PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel

H.-J. Briegel, W. Dür1, S. J. van Enk, J. I. Cirac and P. Zoller

Phil. Trans. R. Soc. Lond. A 1998 **356**, 1841-1851
doi: 10.1098/rsta.1998.0252

The Royal Society

Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel

By H.-J. Briegel[1,2], W. Dür[1], S. J. van Enk[3], J. I. Cirac[1,2] and P. Zoller[1]

[1]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria*
[2]*Universidad de Castilla–La Mancha, 13071 Ciudad Real, Spain*
[3]*Norman Bridge Laboratory of Physics 12-33, California Institute of Technology, Pasadena, CA 91125, USA*

We show how to create maximally entangled Einstein–Podolsky–Rosen pairs between spatially distant atoms, each of them inside a high-Q optical cavity, by sending photons through a general noisy channel, such as a standard optical fibre. An error-correction scheme that uses few auxiliary atoms in each cavity effectively eliminates photoabsorption and other transmission errors. This realizes the 'absorption-free channel'. A concatenation protocol using the absorption-free channel allows for quantum communication with single qubits over distances much larger than the coherence length of the channel.

Keywords: quantum repeater; EPR correlations; purification; quantum communication; quantum network; absorption-free channel

1. Introduction

The concept of a distant maximally entangled pair of particles, i.e. an Einstein–Podolsky–Rosen (EPR) pair (Einstein *et al*. 1935) plays a key role in both theoretical and in practical aspects of quantum communication. It has been shown by Bennett *et al*. (1993) that EPR pairs can be used to send unknown quantum states by means of teleportation. This has also been demonstrated experimentally, using photons, by Bouwmeester *et al*. (1997) and Boschi *et al*. (1998). Other examples include the possibility of secure distribution of cryptographic keys (Ekert 1991), imperfect cloning of a quantum state (Gisin & Massar 1997; Bruss *et al*. 1997), and the implementation of non-local conditional operations in quantum networks (Grover 1997).

In the present paper we concentrate on a realistic scheme that could be used for the creation of EPR pairs between atoms, and thus for quantum communication. We use a quantum optical implementation that combines elements that have been experimentally realized or can be expected to be realized in the near future. For example, a significant process has been reported in experimental quantum optics with trapped ions and in cavity QED (CQED) , both in the optical and in the microwave regime (Karlson 1998). Highlights of this development include first steps towards the implementation of *quantum-logical operations*, such as two-qubit operations that form the building blocks for quantum computing. Monroe *et al*. (1995) have succeeded in performing a universal two-bit quantum gate, using the quantized centre-of-mass

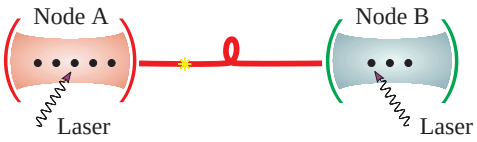

Figure 1. Quantum optical scheme for creating an EPR pair of atoms over a noisy channel.

motion of a trapped ion and its internal quantum degrees of freedom. In CQED the basic elements of gate operations involving the internal state of an atom and a cavity mode have been demonstrated by Turchette *et al*. (1995), and recently entangled internal states of two atoms have been produced (Hagley *et al*. 1997).

This paper gives a brief introduction to the recent work by the Innsbruck group (Cirac *et al*. 1997, 1998; van Enk *et al*. 1997*a–c*) on the subject of quantum communication.

2. Physical scheme

The scheme we propose is decribed in detail by Cirac *et al*. (1997) and van Enk *et al*. (1997*a*). It uses long-lived states of atoms as the physical basis for storing qubits and photons as a means for transferring these qubits from one atom to another. To allow for a controlled transfer of the qubit, the atoms are embedded in high-finesse optical cavities which are connected by an optical fibre, as shown in figure 1. For successful transmission of photons, appropriately tailored Raman pulses are applied to the atoms at the sending and the receiving time. These pulses map the qubit from the atomic state to a specific photon wavepacket and vice versa.

The optical cavity–fibre system, together with the laser pulses constitutes what we abstractly call a *noisy quantum channel*. Before we talk about noise processes in more detail, let us briefly discuss the ideal situation.

Ideally, the scheme realizes the following transmission:

$$[\chi_0|0\rangle_{\mathrm{A}} + \chi_1|1\rangle_{\mathrm{A}}]|0\rangle_{\mathrm{B}} \rightarrow |0\rangle_{\mathrm{A}}[\chi_0|0\rangle_{\mathrm{B}} + \chi_1|1\rangle_{\mathrm{B}}], \tag{2.1}$$

where an unknown superposition of internal states $|0\rangle$ and $|1\rangle$ in atom A in the first cavity is transferred to atom B in the second cavity. The cavities may be part of a larger network, so we often refer to them as node A and node B, respectively. The selected internal states $|0\rangle$ and $|1\rangle$ of the atoms define, in the language of quantum information theory, the 'computational basis' for the qubit.

It is important to realize that the atom A may be entangled to other atoms in the same cavity or at other nodes of the network. In that situation, the coefficients χ_0 and χ_1 in (2.1) are no longer complex numbers but denote unnormalized states of the other atoms. Thus the transmission (2.1) can be used to transfer single atomic states, but also to transfer *entanglement*. For instance, starting from single particle states, an EPR pair can be created by a two-step process:

$$\begin{aligned}[\chi_0|0\rangle_{\mathrm{A}} + \chi_1|1\rangle_{\mathrm{A}}]|0\rangle_{\mathrm{A}_2}|0\rangle_{\mathrm{B}} &\rightarrow [\chi_0|0\rangle_{\mathrm{A}_2}|0\rangle_{\mathrm{A}} + \chi_1|1\rangle_{\mathrm{A}_2}|1\rangle_{\mathrm{A}}]|0\rangle_{\mathrm{B}} \\ &\rightarrow |0\rangle_{\mathrm{A}_2}[\chi_0|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + \chi_1|1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}].\end{aligned} \tag{2.2}$$

Here, the first arrow refers to a *local* C-NOT operation between two atoms A and A_2 in the first cavity. The second arrow transfers the state of A_2 to B, thereby transferring the entanglement between the atoms A and A_2 to an entanglement

between atoms A and B. At the end of this composite transformation, the state of the auxiliary atom A_2 is the same as initially and *factors out*. For $\chi_0 = \chi_1$, an ideal EPR pair is created.

From this simple consideration we conclude that the creation of a distant EPR pair is possible if (1) the local C-NOT operation and (2) the transfer operation (2.1) can be realized without errors, or if these errors can be corrected. Corresponding to these operations, two different kinds of errors need to be corrected: (1) local (gate) errors; (2) transfer errors.

When the photons are sent along optical fibres, then photoabsorption will be a dominant transfer error. Losses may also occur by incoherent scattering on the surface of the cavity mirrors and at the coupling segments between the cavities and the fibres. Another typical transfer error will be caused by imperfectly designed laser pulses for the Raman transition. An example for a local gate error is spontaneous emission in one of the atoms during the gate operation.

In this paper, we will assume that local gate operations can be performed without errors, and concentrate on errors that occur during the photon transfer. A discussion of error correction for two-bit gate operations can be found in van Enk *et al*. (1997*c*).

3. The photonic channel

In a realistic model, we have to consider the possibility that the transfer of the atomic state from cavity A to B is imperfect. There is a certain probability that the atom in B will not be excited, even though A was excited. This is due to the interaction of the compound atom–cavity–fibre system with the environment which, even if small, in principle always exists. This results in an entanglement of the atomic states in (2.1) with the environment, i.e. the cavity walls, the fibre and the radiation field of the free space.

In the following, we assume that photons can be absorbed but not created by the channel. This is a very good approximation for optical photons, where the mean thermal number of photons in the cavities and the fibre is exceedingly small. In this situation, the most general expression for an imperfect transfer operation is of the form

$$\left.\begin{aligned} |0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|E\rangle &\rightarrow |0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|E_0\rangle, \\ |1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|E\rangle &\rightarrow |0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}|E_1\rangle + |0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}|E_a\rangle, \end{aligned}\right\} \tag{3.1}$$

where $|E\rangle, |E_0\rangle, \ldots$ denote unnormalized states of the environment. It is expedient to write $|E_0\rangle = \mathcal{T}_0|E\rangle$, $|E_1\rangle = \mathcal{T}_1|E\rangle$, $|E_a\rangle = \mathcal{T}_a|E\rangle$, thereby introducing operators that entangle the system with the environment. With this notation, (3.1) can be expressed in the compact form†

$$\left.\begin{aligned} |0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} &\rightarrow |0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}\mathcal{T}_0, \\ |1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} &\rightarrow |0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}}\mathcal{T}_1 + |0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}\mathcal{T}_a, \end{aligned}\right\} \tag{3.2}$$

which defines the photonic channel (van Enk *et al*. 1997*b*).

The optical cavities together with the fibre form a compound optical system with a certain resonant structure that defines its spectrum of quasi-modes, its relaxation constants, etc. In the special case when only photoabsorption plays a role,

† In expressions of this type, it is understood that both the left- and the right-hand sides are applied to a given state of the environment. Using this compact notation keeps the expressions much more transparent when twofold or more complex applications of the channel are studied.

the operators in (3.2) have a simple form. For optical frequencies, the state of the environment can be very well approximated by the vacuum state, so one can write $\mathcal{T}_0 = 1$, $\mathcal{T}_1 = \alpha(\tau) \sim \mathrm{e}^{-\kappa\tau}$, $\mathcal{T}_a = \sum_j \beta_j(\tau) b_j^\dagger$, with $\sum_j |\beta_j(\tau)|^2 \sim 1 - \mathrm{e}^{-2\kappa\tau}$ where κ is the damping rate of the total (atom–)cavity–fibre system and τ is the transfer time. The operators $b_j^\dagger$, b_j are amplitude operators of the jth oscillator mode of the environment.

More generally, the operators $\mathcal{T}_{0,1,a}$ in (3.2) may describe spontaneous emission processes, photon absorption, as well as transitions to and repumping from other internal states of the atoms. Thus, all complicated physics is hidden in the three operators. In this general (non-stationary) situation, the time dependence of the environmental terms has to be taken into account. The operators $\mathcal{T}_{0,1,a}$ then depend on the initial time when the transfer starts. As a consequence, when iterating the channel (3.2), the temporal ordering of the operators becomes important, e.g. $\mathcal{T}_1(t_1)\mathcal{T}_0(t_0) \neq \mathcal{T}_0(t_1)\mathcal{T}_1(t_0)$.

When using (3.2) to create an EPR pair as in (2.2), we obtain

$$[\chi_0|0\rangle_\mathrm{A} + \chi_1|1\rangle_\mathrm{A}]|0\rangle_\mathrm{B} \rightarrow [\chi_0|0\rangle_\mathrm{A}|0\rangle_\mathrm{B}\mathcal{T}_0 + \chi_1|1\rangle_\mathrm{A}|1\rangle_\mathrm{B}\mathcal{T}_1] + \chi_1|1\rangle_\mathrm{A}|0\rangle_\mathrm{B}\mathcal{T}_a. \tag{3.3}$$

For $\chi_0 = \chi_1$, this expression can be written in the form†

$$|\Phi^+_\mathrm{AB}\rangle[\mathcal{T}_0 + \mathcal{T}_1] + |\Phi^-_\mathrm{AB}\rangle[\mathcal{T}_0 - \mathcal{T}_1] + (|\Psi^+_\mathrm{AB}\rangle + |\Psi^-_\mathrm{AB}\rangle)\mathcal{T}_a, \tag{3.4}$$

where we use the Bell basis $|\Phi^\pm_\mathrm{AB}\rangle = (1/\sqrt{2})(|0\rangle_\mathrm{A}|0\rangle_\mathrm{B} \pm |1\rangle_\mathrm{A}|1\rangle_\mathrm{B})$ and $|\Psi^\pm_\mathrm{AB}\rangle = (1/\sqrt{2})(|0\rangle_\mathrm{A}|1\rangle_\mathrm{B} \pm |1\rangle_\mathrm{A}|0\rangle_\mathrm{B})$. The fidelity of the resulting pair (3.4) can be defined by its overlap with the ideal result $|\Phi^+_\mathrm{AB}\rangle$. This overlap is given by the norm

$$F = \|\tfrac{1}{2}([\mathcal{T}_0 + \mathcal{T}_1]|E\rangle)\|^2 \sim |\tfrac{1}{2}(1 + \mathrm{e}^{-\kappa\tau})|^2. \tag{3.5}$$

The estimate of F in the second term demonstrates how the coupling of the modes of the cavity–fibre system to the environment reduces the attainable fidelity of the EPR pair. In particular, F decreases exponentially with the transfer time and the corresponding length of the fibre.

In order to create an EPR pair over a distance comparable to or larger than the absorption length of the photonic channel, we need to find a method to *detect and correct* a photon loss that may occur during the transfer. Loosely speaking, we are seeking to eliminate the absorption term $\mathcal{T}_a$ in (3.4), and to minimize the other term $\mathcal{T}_0 - \mathcal{T}_1$.

In the following, we outline a method that uses one (respectively two) auxiliary atoms in each cavity. This outline summarizes just the essential steps. For details, the reader should consult the papers by van Enk *et al.* (1997*a*, *b*) and Cirac *et al.* (1998).

4. Error correction and purification with finite means

The main idea is to entangle the atom in the first cavity with auxiliary (backup) atoms, before transmitting the information. This is reminiscent of a redundant coding scheme, with the fundamental difference being that our scheme allows us to correct errors to *all orders* in the photoabsorption probability. By measuring a certain joint state of two atoms in the receiver cavity, one is able to *detect* a photon loss while

† Throughout this paper, normalization factors are omitted unless they are needed.

maintaining the initial coherence of the atomic state that was sent. Therefore, the transmission can be repeated as often as necessary until no error is detected.

In detail, this requires three steps.

(1) *Encoding* of the atomic state into a three-particle entangled state

$$\chi_0|0\rangle_{\rm A}+\chi_1|1\rangle_{\rm A}\rightarrow\chi_0[|0\rangle_{\rm A}|0\rangle_{{\rm A}_2}|0\rangle_{A_3}+|1\rangle_{\rm A}|1\rangle_{{\rm A}_2}|1\rangle_{A_3}]+\chi_1[|0\rangle_{\rm A}|0\rangle_{{\rm A}_2}|1\rangle_{A_3}+|1\rangle_{\rm A}|1\rangle_{{\rm A}_2}|0\rangle_{A_3}]. \quad (4.1)$$

This can be realized by applying two C-NOT operations between $\rm A_3$ and A, and A and $\rm A_2$, respectively.

(2) *Transmission* of a photon *twice* by using (3.2) between atom $\rm A_2$ and $\rm B_2$ and then between $\rm A_2$ and B, applying a local flip operation on A inbetween. The result of this operation is a multiparticle entangled state (Cirac *et al*. 1998) whose explicit form will not be given here.

(3) *Measuring* the states of certain backup atoms in both cavities. Combined with appropriate local unitary transformations, one obtains one of two results.

The effect of this procedure is summarized in the following *absorption-free channel*:

$$[\chi_0|0\rangle_{\rm A}+\chi_1|1\rangle_{\rm A}]|0\rangle_{\rm B}\rightarrow\chi_0|0\rangle_{\rm A}|0\rangle_{\rm B}\mathcal{S}_0+\chi_1|1\rangle_{\rm A}|1\rangle_{\rm B}\mathcal{S}_1$$
$$\overset{\text{error}}{\searrow}\quad[\chi_0|0\rangle_{\rm A}+\chi_1|1\rangle_{\rm A}]|0\rangle_{\rm B}\mathcal{S}_a. \quad (4.2)$$

Owing to the twofold transmission process, the operators $\mathcal{S}$ appearing in (4.2) are products of the $\mathcal{T}$ operators, e.g. $\mathcal{S}_0=\mathcal{T}_0\mathcal{T}_1$, $\mathcal{S}_1=\mathcal{T}_1\mathcal{T}_0$, or in a different order. The important feature to notice is that, depending on the results of the measurement in step (3), two outcomes are possible: if an error is detected, the state is projected onto the second line of (4.2) and the transmission can be repeated; if no error is detected, the state is projected onto the first line of (4.2), which completes the channel.

By using (4.2) instead of (3.2) one obtains

$$[|0\rangle_{\rm A}+|1\rangle_{\rm A}]|0\rangle_{\rm B}\rightarrow|0\rangle_{\rm A}|0\rangle_{\rm B}\mathcal{S}_0+|1\rangle_{\rm A}|1\rangle_{\rm B}\mathcal{S}_1$$
$$=|\Phi^+_{\rm AB}\rangle\tfrac{1}{2}[\mathcal{S}_0+\mathcal{S}_1]+|\Phi^-_{\rm AB}\rangle\tfrac{1}{2}[\mathcal{S}_0-\mathcal{S}_1]. \quad (4.3)$$

For the simple example considered after (3.2), with $\mathcal{T}_0=1$ and $\mathcal{T}_1=\mathrm{e}^{-\kappa\tau}$, we have $\mathcal{S}_0=\mathrm{e}^{-\kappa\tau}$ and $\mathcal{S}_1=\mathrm{e}^{-\kappa\tau}$; thus the second term in (4.3) vanishes. In this situation, an ideal EPR pair is established after a *single* use of the channel (4.2). This corresponds to an average number of phototransmissions of $\mathrm{e}^{2\kappa\tau}$.

More generally, a similar result is obtained when the state of the environment does not depend on the temporal ordering of the operators $\mathcal{T}_0$ and $\mathcal{T}_1$. Such a *stationary environment* is defined by $\mathcal{T}_1(t_1)\mathcal{T}_0(t_0)|E\rangle=\mathcal{T}_0(t_1)\mathcal{T}_1(t_0)|E\rangle$, i.e. $\mathcal{S}_0|E\rangle=\mathcal{S}_1|E\rangle$. For any system with a stationary environment, an ideal EPR pair is created by a single application of (4.2).

For the discussion of the general non-stationary case, let us first rewrite the result (4.3) in the form

$$|\Psi^{(1)}\rangle=|\Phi^+_{\rm AB}\rangle|E^{(1)}_+\rangle+|\Phi^-_{\rm AB}\rangle|E^{(1)}_-\rangle, \quad (4.4)$$

where $|E^{(1)}_\pm\rangle=\frac{1}{2}(\mathcal{S}_0\pm\mathcal{S}_1)|E\rangle$. The norm (square) of the environment $|E^{(1)}_+\rangle$ determines the fidelity of the pair.

At this point, the key advantage of the absorption-free channel (AFC) comes into play, namely that it corrects errors in the transmission process while maintaining

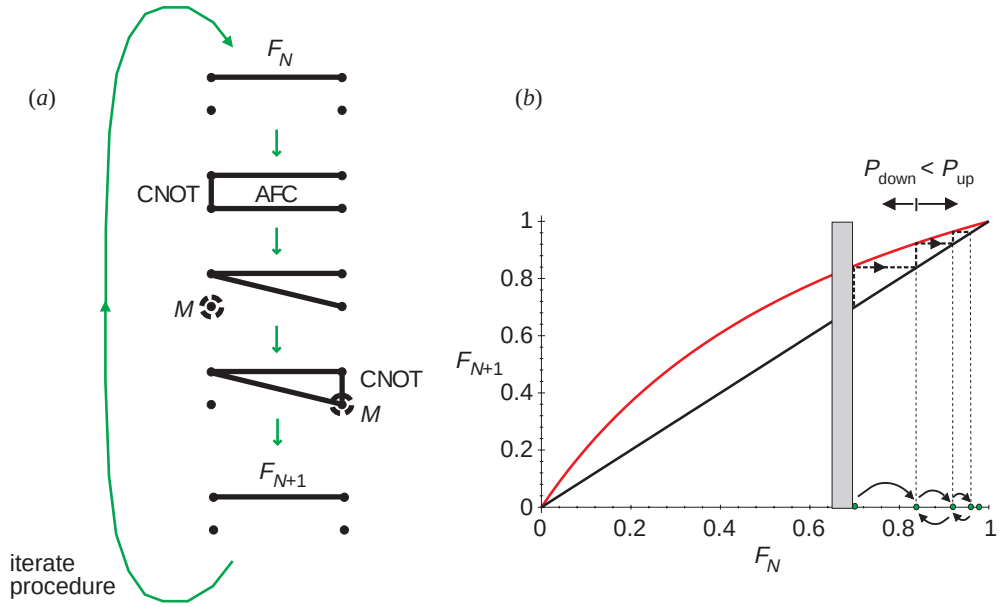

Figure 2. Purification of an EPR pair with finite means. (*a*) Iterative purification protocol. At each purification step, an EPR pair of the form (4.5) with fidelity F_N is temporarily entangled with two auxiliary atoms. This involves two C-NOT operations, the absorption-free channel (AFC) and measurements M. Furthermore, there are some Hadamard transformations that are not shown in the figure. The value of the new fidelity F_{N+1} depends on the result of the measurements M. Note that this scheme operates on the *same set of atoms* at each step, thereby realizing a 'self-purification process'. (*b*) One-sided random-walk process for fidelity. After each iteration step in (*a*), the fidelity F_N increases (decreases) with a certain probability $P_{\rm up}$ ($P_{\rm down}$) that depends on N. If F_N happens to drop below the initial value F_0, we reset the pair to this value by a single use of the AFC, as in (4.3). This is equivalent to a one-sided random walk process with reflections at a lower barrier at F_0, as indicated in the figure. On average, the fidelity thereby approaches unity exponentially fast, $F_N \sim 1 - \mathrm{e}^{-\mathrm{const.}\times N}$.

the coherence and possible entanglement of the state it is applied to. This allows for an iterative purification protocol (van Enk *et al.* 1997*b*). At each purification step, the pair is temporarily entangled with two auxiliary atoms, one at each node, using both local C-NOT operations and the AFC. In some sense, this creates an auxiliary EPR pair that is used to purify (4.4). The detailed protocol is shown schematically in figure 2*a*.

This protocol transforms (4.4) into a sequence of states of the form,

$$|\Psi^{(N)}\rangle = |\Phi^{+}_{\rm AB}\rangle|E^{(N)}_{+}\rangle + |\Phi^{-}_{\rm AB}\rangle|E^{(N)}_{-}\rangle, \tag{4.5}$$

where either

$$|E^{(N)}_{\pm}\rangle = \tfrac{1}{2}(\mathcal{S}_0 \pm \mathcal{S}_1)|E^{(N-1)}_{\pm}\rangle \quad \text{or} \quad |E^{(N)}_{\pm}\rangle = \tfrac{1}{2}(\mathcal{S}_0 \mp \mathcal{S}_1)|E^{(N-1)}_{\pm}\rangle,$$

depending on the result of the measurement. In the first case, which happens with probability $P_{\rm up} = P^{(N)}_{\rm up}$, the fidelity of the pair increases. In the second case, which happens with $P_{\rm down} = 1 - P_{\rm up}$, the fidelity decreases. One can show that this creates a stochastic process corresponding to a one-sided random-walk process as depicted

in figure 2*b*. On average, the fidelity $F_N = \langle E_+^{(N)} | E_+^{(N)} \rangle$ thereby converges towards unity exponentially fast with the number of purification steps.

It is quite remarkable that this describes a finite system that iteratively purifies itself. We note that standard purification protocols (Bennett *et al*. 1996; Deutsch *et al*. 1996; Gisin 1996) assume a large number of EPR pairs which need to be coherently manipulated (connected). In contrast, the present scheme uses iterated operations on *few* atoms.

5. Communication over long distances

With the methods discussed in the previous sections, it is possible to create an EPR pair of high fidelity by sending single photons through a dissipative and noisy channel that connects the atoms.

There is, however, a limitation to the method when the transmission time through the channel becomes much larger than its relaxation time, i.e. if $\kappa\tau \gg 1$. As the absorption probability grows exponentially with τ, so will the required number of repetitions for one successful transmission. We have to keep in mind that in the implementation of the AFC (4.2), we have assumed that all local operations are error free. In reality, these operations will never be perfect, but there will be small probabilities for failure. As the number of required transmissions increases, the error probabilites will eventually add up and spoil the coherence-preserving action of the AFC.

Absorption losses are well known in problems of electric signal transmission through classical channels where, at regularly spaced intervals, amplifiers are put in the channel. In the classical (digital) communication technique such amplifiers are not only used to amplify but also to restore the signal. The distance between the amplifiers is then determined by (1) the damping rate of the fibre and (2) the bit rate of the transmission (dispersion effects). In the classical case, dispersion effects are more important whereas in the quantum case, when we send *single photons*, damping will be the main problem.

In order to build up the EPR correlations, single qubits (photons) need to be transmitted which cannot be amplified (Wootters & Zurek 1982; Glauber 1986). All we can do here is to detect whether a photon has been absorbed and, whenever that is the case, repeat the transmission.

For any practical implementation of the scheme, it is crucial to know how the number of operations scales with the length of the channel, i.e. the distance between the atoms. For the following discussion, let us assume that the dominant transmission error is given by photoabsorption. This corresponds to a photonic channel (3.2) with $\mathcal{T}_0 = 1$ and $\mathcal{T}_1 = \mathrm{e}^{-\kappa\tau} = \mathrm{e}^{-l/2l_0}$ where $l_0 = c/2\kappa$ defines the half-length of the fibre. The probability for a successful transmission from A to B, as indicated in figure 3*a*, is then $p(l) = \mathrm{e}^{-l/l_0}$ where l is the length of the fibre. Correspondingly, the average number of required repetitions is

$$n(l) = 1/p(l) = \mathrm{e}^{l/l_0}. \tag{5.1}$$

It is clear that this leads to unrealistically high numbers for any experiment, if the fibre is much longer than a few half lengths l_0.

In figure 3*b*, this situation is compared with a compound fibre, consisting of a sequence of N segments of length l/N each. At the end of every segment, there is

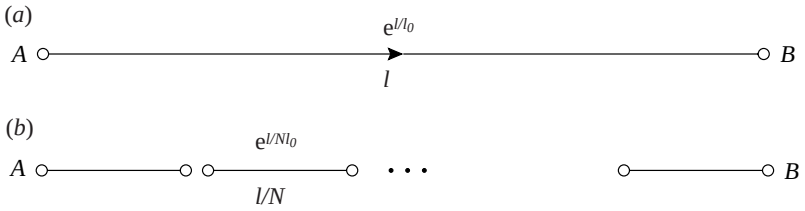

Figure 3. Simple (*a*) and compound (*b*) fibre for transmission of single photons from A to B. As with classical amplifiers, to transmit single photons reliable over long distances, the fibre has to be divided into several segments, at the end of which transmission errors are measured.

a 'checkpoint' at which it is measured whether a transmission error has occurred. This can be done with the method explained in § 4 by using a few ions in a cavity. If an absorption error is detected, the transmission across that segment is repeated. Then a photon is sent through the subsequent segment, and so on. The average total number of repetitions on each segment is $n(l/N) = \mathrm{e}^{l/l_0 N}$. Correspondingly, the total number of transmissions required for successfully sending the photon across the *compound fibre* is

$$n_{\mathrm{com}} = \frac{N}{p(l/N)} = N\mathrm{e}^{l/Nl_0}. \tag{5.2}$$

This is to be compared with (5.1). The compound fibre is preferable to the simple fibre if

$$N\mathrm{e}^{l/Nl_0} < \mathrm{e}^{l/l_0}. \tag{5.3}$$

The optimum number of segments is given by the value of N that minimizes the left-hand side of equation (5.3), which is $N_{\mathrm{min}} = l/l_0$.

The minimum number of transmissions along the compound fibre is thus given by (5.2) with $N = N_{\mathrm{min}}$, that is

$$n_{\mathrm{min}} = N_{\mathrm{min}}\mathrm{e}^{l/N_{\mathrm{min}}l_0} = l/l_0\mathrm{e}^1. \tag{5.4}$$

This optimum situation is realized if the checkpoints are placed along the fibre with a spacing corresponding to the half length l_0.

Example. The fibre used in the recent cryptographic experiments by the Geneva group (Zbinden *et al.* 1997; Tittel *et al.* 1998) has a half length l_0 of the order of 10 km. Using such a fibre for establishing an EPR pair between Innsbruck and Oxford, say, ($l \sim 1000\,\mathrm{km} = 100l_0$) requires $100\mathrm{e} = 272$ transmissions if one uses a compound fibre with 100 checkpoints. For a simple fibre, with no checkpoint, this average number is as high as $\mathrm{e}^{100} = 2.69\times10^{43}$! For one transmission per microsecond, the total time needed in the first case would be of the order of 1 ms; in the latter case it would be larger than the age of the universe.

So far we have only talked about 'successfully sending a photon across the fibre'. What we really have in mind, however, is not to directly send arbitrary states of photons, but to establish an EPR pair between distant atoms A and B with the aid of this fibre. Although these two problems are closely related, there is an important difference. To build up the EPR correlations, we need only to send very specific states of photons, namely, according to (4.3), those which correspond to the atomic state

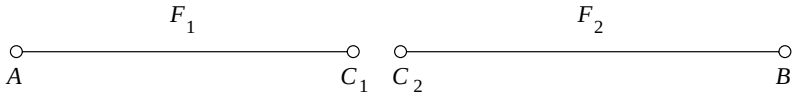

Figure 4. Connection of two EPR pairs A ↔ C_1 and C_2 ↔ B with fidelity F_1 and F_2, respectively, at checkpoint C. This creates a new pair A ↔ B between A and B with fidelity $F \leqslant \min\{F_1, F_2\}$.

$(|0\rangle + |1\rangle)/\sqrt{2}$. This has the advantage that we do not need to trace the evolution of some arbitrary qubit throughout the channel, including the checkpoints, simply because there is no information processing. The channel may be used for quantum communication *after* we have established the EPR correlations between A and B but, at that stage, the state of the channel is irrelevant (the fibre need no longer exist).

The problem we are dealing with can be rephrased in more general terms, without referring to a particular physical realization of the channel. For this, we divide the problem into two steps. To create an EPR pair over a noisy channel of length l, which is composed of N segments of length l/N, we (1) establish N (short-distance) EPR pairs, one pair across every segment, and (2) connect the EPR pairs by making Bell measurements at each checkpoint, followed by classical communication between the checkpoints. As a result, a (long-distance) EPR pair is created between the outermost atoms.

For a compound fibre consisting of just two segments, this scheme is shown in figure 4. The connection process, i.e. step (2), is equivalent to a teleportation of the state of particle C_1, which is entangled with particle A, to B.

To study the connection process in more detail, let us go back and relax our previous assumption that only absorption errors occur, while maintaining the assumption that local two-bit operations can be performed without error. For example, suppose the timing of the Raman pulses at the beginning and at the end of the transmission is not perfect. In this case, on each segment an EPR pair of the form (4.5) is created as the result of an N-step process, with a fidelity $F_N = \langle E_+^{(N)} | E_+^{(N)} \rangle$ that may be high but is not equal to unity†.

When connecting two EPR pairs of the form (4.5), with fidelity $F_1 = F_{N_1}$ and $F_2 = F_{N_2}$, respectively, as depicted in figure 4, the resulting pair has a fidelity that is smaller than F_1 and F_2. A brief calculation shows that the fidelity F of the new pair satisfies

$$2F - 1 = (2F_1 - 1)(2F_2 - 1). \tag{5.5}$$

Upon connecting N pairs of fidelity F_0, we obtain one distant pair of fidelity

$$F = \tfrac{1}{2}\{1 + (2F_0 - 1)^N\}, \tag{5.6}$$

which can be seen by iterating (5.5) N times. Note that the connecting need not be done sequentially, i.e. first at checkpoint one, then at two, and so on. A faster (or rather the fastest) way to do this would be in step 1 to simultaneously connect the pairs at every second checkpoint, which leaves one with $\frac{1}{2}N$ pairs of fidelity $F_1 = \frac{1}{2}\{1 + (2F_0 - 1)^2\}$. In step 2 the remaining pairs are again connected at every second checkpoint, which results in $\frac{1}{4}N$ pairs with fidelity $F_2 = \frac{1}{2}\{1 + (2F_0 - 1)^4\}$.

† The actual value of F_N will be determined by the maximum number of purification steps one is willing to apply, or by the limitation inherent in the implementation of the AFC, due to imperfections of the local operations in step (1) that leads to (4.1).

If $N = 2^n$, then the final EPR pair with fidelity (5.6) is obtained by iteration after a total of $n = \log_2 N$ steps.

The lesson to be learned from (5.6) is the following. The fidelity decreases exponentially with the number of segments unless the initial fidelity F_0 on every segment is unity. By dividing the fibre into shorter segments, we have thus eliminated the effect of exponentially increasing transmission losses while, at the same time, introducing an exponential decrease in the fidelity.

The drawback of the second effect, however, does not completely ruin the gain from the first effect. Since the purification protocol described by the sequence (4.5) converges towards unit fidelity exponentially fast, one can compensate for the exponential decrease of F in (5.6) by starting from a higher initial value F_0. This requires only a few extra purification steps on each segment, before they are connected. There is a limit to this, which is given by the maximum fidelity attainable on each segment. Furthermore, the connection process itself will in general be imperfect. Even if we started from N EPR pairs of unity fidelity, any imperfection in the connection operation would decrease the fidelity of the connected pair, and therefore the fidelity of the connection operation would enter exponentially and reduce the final fidelity.

In summary, any imperfections in local operations (i.e. two-bit, one-bit and measurements) result in a fidelity that decreases exponentially with the length of the channel. Conversely, the number of operations required to produce an EPR pair of a given fidelity increases exponentially with the distance of the particles. This poses a severe limitation on any distant quantum communication.

We just report here that there is a way around this exponential scaling property by using a purification protocol which re-purifies the obtained EPR pairs after a number of connecting steps (Cirac *et al*. 1998). The idea of the procedure is similar to what has been called a 'concatenated quantum code' by Knill & Laflamme (1996) in the context of fault-tolerant quantum computing. However, the problem of creating an EPR pair via a noisy channel—consisting of a sequence of imperfect gate operations and transfer operations—is different from fault-tolerant quantum computation. The crucial difference is that we are not, in the first place, sending an arbitrary qubit through the channel. In other words, *while creating the EPR correlations, there is no quantum information being processed*, although the EPR pair may subsequently be used for communication via teleportation.

As a result, we obtain fidelity requirements on the local operations which are in the region of a few per cent. This should be compared with the number of 10^{-5} (Knill & Laflamme 1996) for fault-tolerant quantum computing.

6. Conclusion

We have outlined a procedure for creating maximally entangled pairs of atoms which are connected by a noisy quantum channel. The essential features of this procedure are (1) the usage of *finite means*, i.e. a few ions in two resonators; (2) the implementation of an *absorption-free channel* that is used for non-local entanglement operations between ions in different resonators; and (3) a *concatenated purification* algorithm that allows for communication beyond a certain distance that, in usual approaches, is imposed by the exponential transmission losses.

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

References

Bennett, C. H., Brassard, G., Crepeau, C., Josza, R., Peres, A. & Wootters, W. K. 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899.

Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A. & Wootters, W. K. 1996 Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725.

Boschi, D., Branca, S., De Martini, F., Hardy, L. & Popescu, S. 1998 Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Phys. Rev. Lett.* **80**, 1121–1125.

Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H. & Zeilinger, A. 1997 Experimental quantum teleportation. *Nature* **390**, 575–579.

Bruss, D., DiVincenzo, D. P., Ekert, A., Fuchs, C. A., Macchiavello, C. & Smolin, J. A. 1997 Optimal universal and state-dependent quantum cloning. *Phys. Rev.* A **57**, 2368.

Cirac, J. I., Zoller, P., Kimble, H. J. & Mabuchi, H. 1997 Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Phys. Rev. Lett.* **78**, 3221–3224.

Cirac, J. I., van Enk, S. J., Zoller, P., Kimble, H. J. & Mabuchi, H. 1998 Quantum communication in a quantum network. In *Proc. of the Nobel Symposium 104, 13–17 June 1997. Physica Scr.* (In the press.)

Deutsch D., Ekert, A., Josza, R., Macchiavello C., Popescu S. & Sanpera, A. 1996 Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818–2821.

Einstein, A., Podolsky, B. & Rosen, N. 1935 Can quantum mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780.

Ekert, A. K. 1991 Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **70**, 661–663.

Gisin, N. 1996 Hidden quantum locality revealed by local filters. *Phys. Lett.* A **210** 151–156.

Gisin, N. & Massar, S. 1997 Optimal quantum cloning machines. *Phys. Rev. Lett.* **97**, 2153–2156.

Glauber, R. J. 1986 In *Frontiers in quantum optics* (ed. E. R. Pike & S. Sarkar), pp. 534–582. Bristol: Adam Hilger.

Grover, L. K. 1997 Quantum telecomputation. quant-ph/9704012.

Hagley E., Maitre, X., Nogues, G., Wunderlich, C., Brune, M., Raimond, J. M. & Haroche, S. 1997 Generation of Einstein–Podolsky–Rosen pairs of atoms. *Phys. Rev. Lett.* **79**, 1–5.

Karlson, E. (ed.) 1998 *Proc. of the Nobel Symposium 104, 13–17 June 1997. Physica Scr.* (In the press.)

Knill, E. & Laflamme, R. 1996 Concatenated quantum codes. quant-ph/9608012.

Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. & Wineland, D. J. 1995 Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.* **75**, 4714–4717.

Tittel, W., Brendel, J., Gisin, B., Herzog, T., Zbinden, H. & Gisin, N. 1998 Experimental demonstration of quantum-correlations over more than 10 km. *Phys. Rev.* A **57**, 3229.

Turchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H. & Kimble, H. J. 1995 Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.* **75**, 4710–4713.

van Enk, S. J., Cirac, J. I. & Zoller, P. 1997*a* Ideal communication over noisy channels: a quantum optical implementation. *Phys. Rev. Lett.* **78**, 4293–4296.

van Enk, S. J., Cirac, J. I. & Zoller, P. 1997*b* Photonic channels for quantum communication. *Science* **279**, 205–209.

van Enk, S. J., Cirac, J. I. & Zoller, P. 1997*c* Purifying two-bit quantum gates and joint measurements in cavity QED. *Phys. Rev. Lett.* **79**, 5178–5181.

Wootters, W. K. & Zurek, W. H. 1982 A single quantum cannot be cloned. *Nature* **299**, 802–803.

Zbinden, H., Gautier, J. D., Gisin, N., Huttner, B., Muller, A. & Tittel, W. 1997 Interferometry with Faraday mirrors for quantum cryptography. quant-9703024.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES