R(P_{U_{\mathcal{E}|\psi}\rangle})=\mathcal{E}(P_\psi)$, with some auxiliary system R, it is straightforward to show that applying entanglement purification and then teleportation is equivalent to quantum error correction, where the message is sent through the same channel. The minimal required fidelity for this entanglement purification protocol, the purification threshold, turns out to be more stringent than for two-way classical communication [12,21] ($F \gtrsim 0.8$ as compared to $F > 0.5$ for a protocol using two-way classical communication). However, the advantage of error correction protocols is that they are deterministic. Note that the one-way purification protocols in [21] are based on the Bell $|\Phi^+\rangle$ state. One could easily make them consistent with our graph basis by applying local basis changes.

C. Entanglement swapping

Entanglement swapping [20] is the operation on two maximally entangled qubit pairs, where a Bell measurement is performed on one qubit of each pair with the result that the remaining two qubits are afterward maximally entangled. If the maximally entangled pairs are the graph Bell states A_1B_1 and B_2C_1, a Bell measurement on the qubits B_1, B_2 is, e.g., realized, e.g., by a CNOT-operation $U_{\mathrm{CNOT}}^{B_1\rightarrow B_2}$ followed by σ_z measurements on qubits B_1, B_2 with outcomes ζ_{B1}, ζ_{B2}, leaving A_1, C_1 in the desired maximally entangled state up to a local basis change that depends on the measurement outcomes. We remark that classical communication is required to perform a proper adjustment of the local basis at the final state. Entanglement swapping can be viewed as a teleportation of the state of qubit B_1 to C_1. If we assume that qubit C_1 is at some distance from A_1 and B_1, B_2 are somewhere in the middle, we will often call this swapping process a "connection" or a "link" because the goal of the quantum repeater is to establish entanglement over larger distances, here between parties A and C.

If both pairs are not maximally entangled, the teleportation will be that of an imperfect pair by imperfect means, resulting in a decreased or even vanishing entanglement of the final pair between A and C. We call this an imperfect connection or imperfect link, and it is easy to understand that the fidelity of a pair after L imperfect connections is decreasing exponentially with L. To see this, consider nonmaximally entangled pairs of Werner form, Eq. (1). Connecting two such pairs by means of a Bell measurement as outlined above results in a state that is diagonal in the graph state basis, and has a reduced fidelity. After depolarization of the resulting state and performing the required basis change depending on the measurement outcome, one obtains again a Werner state $\rho_W(x')$ with $x'=x^2$, i.e., the fidelity $F'=(3x'+1)/4$ is reduced quadratically. The connection of L pairs yields $x'=x^L$, i.e., an exponential decrease with L.

If we consider two graph diagonal pairs of the form Eq. (2), the resulting pair after the Bell measurement has coefficients

$$\lambda'_{i_1\oplus m_1\oplus n_1\oplus\zeta_{B1},i_2\oplus m_2\oplus n_2\oplus\zeta_{B2}}=\sum_{k_1,k_2=0}^{1}\lambda_{k_1\oplus i_1,k_2\oplus i_2}\mu_{k_1,k_2}, \quad (4)$$

where ζ_{B1},ζ_{B2} denote the outcomes of the Bell measurements leading to a permutation of the output vector (which could be undone by performing appropriate local unitary operations of the form $\sigma_z^{\zeta_{B1}}\sigma_z^{\zeta_{B2}}$). Again, the resulting state is graph diagonal, but the basis is shifted by $(m_1\oplus n_1\oplus\zeta_{B1},m_2\oplus n_2\oplus\zeta_{B2})$, an expression that depends on the initial basis shifts and the measurement outcomes. As in the purification protocol, these random basis shifts do not matter because one simply can keep track of them without the need to actually correct them. In fact, the same sequences of operations (i.e., the same protocol for entanglement swapping) can be applied, only the basis of the resulting density matrix changes.

The scaling of the fidelity with the number of simultaneous links becomes even worse with imperfect operations, which we have not considered yet. We will describe the map resulting from imperfect connections later after introducing our error model. For the moment we have seen that even with perfect local operations we could only connect a few pairs before the entanglement would vanish. This is where the quantum repeater comes into play, whose repeater protocol determines where to interrupt the connection process and to repurify the involved states. We turn to repeater protocols in the following.

D. Repeater protocols

The repeater protocol governs which purification protocol to use (e.g., DEJMPS), which purification strategy (regular; pumping), and which "geometry." By geometry we mean where to place repeater stations and with which resources to equip them depending on the purification protocol, the purification strategy, and the linking strategy, i.e., how many stations to link after one purification round is complete. We will describe some repeater protocols with two-way purification protocols that have been developed to demonstrate functionality of the quantum repeater (and which are not optimized for any specific physical implementation).

1. Standard repeater protocol

The original repeater protocol [12,13] uses regular entanglement purification where all required pairs are stored in parallel and the number of purification steps on each level is constant, say M. The total distance is divided into $N=2^n$ segments, and after each purification round two segments will be connected such that we have n repeater levels. The time for the completion of the whole repeater process is $M(2^{n+1}-1)$ in units of the time we need for the first purification step, and we have neglected gate operation times and the times we need for connections. While the total time is already determined by the standard repeater protocol, the physical resources depend on the initial, elementary pairs, the purification protocol, and the errors. In this scheme the physical resources are very demanding since all pairs ever used in the process are created right at the beginning and the required resources (i.e., total number of pairs) are given by $R=(M+1)^n$. Despite the fact the required resources (i.e., parallel channels or pairs to be stored) grow only polynomially with the distance, since R can be rewritten as $R=N^{\log_2 M+1}$, the overhead can be substantial.

2. Innsbruck protocol

The Innsbruck protocol [4] is based on entanglement pumping using the DEJMPS-purification protocol. As in the standard repeater protocol the total distance is divided into $N=2^n$ segments. On the lowest repeater level, elementary pairs are purified, and once they have reached some sufficiently high "working" fidelity, always two adjacent pairs are connected throughout the chain. The resulting pairs of lower fidelity must be stored, so every second repeater station needs an extra qubit for storage. On the lowest level the process of purification and connection is repeated and the resulting low fidelity pair is used to purify the one that is stored. Iteration leads to a high fidelity pair over twice the initial distance. The whole scheme is repeated on higher and higher repeater levels, and we need again extra storage qubits on every 4th, 8th, etc., repeater station. The physical resources hence grow logarithmically with the distance. Compared with the standard repeater protocol, the physical resources have been drastically reduced at the expense of a polynomial overhead in time [4]. Purification now takes place sequentially, where new elementary pairs at each repeater level need to be recreated using the same physical resources, and one hence needs to wait until the new elementary pair arrives. In addition, a failure in the purification process on any repeater level means that the pair in question has to be discarded, and the stochastic process to rebuild it must be started again from the lowest level. Note that this means extra waiting times for pairs on higher repeater levels that depend on the supply of pairs from the level where the failure occurred. As pointed out above, these waiting times become significant when we include memory errors.

3. Harvard protocol

From a practical point of view it is desirable to use the minimum of physical resources since many qubits are hard to control and to store. In that respect the Harvard protocol [5], a variant of the Innsbruck protocol, is the most advanced since it uses the minimum possible number of two qubits at each repeater station. This reduction of physical resources compared to the Innsbruck protocol is possible because the capacities of some repeater stations were not fully used in the Innsbruck protocol, but are now fully activated by an ingenious setup. We will not describe this setup here in detail, but merely note that the price for minimal resources is (a) connection of up to five pairs at once (among them three elementary ones) and (b) even longer waiting times for high-level qubits in case of failure. Point (a) implies that we need tighter error thresholds because otherwise five connections may lead to a fidelity below the purification threshold. From point (b) follows that the limits of the Innsbruck protocol, which we are going to derive when we include memory errors, also hold for the Harvard protocol.

4. Protocols using purification by error correction

In principle the above protocols could also use entanglement purification by error correction. But the purification range determined in [21] is already small for protocols run in a concatenated way, which is the equivalent of regular entanglement purification in the error detection mode. An equivalent to entanglement pumping was not discussed, but the purification ranges would certainly be very small if not vanishing. Memory errors would thus render both approaches useless very soon. Later, we will show that we can get rid of the problem with memory errors for the case of a concatenated, error correction type purification. Hence, we will only consider the equivalent of the standard repeater protocol later.

E. Error model and purification and connection with imperfect means

1. Error model

We conclude the section by presenting the error model we are going to use in the rest of the paper. We emphasize that the results we obtain and in particular the conclusions we draw are independent of the details of the error model, but are rather a consequence of unavoidable waiting times when using the quantum repeater in one of its standard operational modes. What may, however, differ slightly are the actual numbers, where the white noise model we assume turns out to provide a rather conservative estimate of the noise threshold, in particular when compared to situations where one particular kind of noise (e.g., phase noise) is dominant and much better performance and error thresholds can be obtained. We model imperfect operations on two qubits x_1 and x_2 as a mixture of perfect operations and white noise:

$$O_{x_1,x_2}(\rho) = pO^{\text{ideal}}_{x_1,x_2}(\rho) + (1-p)\tfrac{1}{4}\mathbb{1}_{x_1,x_2} \otimes \text{tr}_{x_1,x_2}(\rho), \tag{5}$$

where $O^{\text{ideal}}_{x_1,x_2}$, the ideal two-qubit operation, has probability p, and the two-qubit white noise has probability $1-p$. The measurements are based on imperfect projections described by positive operator valued measure elements $P_0=\eta|0\rangle\langle 0|+(1-\eta)|1\rangle\langle 1|$ and $P_1=\eta|1\rangle\langle 1|+(1-\eta)|0\rangle\langle 0|$.

Finally, we use local depolarizing channels to describe memory errors, i.e., local white noise. On a single qubit the depolarizing CP map reads

$$(D\rho)(t) = q(t)\rho + [1-q(t)]/4\sum_{k_1=0}^{3}\sigma_{k_1}\rho\sigma_{k_1}, \tag{6}$$

with $q(t)=e^{-\kappa t}$ and κ is the inverse decoherence time. On a graph-diagonal, two-qubit density matrix $\rho=\Sigma^1_{k_1,k_2=0}\lambda_{k_1,k_2}|k_1,k_2\rangle\langle k_1,k_2|_G$ the map is

$$[(D^{[1]}\otimes D^{[2]})\rho](t) = \sum_{k_1,k_2=0}^{1}[q^2\lambda_{k_1,k_2}+(1-q^2)/4]P_{k_1,k_2}. \tag{7}$$

Now, we rederive the DEJMPS map and entanglement swapping for imperfect operations and measurements of the above form.

2. Purification with imperfect operations and measurements

When we include the errors in operations and measurements, the DEJMPS map, Eq. (3), is modified. Intuitively it is clear that the errors in the measurements, η, will mix the results of a successful step with those of an unsuccessful step, while the errors in the operations, p, will introduce white noise. The modified formula is

$$\lambda'_{i_1\oplus m_1\oplus n_1, i_2\oplus m_1\oplus m_2} = \frac{1}{N}\left(\frac{1-p^2}{8} + p^2\sum_{a=0}^{1}[\eta^2+(1-\eta)^2]^{a\oplus 1\oplus\zeta_2\oplus\xi_2} \times[2\eta(1-\eta)]^{a\oplus\zeta_2\oplus\xi_2}\sum_{k_1=0}^{1}\lambda_{k_1,k_1\oplus i_2}\mu_{k_1\oplus i_1,k_1\oplus i_1\oplus i_2\oplus a}\right). \tag{8}$$

Again, ζ_2, ξ_2 are the measurement outcomes of step (iv). The normalization $N=\Sigma_{i_1,i_2}\lambda'$ represents the probability for a successful purification step, where the criterion for success, $\zeta_2\oplus\xi_2=m_1\oplus m_2\oplus n_1\oplus n_2$, also remains the same.

As before, initial basis shifts of the two pairs simply lead to a different basis shift on the resulting pair. This fact remained true because we can still commute the local basis shifts through the Clifford operations and the Pauli errors. In this sense, local basis shifts still only lead to a reinterpretation of what successful measurement outcomes are.

3. Entanglement swapping with imperfect operations and measurements

So far we have concentrated on entanglement purification. The second part of the repeater protocols is the linking of farther apart stations when stations in between perform (imperfect) entanglement swapping on two pairs of graph diagonal states. With the error model from above, we expect that the measurement errors lead to an admixture of the results of the other measurement outcomes, and that the errors in the operations lead to an admixture of white noise. The modified version of Eq. (4) is

$$\lambda'_{i_1\oplus m_1\oplus n_1\oplus\zeta_{B1}, i_2\oplus m_2\oplus n_2\oplus\zeta_{B2}} = \frac{1-p}{4} + p\sum_{a,b=0}^{1}(\eta^2)^{(a\vee b)\oplus 1}[\eta(1-\eta)]^{a\oplus b}[(1-\eta)^2]^{a\wedge b} \times\sum_{k_1,k_2=0}^{1}\lambda_{k_1\oplus i_1\oplus a,k_2\oplus i_2\oplus b}\mu_{k_1,k_2}, \tag{9}$$

where ζ_{B1}, ζ_{B2} are still the outcomes of the Bell measurement, and $\vee$ is the logical OR, $\wedge$ the logical AND. Note again that initial basis shifts of the pairs merely result in a different basis shift of the linked pair, where the shift is now randomized by the measurement outcomes.

III. LIMITS OF THE QUANTUM REPEATER

In this section we show how uncorrected errors in memory limit the maximal distance over which entangled pairs can be created. First, we study the repeater in standard mode, then in error correction mode.

A. Limits of the quantum repeater in standard mode

As mentioned, the standard scheme for the quantum repeater uses two-way classical communication to reveal whether purification steps have been successful or not, and only in the first case the resulting pair is kept for further processing. Otherwise, the process must be started anew. The classical signal needs time to cover the distance between the repeater stations, and this time increases on higher repeater levels, where the stations are further apart. On higher repeater levels the signal time dominates by far all other timescales such as the gate operation time. During the time needed for the classical communication, the quantum systems have to be kept in some quantum memory where they are subject to memory errors. If this quantum memory is not perfect, there is a distance between parties A and B that cannot be exceeded in the standard quantum repeater scheme because during the time the classical signals need to cover this distance the fidelity of the entangled pairs drops below the purification threshold. Naturally, this maximal distance depends on memory errors, but also on the errors and the repeater protocol, where now protocols needing less *temporal* resources are favored.

In previous work, repeater protocols were developed in a kind of "bottom-up" strategy. With chosen error models (except memory errors) and purification protocols one created a certain base module that ensured the functionality of purification and entanglement swapping, and made sure that this module could be repeated on higher levels with polynomial scaling of time and physical resources. One can keep this point of view when one includes strategies to reduce or eliminate memory errors. This will be discussed in Sec. IV. On the other hand, when memory errors are present, then the maximal distance is a constraint and it is more natural to adopt a "top-down" approach. Given a distance between the parties A and B the question is, can we reach it and what resources does it cost us?

Our goal in this section is to determine the maximal distance that different repeater protocols can achieve. As a first step, we look at the purification range of the DEJMPS protocol on different repeater levels. We will assume throughout that the distance between two repeater stations is 10 km, such that a classical signal needs 0.333×10^{-4} s to travel. Further, each higher repeater level doubles this distance and hence also the signal time. We include all errors presented in the last section into the analysis of the purification range. In a second step, we simulate the full quantum repeater, where we concentrate on the standard and Innsbruck protocol having in mind that the Harvard protocol cannot perform better than the Innsbruck protocol in terms of thresholds and reachable distance.

1. Limits of DEJMPS *purification protocol on different repeater levels*

In the standard schemes we must wait for the classical signals to cover the distance between the repeater stations in question before we can do the next purification step. We want to determine the purification range of the DEJMPS map, Eq. (8), on different repeater levels when memory errors are present. The purification range lies between a lower fixed point of this map [27], which we call the purification threshold, and some upper fixed point.

The purification range of this map is hard to determine analytically. For fixed parameters, a numerical analysis is straightforward, and can be used to analyze the performance of the protocol and in particular the influence of memory errors. Note that we are not considering the whole repeater in the following, but isolated repeater levels. To determine the purification range on some level we iterate the map several times (strictly speaking one would need an infinite number of times). Between each application of the map we let the involved states decohere for a certain amount of time. We also choose some initial state, and the purification threshold depends on that state. For regular entanglement purification, the upper fixed point of the map is independent of the initial state, while for entanglement pumping it strongly depends on the initial state.

Here, we do a general treatment of the quantum repeater, and hence we do not use parameters of any specific, physical setup. Since we would like to obtain tolerable errors for local operations and measurements on the order of percent we choose $p=\eta=0.99$. As coherence time we assume $\kappa^{-1}=1$ s. The coherence time has a strong influence on the purification range and even more on the whole quantum repeater, and we will demonstrate this fact in the discussion of the repeater. With repeater stations that are about 10 km apart, such that the signal time on repeater level 1 is $t_0=0.333\times10^{-4}$ s, the waiting time for a signal on the nth level is $2^{n-1}\times t_0$ since we assume that each level doubles the distance. The memory error, Eq. (7), will hence act for at least a time $2^{n-1}\times t_0$ on the nth repeater level between every purification step. We neglect gate operation times that, on higher levels, are dominated by the classical signal times. To test the purification ranges of the DEJMPS map on different repeater levels we are going to use this minimal waiting time.

As initial states for the DEJMPS protocol we take Werner states $\rho_W(x)$, Eq. (1), on each repeater level. We make this choice here and in the rest of the section, because we want to stay consistent with our error model, i.e., we also assume the channels through which we establish pairs to be subjected to white noise processes. Usually this is not true, e.g., in optical fibers we find a dominance of dephasing noise, but it is the worst choice we can make for the DEJMPS protocol, so we are definitely not being overoptimistic. Note that any noise model for channels can be brought to white noise form without changing the channel fidelity [28].

In Table I we give purification regimes for different repeater levels. The second column lists the purification threshold for regular entanglement purification. The third column gives the maximal reachable fidelity in this case, whereas in the fourth column we give the maximal reachable fidelity using entanglement pumping with initial Werner states of fidelity 0.8. Naturally the data will vary if one inserts the actual parameters of some physical setup, but there will always be some maximal distance, which, with the chosen parameters, lies between repeater level 11 and 12, corresponding to about 10 000–20 000 km between the most remote stations. That the maximal distance corresponds to these repeater levels is intuitively clear, since the signal time on the 12th level is $2^{11}\times t_0\approx0.07$ s which begins to approach the order of the decoherence time $\kappa^{-1}=1$ s. The maximal distance will go down drastically for a repeater using the Innsbruck protocol (or other qubit-saving but time-consuming) protocols. But this distance will also go down for the standard repeater protocol when there are only a finite number of purification steps and imperfect links between repeater stations.

TABLE I. Purification regimes. The first column displays the repeater level where we assume a doubling of distance with each level. The second column contains the lowest possible fidelities of Werner states that can still be purified and the third column contains the fidelity to which they can be purified. The last column shows the maximal achievable fidelities of states that are purified by entanglement pumping with Werner states of fidelity 0.8.

Repeater level	Min. fidelity	Max. fidelity	Max. fidelity (pumping)
1	0.5276	0.985870	0.882761
2	0.5276	0.985778	0.882689
3	0.5278	0.985595	0.882545
4	0.5280	0.985227	0.882257
5	0.5284	0.984491	0.881682
6	0.5292	0.983017	0.875948
7	0.5310	0.980056	0.878236
8	0.5344	0.974090	0.873666
9	0.5417	0.961958	0.864609
10	0.5575	0.936728	0.846823
11	0.5965	0.880294	0.812544
12			

When we relate these results to the whole quantum repeater we realize the following.

(a) The standard repeater protocol uses regular entanglement purification, but only a few steps on each level as opposed to the infinitely many steps we apply to determine the purification range. Hence, there will be a dependence on the initial, lowest level state. But this dependence is weak and becomes less and less significant on higher levels, where more and more purification steps have been executed. Since the upper fixed point of the purification map for regular entanglement purification is independent of the initial state it translates into a general upper bound for the maximal reachable fidelity of any repeater run in error detection mode—with the exception of blind operation, see Sec. V.

(b) Repeater protocols based on entanglement pumping, e.g., the Innsbruck protocol, start with some initial state on the lowest level, and, again, the dependence on that initial state becomes weaker on higher levels. Note, however, that

TABLE II. Quantum repeater with standard repeater protocol and operational and memory errors included. For the parameters of errors and initial states see the text. The first column displays the repeater level. Level 1 corresponds to about 10 km, and we assumed a doubling of distance with each level. The second column contains the resources, i.e., the qubit pairs, needed to reach the corresponding level. The values in the third column are the fidelities we obtain on these levels.

Repeater level	Resources	Max. fidelity
1	15	0.956246
2	151	0.981122
3	1480	0.983974
4	1.44×10^4	0.983830
5	1.40×10^5	0.983086
6	1.37×10^6	0.981557
7	1.36×10^7	0.978481
8	1.36×10^8	0.972266
9	1.42×10^9	0.959568
10	1.61×10^{10}	0.932962
11	2.19×10^{11}	0.873666
12		

in the repeater process the DEJMPS map drives the states closer to binary mixtures, on which it afterward operates more efficiently. That is, higher repeater levels get states close to binary mixtures as their initial pumping states. The situation can be completely different when we determine the fixed points of the purification map and always use the same initial pumping state that is far from a binary mixture and closer to Werner states. Hence, these fixed points do not say much about the repeater, but they still illustrate the influence of the memory errors in a simple way.

2. Maximal distance of different repeater protocols

Now we have assembled all tools to analyze the quantum repeater operated in error detection mode with different repeater protocols. We do not simulate the repeater, but use the success probabilities of the purification steps to estimate the physical or temporal resources we need. In this way we obtain *average* values for the performance of the repeater and do not explore the worst cases when the purification on some level fails unusually many times.

For the standard repeater protocol where all pairs are initially prepared and then processed in parallel we expect to get a maximal distance close to the one where purification is no longer possible (see Table I). On the one hand, there is the advantage that purified pairs from lower levels are already closer to a binary mixture such that the purification threshold is better than for Werner states. On the other hand, the imperfect linking of pairs is additionally decreasing the fidelity. With the same choices for the parameters as above, and executing three purification steps on each level, we obtain Table II showing the repeater levels, the resources (qubit pairs) needed, and the maximal fidelity we reach. The resources are easy to compute. Let $p_i^{[l]}$ be the probability to succeed in the ith purification step on the lth repeater level. These probabilities correspond to the normalization factor in the DEJMPS map, Eq. (8). On average we need $2/p_i^{[l]}$ pairs to get one purified pair for round $i+1$. For three steps, we need $2^3/\Pi_{i=1}^3 p_i^{[l]}$ pairs on level l, and for the whole repeater with n levels we need $2^{3n}/(\Pi_{l=1}^n \Pi_{i=1}^3 p_i^{[l]})$ qubit pairs. We see that the maximal distance corresponds to repeater level 11, i.e., about $2^{10} \times 10$ km $\approx 10^4$ km where we get a fidelity of about 0.87. This distance is intercontinental, but the resources required are ridiculously high (hundreds of billions), and no optimization can change this order of magnitude significantly.

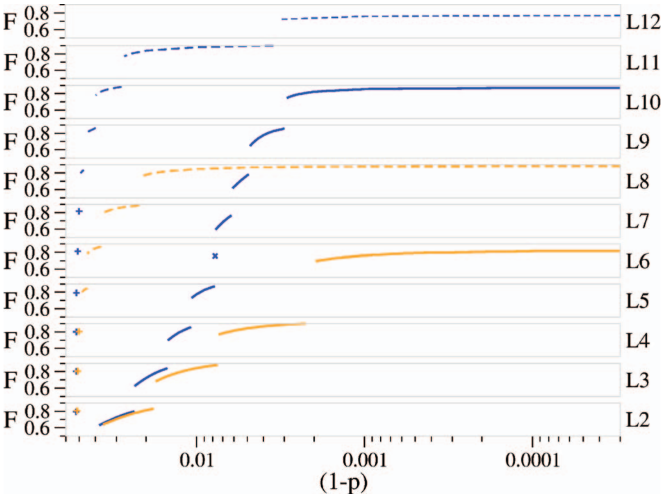

FIG. 1. (Color online) Maximal repeater level and fidelity F as function of the operational and measurement errors $(1-p=1-\eta)$. The distance on repeater level 1 is 10 km; every level ($L2$ to $L12$) doubles this distance. Dark lines have decoherence time $\kappa^{-1}=1$ s, light lines have $\kappa^{-1}=0.1$ s. Solid lines are a lower bound on the maximal distance for a repeater run with the Innsbruck protocol and with initial Werner states of fidelity 0.8 on level 1. Dashed lines show the limits of the purification map, which are an upper bound on any repeater run in error detection mode (with the exception of blind mode, Sec. V). For a more detailed discussion see text.

The Innsbruck protocol, which uses entanglement pumping for the purification, will profit even more from the fact that the states used to pump are close to binary mixtures on higher levels as compared to the pumping with Werner states (worst case, see Table I). However, the protocol saves physical resources (logarithmic scaling with distance) at the expense of polynomial temporal overhead [4]. This means that pairs on higher levels do not only have to wait for the classical signals that determine whether they have undergone a successful purification step, but also for all lower levels to produce a pair they can be purified with. While the temporal resources, the waiting times, scale polynomially with distance, any waiting time enters in the exponent of the decoherence map, Eq. (7), so this poses a severe restriction on the maximal distance.

In Fig. 1 we plotted the error rates $(1-p)=(1-\eta)$ against the maximal repeater level ($L1$ to $L6$, and $L1$ to $L10$, respectively) and the maximal fidelity F thereon for the Innsbruck protocol (solid curves). The upper curve (dark, solid) corresponds to a decoherence time $\kappa^{-1}=1$ s, the lower to $\kappa^{-1}=0.1$ s (light, solid). The initial states were Werner states of fidelity 0.8. Before we go into details, let us examine the key features of these curves. (a) On the left, we are in a regime that is dominated by the errors in operations $(1-p)$ and measurements $(1-\eta)$, where we set $p=\eta$ for convenience. In this regime, a decrease in the error rate quickly leads to higher repeater levels that we can reach. (b) On the right, where the errors are already small, the curve is dominated almost entirely by the decoherence time κ^{-1}. Naturally, a larger decoherence time allows for higher maximal repeater levels. In this regime we can decrease the error rates by orders of magnitude and still gain almost nothing. Note, however, that once the error rates are below 10^{-4} other schemes (concatenated CSS codes, quantum repeater in error correction mode) become available.

In the following we explain the details of the simulation and rules under which the plot was created. First, we estimated the waiting times in a conservative way. The waiting time of a qubit pair on some repeater level is the time this pair has to wait either until the classical signal arrives telling us whether a purification step was successful, or until the lower levels have produced the next pair for purification (whichever takes longer). In our conservative estimate we simply add both times, that is, we wait until we get the signal, then start to build up a new pair. Decoherence affects the qubit pairs during these waiting times. With our conservative estimate we establish a lower bound on the maximally reachable distance and fidelity telling us that we can expect to reach these levels with certainty for the Innsbruck protocol. Better estimates of the waiting times will shift the solid curves upward, but not very much: We usually gain at most one level with a better estimate. When we change the initial state on the lowest level (from the Werner states with fidelity 0.8 we used) we affect the curves only slightly. A higher fidelity for the initial Werner state (or a shape closer to a binary mixture) shifts the curves upward, and the difference becomes smaller in the region where the decoherence time dominates the plot. A lower fidelity shifts the curves downward, and there will be a point where we lose the whole curve when we drop below the purification threshold of the first level. Second, for each point in the plot, we optimized the number of purification steps executed on each level. We call this the purification strategy in the following. The aim of the optimization is to reach the highest level possible. The rule when a jump from some level l to a level $l+1$ occurs is the following. Assume that by some purification strategy X that is optimal for level l we have reached a certain fidelity $F_X^{[l]}$. Then we connect two pairs with this fidelity and get some pair with reduced fidelity $F_X^{[l+1]}$ on the next level without doing any purification on level $l+1$. If by some, usually different, purification strategy Y, which really does purification on level $l+1$, we can produce a level $l+1$ pair with fidelity $F_Y^{[l+1]} > F_X^{[l+1]}$, then the point in the plot moves to at least level $l+1$, where we repeat the test. If we cannot find such a Y, then the point is drawn on level l with fidelity $F_X^{[l]}$. Consider such a level-l point obtained by strategy X. Another technical restriction is that we do not allow to execute more purification steps on level l than we did on level $l-1$ in the strategy X. The reason is that once we cannot go to a higher level, we do not have to try to save time anymore and we could in principle do infinitely many purification steps on level l, but this would—while increasing the fidelity—drastically diminish the rate with which we create pairs. Changing the above rules would alter the jumping points and fidelities, but for every reasonable restrictions the effects would not matter much. We remark that similar optimization strategies of the number of purification steps at the different repeater levels were performed by the Harvard group [30].

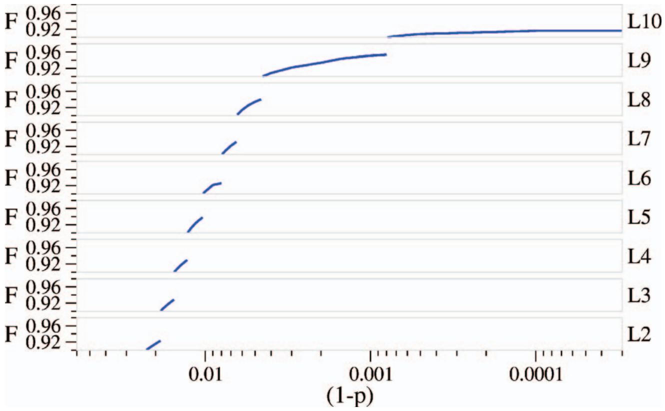

FIG. 2. (Color online) Maximal repeater level and fidelity F as function of the operational and measurement errors $(1-p=1-\eta)$. The distance on repeater level 1 is 10 km; every level ($L2$ to $L10$) doubles this distance. The decoherence time is $\kappa^{-1}=1$ s, the curve is a lower bound on the maximal distance for a repeater run with the Innsbruck protocol and with initial Werner states of fidelity 0.9 on level 1, showing a weak dependence on the initial fidelity as compared to Fig. 1. Additionally the fidelity was required to finally be above 0.9 on every level and all its lower levels in the repeater.

The dashed lines in Fig. 1 are the fixed points of the DEJMPS map obtained in the way discussed in Sec. III A 1, where the dark, dashed line corresponds to $\kappa^{-1}=1$ s, and the light, dashed line to $\kappa^{-1}=0.1$ s. Take, e.g., the point at $(1-p)=0.01$ in the upper dashed curve. There we find the value of level 11 from Table I. As explained in Sec. III A 1, these curves are absolute upper bounds on any repeater run in error detection mode—with the exception of blind mode that we discuss later. Generally speaking, when we run the repeater with the standard repeater protocol, i.e., with regular entanglement purification, we will be close to the upper bound; when we run it with the Innsbruck protocol using entanglement pumping, we will be close to the lower bound. Other entanglement pumping protocols, like the Harvard protocol, can, and likely will be, even below the lower bound valid for the Innsbruck protocol.

When we look at the fidelities in Fig. 1 we see that they can be very low, and we might ask whether this is not a drawback. However, there are two things to say about this. First, even final pairs with these low fidelities can be used, e.g., for communication purposes. Under certain conditions, an eavesdropper is factored out by the purification process [31] such that the pairs, though of low fidelity, are private. Second, we simply did not ask for pairs of higher fidelity and optimized for distance only. If, say for quantum teleportation, we need pairs of higher fidelity, we add this requirement to the rules. In Fig. 2 we added the rule that on any level and on all levels below it the fidelity must finally have been above 0.9. For the same initial conditions compared to Fig. 1 this additional restriction would mean that the curves would move downward. In Fig. 2 we changed the initial fidelity of the Werner states to 0.9 to comply with the new rule, so we cannot assert this claim by directly comparing the two plots. However, with the changed initial fidelity we support the claim that such a change does not have a strong influence on the curves. This, we can check by comparing the plots.

Let us sum up the key message. If we use a repeater protocol with entanglement pumping, which we do to avoid unmanageably large qubit numbers, and demand tolerable errors of one percent, then we cannot reach intercontinental distances. From Fig. 1, at a value of $1-p=0.01$, we read off a maximal level of 5 for a decoherence time of 1 s, and 3 for 0.1 s. If we assume better initial states and better estimates of the waiting times than our conservative ones, we might reach, say, level 7 in the first case. But $2^6 \times 10$ km $=640$ km is still not intercontinental. There are two ways to overcome this problem: Trivially, one can try to improve the error rates or the decoherence time (see Sec. IV). One reaches intercontinental distances, e.g., for a decoherence time of 1 s and error rates increased by one order of magnitude, namely 0.001. Second, one can combine protocols. On higher levels one can, e.g., switch from the Innsbruck protocol to the standard repeater protocol at the expense of larger physical resources. We will come back to the question of such repeater architectures in a later section.

Note that decreasing the errors by another order of magnitude, to 10^{-4}, does not give us much further advantage. However, at this error rate different strategies become available, and we will now turn to one of these, the repeater in error correction mode.

B. Limits of the quantum repeater in error correction mode

In error correction mode, the repeater is limited both by the memory errors and the very stringent thresholds for operation fidelities. The first limit can be completely removed (see Sec. V) and we discuss it only shortly. The second limit remains, and we present the results for thresholds below.

1. Limits by memory errors

If we use purification via error correction in some repeater protocol instead of purification via error detection we still have to wait for the classical one-way signal to arrive in order to know which correction operation to apply. Concerning waiting times during which memory errors occur we gain nothing in this way. On the contrary, since purification ranges are much smaller than for error detection schemes [21], we have the following situation. We need higher fidelities in operations and measurements (at least 10^{-4}) and are still sooner out of the game than in the error detection repeater protocols. This seems like a lose-lose situation, but we will show in Sec. V that we can overcome the problem of waiting times completely for a repeater in (concatenated) error correction mode, while this is not true for a repeater in error detection mode. For the discussion of threshold limits we will hence already assume that memory errors are absent, or, more precisely, absorbed into lowered operation fidelities.

2. Threshold limits

Even when memory errors do not have to be taken into account explicitly, the threshold limits of operation and measurement fidelities for the whole repeater must be derived from the thresholds for entanglement purification and connection. As pointed out in Sec. II B 2, one can construct entanglement purification protocols from CSS codes using only one-way classical communication (i.e. the protocols run in error correction mode). Transmitting several copies of an entangled state through noisy channels and purifying them using a single step of such an entanglement purification protocol results in a single copy with increased fidelity, which can then be used to transmit quantum information via teleportation. As shown in Sec. II B 2, this procedure is in fact equivalent to encoding quantum information into several qubits using this CSS code, transmitting the encoded state through the noisy channel and performing error correction (decoding) at the receiver station.

If we perform several purification steps, i.e., use output states of the previous purification round as input states for the next purification round, we can establish a similar equivalence, this time to *concatenated* error correction CSS codes. The number of purification steps corresponds to the number of concatenation levels of the code. This equivalence also holds when taking noise (of the form we consider here) in local control operations into account. As a consequence, entanglement purification protocols in error correction mode and quantum error correction (QEC) schemes have the same thresholds with respect to tolerable channel noise and noise in local control operations. In particular, thresholds for tolerable noise in local control operations for QEC have been estimated to be of the order of 10^{-4}, leading to the same threshold for the corresponding one-way entanglement purification protocols. This number has to be compared to a tolerable noise of the order of several percent for entanglement purification protocols with two-way classical communication, i.e., run in error detection mode. Aschauer [21] explicitly investigated the performance of entanglement purification protocols constructed from specific CSS codes in the presence of noisy local control operations for a simplified error model. He finds that the threshold for noise in local control operations (in his error model) is almost ten percent when using two-way classical communication, while it is of the order of 0.5 percent for one-way purification protocols. Also the tolerable channel noise (i.e., minimal required fidelity) is significantly lower for one-way purification protocols as compared to two-way protocols.

Notice that thresholds for entanglement purification, together with the influence of noise on the connection process, determine the maximal length of the elementary segments in the quantum repeater, and also the threshold for the total repeater protocol. This threshold is even more stringent than the threshold for entanglement purification. In particular, when using one-way entanglement purification protocols, one needs to use elementary segments with smaller distance (i.e., more repeater stations), and the threshold for the repeater protocol will be significantly more stringent (by a factor of about 20–100) as compared to thresholds for the quantum repeater based on two-way entanglement purification.

We finally remark that the equivalence between entanglement purification protocols and QEC schemes based on CSS codes carries over to the whole repeater protocol, where also entanglement swapping is involved. It turns out that establishing an entangled pair using the repeater protocol, i.e., by a nested sequence of entanglement purification and entanglement swapping operations, and using the pair to teleport an unknown quantum state is in fact equivalent to transmitting the quantum state in an encoded form through the noisy channel using a specific concatenated CSS code. Strictly speaking, this equivalence only holds for noise channels which are diagonal in the Pauli basis, however, this is exactly the noise model we consider here. The essential property one uses is that coding and decoding operations for CSS codes, and hence also all involved operations in the entanglement purification protocol, are Clifford operations. It follows that Pauli operators can be commuted through the coding and decoding operations as well as through the noise maps (if they are Pauli diagonal) and simply become a different Pauli operation corresponding to a (correctable) basis change. These Pauli operations appear either due to different outcomes in Bell measurements of the connection process, or due to required correction operations after establishing the error syndrome in a certain purification step. The communication scheme that is equivalent to the quantum repeater corresponds to using a concatenated CSS code. Concatenation comes, on the one hand, from several purification steps performed at a fixed repeater level, and, on the other hand, from the concatenated scheme of the quantum repeater to establish entangled pairs over larger and larger distances. The latter concatenation translates to a specific way in which error correction is performed at different repeater stations. At certain repeater stations, e.g., at the final station error correction at all nesting levels is performed, while at intermediate repeater stations error correction is done only up to a fixed concatenation level. For instance, at the second repeater station, only error correction at the lowest concatenation level is executed, while at the middle repeater station (at half the distance) error correction is applied up to the second highest concatenation level.

IV. REDUCING MEMORY ERRORS

As we have seen in the previous section, memory errors limit the possible communication distance when using a quantum repeater run in standard mode. The actual achievable distance crucially depends on the quality of local memory, characterized by the coherence time, as is evident, e.g., from Fig. 1. If one aims to achieve quantum communication over some fixed distance, say intercontinental distance, then it is sufficient to ensure that quantum memories of sufficiently high quality are available. There are various strategies known to increase coherence times, including quantum systems with extremely weak coupling to the environment, decoherence free subspaces [32], dynamical decoherence free subspaces [33], or topologically protected quantum memory [34]. Some experimental proposals for a quantum repeater take these strategies into account [6,8,9], where, e.g., a quantum repeater with qubits in a decoherence free subspace has been proposed in [6]. Coherence times of up to 20 s have been demonstrated experimentally [35] for qubits in decoherence free subspaces. Although coherence times are long in this case and might be sufficient for practical purposes, they are not infinitely long, which would be required for communication over arbitrary distance. Further reduction of memory errors may be possible, at the price of increased complexity and eventually reduced error thresholds of the repeater protocol.

The complete elimination of the influence of memory errors seems only possible when using strategies from fault tolerant quantum error correction, where concatenated error correction codes are used to obtain a perfect quantum memory [36], leading to error threshold estimates of the order of 10^{-3}. Notice that the problem of storage of quantum information is less demanding than the problem of processing (encoded) quantum information as it is required in fault tolerant quantum computation. When using concatenated CSS codes, only Clifford operations are required for storage, and thus one might expect less stringent error thresholds. The whole repeater protocol as such can still be applied in the standard fashion, and the distance between repeater stations is the same as in the case where memory errors are disregarded. This distance is essentially given by the minimal required fidelity of the two-way entanglement purification protocol. Clearly the thresholds on noisy local control operations for the whole repeater scheme are now determined by the more stringent thresholds for quantum memory. However, not at all repeater levels perfect quantum memory is required. At lower repeater levels, no quantum memory is needed. At higher repeater levels, the required storage time (and hence the required coherence time) gets larger, and high fidelity quantum memory is needed, where the effort to produce the required fidelity increases with the repeater levels. The complexity of the protection mechanism also increases, and so does the requirement on the fidelity of local control operations. Finally, at a certain repeater level, concatenated error correction codes need to be used that provide *perfect* quantum memory, and threshold results for such schemes can then apply.

When concatenated error correction codes are used for local memory, it is important to note that the repeater protocol based on two-way entanglement purification (error detection mode) is still *inequivalent* to sending encoded quantum information through a noisy quantum channel by using again some concatenated code. For instance, the repeater stations need to be much closer in the latter case, leading to a significant overhead and possibly also to more stringent thresholds.

V. QUANTUM REPEATER IN BLIND MODE

In this section we consider a blind operational mode for the quantum repeater to overcome or lessen the limitations due to memory errors. Blind operation of the quantum repeater works for both error detection mode as well as error correction mode. In the first case, blind mode can add some additional repeater levels on top of the ones possible otherwise with reasonable overhead, in the second case it enables the quantum repeater to create entanglement over arbitrary distances, albeit with lower thresholds.

A. Blind error detection mode

We show that the DEJMPS protocol can be executed blindly [29], i.e., without waiting for classical communication, at the price of an exponentially decreasing success probability. Entanglement swapping can also be performed blindly such that the whole repeater can run in blind mode, at least on a few levels where the additional resources, which are required to counteract the exponentially decreasing success probability, stay reasonably low.

1. Blind purification

Blind two-way purification is a variant of the standard entanglement purification in error detection mode. The only difference is that one does not wait for any classical signal to arrive, which would tell whether a purification step was successful, and thus eventually operates on "bad" pairs. In fact, any basis shift of input states only leads to (i) a reinterpretation of what is called a successful purification step and (ii) a new basis shift of the resulting density matrix. In this sense, the basis shifts do not matter, and the same sequence of operations (i.e., the same protocol) can be used, regardless of the initial basis shifts.

This is most evident in Eq. (3), where entanglement purification with perfect local control operations is described. It is straightforward to see that also for noisy local operations (of the form we consider here), these properties are kept, Eq. (8), because basis shifts (corresponding to σ_z operations) can be commuted through noise maps that are diagonal in the Pauli basis.

This implies that, in principle, several purification steps can be performed without knowing the required correction operations. Only the interpretation of the obtained measurement outcome, and hence the decision whether the purification step was successful or not, requires knowledge of basis shifts, and hence classical communication. Clearly, if several purification steps are performed blindly in such a way, the resulting pair is only useful if it turns out that in fact all steps correspond to successful purification steps. The success probability for the total procedure thus goes down exponentially with the number of purification steps. If the operations were perfect, the success probabilities would converge to one since also the fidelity converges to one, and the total success probability need not necessarily go down exponentially. With errors in the operations and measurements, on the other hand, the maximum reachable fidelity and thus the maximum success probability for a purification step is bounded away from one, and exponential decay of the total success probability follows.

2. Blind swapping

The maps for connection (entanglement swapping) do not require any specific form of the input states. Also imperfect connection processes can be performed on two pairs with arbitrary basis shifts, leading to a new pair with a new basis shift depending on measurement outcomes and the initial basis shifts. Again, this is evident from the description of the connection process when local operations are perfect [see Eq. (4)]. The property is kept for noisy operations if the noise is Pauli diagonal, Eq. (9), since then we are again dealing with Clifford operations only.

TABLE III. Required *additional* resources p_{tot}^{-1} when operating the quantum repeater in blind operational mode under the assumption that $M=3$ purification steps with constant success probability p_{suc} are required. Number of additional repeater levels is given by m, and the communication distance is increased by a factor of 2^m.

	$p_{\mathrm{suc}}=0.95$	$p_{\mathrm{suc}}=0.9$
$m=1$	$p_{\mathrm{tot}}^{-1}=1.17$	$p_{\mathrm{tot}}^{-1}=1.37$
$m=2$	$p_{\mathrm{tot}}^{-1}=2.52$	$p_{\mathrm{tot}}^{-1}=6.66$
$m=3$	$p_{\mathrm{tot}}^{-1}=254.6$	$p_{\mathrm{tot}}^{-1}=8.7\times 10^{4}$
$m=4$	$p_{\mathrm{tot}}^{-1}=2.7\times 10^{14}$	$p_{\mathrm{tot}}^{-1}=4.4\times 10^{19}$

3. Blind repeater protocol

Since both entanglement purification and swapping can be done blindly in the two-way, error detecting scenario the whole repeater can be operated in blind mode. Operating the repeater blindly, one can sidestep the problem of memory errors due to the long waiting times for classical signals. A new limit is set by the gate operation time, which, for entanglement pumping, still accumulates. While in principle the new maximal distance is infinite when operating the repeater with standard entanglement purification where all pairs are available in parallel, and very large for the protocols based on entanglement pumping, the success probability of the whole repeater goes down exponentially with distance. Consider the following example. We assume that three purification steps at each repeater level are required, $M=3$, and consider the scaling of the required resources when operating m repeater levels blindly. We also assume that only two pairs are connected before repurification. This leads to an increase of the distance by a factor of 2^m. For simplicity we say that each purification step succeeds with a certain fixed success probability p_{suc} (the success probability depends on the fidelity of the initial pairs and hence is strictly speaking different for different purification steps, however, we neglect this effect since the overall scaling behavior will not be affected by this simplifying assumption). In this case, the total success probability that all involved purification processes up to repeater level m were successful is given by

$$p_{\mathrm{tot}}=p_{\mathrm{suc}}^{(2^{m-1}M^m)},$$

and thus on average $1/p_{\mathrm{tot}}$ copies of the whole setup (i.e., parallel channels) are required to obtain on average a single pair at the end of the procedure. Alternatively, one can say that the rate of the resulting pairs is decreased by a factor p_{tot}. Table III illustrates that up to three additional repeater levels, $m=3$, lead to a reasonable overhead, while for $m>3$ the overheads explode and become completely impractical. For $m=3$, the possible communication distance is increased by a factor of 8, i.e., almost an order of magnitude.

We remark that when fewer purification steps M at each repeater level are required, or more than only two elementary pairs can be connected before repurification, one can increase the communication distance even further. One may even design the repeater scheme in such a way that at higher repeater levels (where blind mode is used) fewer purification steps M are required. In this case in principle more additional repeater levels can be added while keeping the overhead moderate (for smaller M), and each additional repeater level not only allows one to double the distance but to increase it by a factor of L (if L elementary pairs can be connected), leading to a total gain of a factor of L^m. For instance, if $M=2$ and $L=3$, three repeater levels, $m=3$, yield an overhead factor of about 40 if $p_{\mathrm{suc}}=0.95$, while the communication distance is increased by a factor of $3^3=27$. Thus a gain of about an order of magnitude in distance with overhead of order 10^2 seems possible, where in some favorable situations even higher gains can be expected.

Because of the exponentially small success probability, blind mode is not a solution for the whole repeater in error detection mode. However, for practical purposes one may still use blind mode on a few of the topmost repeater levels at the cost of a reduced production rate of entangled pairs. In this sense, the parameter m above corresponds to the *additional* repeater levels that are operated blindly, while low repeater levels are operated in the standard way. These last levels should be run in the parallel, standard repeater mode, since for protocols using entanglement pumping the classical signals will usually have arrived before a new pair is ready from lower levels, and it would be disadvantageous to operate blindly and to ignore the information available.

B. Blind error correction mode

In this subsection we describe a possible solution to overcome the limitation of communication distance due to memory errors. This solution is due to the fact that the repeater can be unconditionally run blindly in error correction mode, i.e., there is no exponentially small success probability, when special error correcting codes, CSS codes, are used.

1. Blind purification and entanglement swapping

Again, the key point is that the entanglement purification protocols can also be used if the initial bases of the pairs are shifted. More precisely, since the coding and decoding networks are based on CSS codes, all unitary operations applied in the purification protocol are Clifford operations. Therefore, any basis shift (described by some Pauli operation applied to the state before coding and decoding) can be commuted through the network, still leading to a (different) Pauli operation corresponding to a (different) basis shift. Only the interpretation of measurement outcomes when attempting to detect an error syndrome, and the final basis shift, may differ. In this sense, the classical information on measurement outcomes are not really required when performing the protocol, as the required operations are independent of eventual basis shifts. Only at the end of the procedure, when a final basis shift or correction operation needs to be determined, the classical signals containing all measurement outcomes are needed. That is, the purification protocol can be run blindly. The connection process by entanglement swapping is the same as in the two-way, error detecting scenario and can hence be performed blindly.

2. Blind repeater protocol

Since both entanglement purification by error correction and the connection process by entanglement swapping can be executed blindly the whole repeater can be run in blind mode. The main difference to the error detection mode is the following. Recall that in the error detection mode the purification process is probabilistic, and the total success probability hence goes down exponentially with the number of purification steps, whereas in error correction mode the purification is deterministic. Since entanglement swapping is also deterministic, the whole repeater can be run in blind error correction mode without restrictions. In particular this means that there are no true waiting times if concatenated error correction is used, where, similarly as in the standard repeater protocol, all pairs involved in the process are created in the very beginning. With true waiting times we mean times other than gate operation times because memory errors occurring during gate operations can be absorbed into a lowered gate fidelity. Hence, entangled pairs over arbitrary distances can be generated in this way. However, the limiting factors are the very stringent error thresholds (see Sec. III B 2) and the huge number of qubits one would need.

We remark that despite the equivalence of the repeater run in (blind) error correction mode with direct transmission of quantum information using a certain concatenated CSS code, there is an advantage of the quantum repeater in a different respect. In particular, when one considers the time required to establish an entangled pair over distance N, the repeater scheme allows one to do this in $\log_2 N$ time steps where each time step corresponds to the time required for quantum communication over the distance of an elementary segment τ_0. Although the pair produced in this way is unknown at this stage until classical information arrives (which requires a time of order Nt_0, where t_0 is the time for classical communication over one segment), it can nevertheless already be used for teleportation or for key distribution as outlined below. On the other hand, using error correction to protect transmitted quantum information corresponds to sending the information sequentially through quantum channels, leading to a communication time of $N\tau_0$.

The difference in the communication time can be significant. Even when taking the additional classical communication into account, the repeater scheme may offer still advantages, in particular in situations where $\tau_0 > t_0$. This is already the case when transmitting photons through optical fibers and using free-space classical communication, however, the effect is much more evident when considering quantum information transport, e.g., by means of electron transmission. Such a repeater scheme is discussed in [33], where entanglement between distant quantum dots is generated by transporting electrons via charge control, connecting entangled pairs and repurifying them. In this case, entanglement can be used to perform teleportation-based gates between far distant qubits, providing an important element for a scalable fault tolerant quantum computer architecture based on charge controlled quantum dots.

C. Using unknown entangled pairs

In both blind modes, error detection as well as error correction mode, the basis shift and hence the correct interpretation or the required correction operation remains unknown as long as all the measurement results from purification steps and connection processes are not known at the end node. Still, the entangled pairs produced in such a way can be useful, although one does not know the state that actually is at hand. This can only be determined at a later stage after all classical signals arrive.

First, one may assume that memory errors are only relevant at intermediate repeater stations and other ways of protecting quantum information are available at starting and end points. Such an assumption is in some sense natural, as keeping produced entangled pairs as a resource requires a quantum memory anyway. In addition, even if (almost) perfect memories are available, technologically they might be difficult to realize and thus one may assume that at intermediate repeater stations memory errors play a role, while at end nodes memory errors can be avoided.

Second, one may use the resulting entangled pair for teleportation of an unknown quantum state, thereby realizing high-fidelity quantum communication. However, the correction operations required in the teleportation protocol now do not only depend on the measurement outcomes in the teleportation process, but also on the basis of the used Bell pair (and hence on all intermediate measurement outcomes in the generation of the Bell pair). In this sense, a quantum memory is required again (at least at the end node), such that the teleported quantum state can be restored and further processed.

Third, one may use the resulting pair for quantum cryptography, i.e., to establish a secret key between A and B. In this case, measurements are performed to either run a teleportation based version of a protocol such as the BB84 protocol [37], six-state protocol [38], Singapore protocol [40], or alternatively the E91 protocol [39]. From now on, all information is classical, and storage of quantum information is no longer required. The additional information about the basis of the involved entangled pair (i.e., the outcomes of all measurements involved in the repeater protocol) may arrive at any later stage, and only lead to a re-interpretation of the measurement outcomes (i.e., the used measurement basis). Eventually, the yield of the key-distribution protocols is reduced since not all measurement bases can be used to establish a key, however, key generation will still be possible.

We remark that the possibility to operate the repeater in such a blind mode may also have consequences on the practical realization of such a device. For the repeater operated in standard mode, it is usually argued that there should be flying qubits (usually photons) that are mapped on static qubits (atoms, ions, solid state devices, atomic ensembles) and vice versa. The flying qubits are used to distribute entanglement over noisy quantum channels, while static qubits are used to store and process quantum information at different repeater stations. However, as for a repeater operated in such a blind mode there is *no longer a need to store qubits*, the procession (i.e., error correction, measurements) might be performed right away on the flying qubits. In this way, one could avoid the (technically demanding) interfaces between flying and static qubits. What remains is the requirement to process the qubits, i.e., to perform appropriated unitary operations for coding, decoding, and measurements.

VI. REPEATER ARCHITECTURE

While the quantum repeater in error correction mode offers a solution to achieve infinite communication distance, the stringent error thresholds and huge physical resources needed make it unfavorable for practical implementations.

The most reasonable architecture of a quantum repeater, solely using error detection mode, could be the following. On the lowest levels, where classical signalling time is still short, one should employ a repeater protocol using entanglement pumping for purification. In this way, one saves physical resources. Which protocol to use exactly depends on the physical resources available, and one should always fully use the available resources to save time. Once one cannot go further with this first protocol, one can switch to a protocol that operates on many copies in parallel, like the standard repeater protocol. In addition, techniques to reduce memory errors can be applied at higher repeater levels. Finally, when even the capabilities of that protocol and improved quantum memories are exhausted, one may change to operate the second protocol in blind mode on the topmost levels. The requirements for the physical resources become very demanding for the last two stages.

The principal constraints are the distance over which one wants to establish an entangled pair, the physical resources available, and the parameters of the errors that will occur. Given these, the building of the quantum repeater is then an intricate engineering and optimization problem that has to deal with questions like: Which purification protocol do we use? Which working fidelity is best or how many purification steps do we perform on some repeater level? Which repeater protocol do we use and when do we switch to another? In theory this optimization can be very complicated since all these questions are dependent on each other, but in practice one will most likely also be limited in the ways one can optimize the working processes.

We want to make one last remark on the reuse of qubits. In the standard repeater scheme, most qubits, when they have been measured, do nothing until the repeater has completed its cycle. But one can immediately reuse any qubits that are no longer involved in the repeater process. Assume we add one more qubit at each repeater level, say n qubits, then we can run a "second wave" right after operations on the lowest level are performed under the same initial conditions we found before. If we add $n-1$ qubits on each repeater level, i.e., $n(n-1)$ qubits in total, then the "first wave" will be complete when we start the nth, since the repeater in standard mode needs n time steps for completion when there are n repeater levels. Then, the wave $n+1$ can use again the qubits of the first wave. In this way all qubits are used at all times, and for the price of the very demanding resources we get at least a very high bit rate that is only limited by the gate operation time.

VII. SUMMARY

We have studied the quantum repeater subject to memory errors. We have shown that memory errors imply that the standard operation mode of the repeater, error detection mode, can establish entangled pairs only over some maximal distance. To overcome this restriction, a direct solution is to reduce or correct memory errors by using methods to increase coherence times or a local quantum memory based on concatenated error correction codes. However, the complexity and requirements on accuracy of local control operations increase with the distance, and the error thresholds for quantum memory determine the error thresholds of the quantum repeater. Alternatively, one can run the repeater in error correction mode. We showed that this operation mode is equivalent to the protection of quantum information with concatenated quantum codes and has again unfavorable error thresholds. If one wants to benefit from the much higher thresholds of the standard mode using two-way entanglement purification and does not have the capability to correct memory errors, one has to accept some maximal distance and questions like scalability are no longer an issue (top down view). In their place are now questions about engineering and optimization. As an additional tool of practical importance, we described an operation mode for the repeater called blind mode, which can help to push the limits for the maximal distance farther. In particular, one can increase the communication distance by an order of magnitude with only modest overhead in physical resources. With a given error model we analyzed different repeater protocols, the resources they require, and the maximal distance over which they can distribute entangled pairs. We suggested a general architecture for the quantum repeater that switches protocols according to demand.

We finally also mention that free-space, satellite-based quantum communication [41] over long distances has been discussed as an alternative approach to the (ground-based) quantum repeater. At present it is not clear whether technological difficulties can be overcome in this proposed scheme. Notice, however, that elements of the quantum repeater and the schemes discussed here may be adopted to enhance satellite-based schemes as well. Very recently, the problem of memory errors in a quantum relay [42] has been addressed in [43], where it was shown how to use multiplexing to increase the yield. However, this investigation does not solve the problem of memory errors in the full quantum repeater as discussed here. To summarize, while intercontinental quantum communication with entangled pairs, created by the quantum repeater, seems to be out of reach today, the perspective that this goal can be realized in the foreseeable future is still very promising.

ACKNOWLEDGMENTS

This work was supported by the Austrian Science Foundation (FWF) and the European Union (OLAQUI, SCALA, QICS). W.D. acknowledges support from the ÖAW through project APART, and B.K. from the FWF through project Elise-Richter.

[1] E. Knill and R. Laflamme, e-print quant-ph/9608012. See also D. Aharonov and M. Ben-Or, *Proceedings of the 29th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1997), p. 176; e-print quant-ph/9611025; C. Zalka, e-print quant-ph/9612028.

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

[3] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[4] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[5] L. Childress, J. M. Taylor, A. S. Sorensen, and M. D. Lukin, Phys. Rev. A **72**, 052330 (2005); Phys. Rev. Lett. **96**, 070504 (2006).

[6] A. Klein, U. Dorner, C. Moura Alves, and D. Jaksch, Phys. Rev. A **73**, 012332 (2006).

[7] S. J. Enk, J. I. Cirac, and P. Zoller, Science **279**, 205 (1998).

[8] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).

[9] Z.-B. Chen, B. Zhao, J. Schmiedmayer, and J.-W. Pan, e-print quant-ph/0609151; B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, e-print quant-ph/0609154; L. Jiang, J. M. Taylor, and M. D. Lukin, e-print: quant-ph/0609236.

[10] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New J. Phys. **8**, 184 (2006).

[11] W. Dür, P. Zoller, and H.-J. Briegel, in *Lecture Notes on Quantum Information*, edited by D. Bruss and F. Leuchs (Wiley-VCH, Weinheim, 2006).

[12] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[13] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[14] J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Nature (London) **410**, 1067 (2001).

[15] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, Nature (London) **409**, 1014 (2001).

[16] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Nature (London) **423**, 417 (2003).

[17] T. Yamamoto, M. Koashi, S. K. Özdemir, and N. Imoto, Nature (London) **421**, 343 (2003).

[18] P. Walther, K. J. Resch, C. Brukner, A. M. Steinberg, J.-W. Pan, and A. Zeilinger, Phys. Rev. Lett. **94**, 040504 (2005).

[19] R. Reichle, D. Leibfried, E. Knill, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Nature (London) **443**, 838 (2006).

[20] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993); S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998); J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998); H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **71**, 050302(R) (2005).

[21] H. Aschauer, Ph.D. thesis, LMU Munich (2004); http://edoc.ub.uni-muenchen.de/archive/00003588/.

[22] The CNOT operation is defined by $|i\rangle_A|j\rangle_B \rightarrow |i\rangle_A|i\oplus j\rangle_B$, where $\oplus$ denotes addition modulo 2.

[23] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, in *Quantum Computer, Algorithms and Chaos, Volume 162*, Proceedings of the International School of Physics "Enrico Fermi", edited by G. Casati, D. L. Shepelyansky, P. Zoller and G. Benenti (IOS, Amsterdam, 2006); see also e-print quant-ph/0602096.

[24] W. Dür and H. J. Briegel, in *Lecture Notes on Quantum Information*, edited by D. Bruss and F. Leuchs (Wiley-VCH, Weinheim, 2006).

[25] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[26] W. Dür and H. J. Briegel, Phys. Rev. Lett. **90**, 067901 (2003).

[27] Strictly speaking this is not a point but a manifold in $\mathbb{R}^4$ since whether the map can still purify a certain state depends on all 4 coefficients $\lambda_{00}, \ldots, \lambda_{11}$.

[28] W. Dür, M. Hein, J. I. Cirac, and H. J. Briegel, Phys. Rev. A **72**, 052326 (2005).

[29] W. Dür, J. Calsamiglia, and H. J. Briegel, Phys. Rev. A **71**, 042336 (2005).

[30] J. M. Taylor (private communication).

[31] H. Aschauer and H. J. Briegel, Phys. Rev. Lett. **88**, 047902 (2002).

[32] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997); L.-M. Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998); D. A. Lidar, I. L. Chuang, and K. B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998); D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley, *ibid.* **85**, 1758 (2000).

[33] J. M. Taylor, W. Dür, P. Zoller, A. Yacoby, C. M. Marcus, and M. D. Lukin, Phys. Rev. Lett. **94**, 236803 (2005).

[34] A. Yu. Kitaev, in *Proceedings of the Third International Conference on Quantum Communication and Measurement*, edited by O. Hirota, A. S. Holevo, and C. M. Caves (Plenum, New York, 1997); E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, J. Math. Phys. **43**, 4452 (2002).

[35] H. Häffner, F. Schmidt-Kaler, W. Hänsel, C. F. Roos, T. Körber, M. Chwalla, M. Riebe, J. Benhelm, U. D. Rapol, C. Becher, and R. Blatt, Appl. Phys. B: Lasers Opt. **81**, 151 (2005).

[36] Andrew M. Steane, Phys. Rev. A **68**, 042322 (2003); in *Decoherence and its Implications in Quantum Computation and Information Transfer*, edited by Gonis and Turchi (IOS, Amsterdam, 2001), pp. 284–298.

[37] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[38] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

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

[40] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Rehcek, and J. Anders, e-print quant-ph/0412075; J. Anders, H. K. Ng, B.-G. Englert, and S. Y. Looi, e-print quant-ph/0505069.

[41] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002); C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P. Tapster, and J. Rarity, Nature (London) **419**, 450 (2002); M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, Science **301**, 621 (2003); J. G. Rarity, P. R. Tasper, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82.1 (2002); M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).

[42] E. Waks, A. Zeevi, and Y. Yamamoto, Phys. Rev. A **65**, 052310 (2002); B. C. Jacobs, T. B. Pittman, and J. D. Franson, *ibid.* **66**, 052307 (2002); N. Gisin, I. Marcikic, H. de Riedmatten *et al.*, Proceedings of the 6th International Conference on Quantum Communication, Measurement and Computing (QCMC 02), e-print quant-ph/0301181; H. De Riedmatten *et al.*, Phys. Rev. Lett. **92**, 047904 (2004); D. Collins, N. Gisin, and H. de Riedmatten, J. Mod. Opt. **52**, 735 (2005).

[43] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, e-print quant-ph/0610036.