LONG DISTANCE QUANTUM COMMUNICATION USING QUANTUM ERROR CORRECTION

ROBERT M. GINGRICH, HWANG LEE, AND JONATHAN P. DOWLING

Exploration Systems Autonomy, Section 367, MS 126-347
Quantum Computing Technologies Group
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Drive, Pasadena, CA 91109-8099

Currently long distance quantum communication is limited by the photon loss. We describe a quantum error correction scheme that can increase the *effective* absorption length of the communication channel. This device can play the role of a quantum transponder when placed in series, or a cyclic quantum memory when inserted in an optical loop.

When we send a photon through an optical fiber of length d, the probability of successfully transmitting the photon is given by

$$p(d) = \exp(-\alpha d) \ . \tag{1}$$

Here, the absorption coefficient of the fiber is given by α, which is a property of the fiber. The best fibers have an absorption length, $1/\alpha$, of about 30 km. While there can be errors caused by dephasing, the photon losses restricts the distance of the secure channel for quantum information transmission. A quantum repeater has been devised to overcome such a limit[1]. It utilizes entanglement purification and swapping to distribute quantum entanglement between the two distant parties[2,3,4]. For some schemes such as BB84[5], however, the distribution of entanglement is not need. Instead, one can increase the effective absorption length by repeated applying a quantum error-correction (QEC) code that recovers photon loss.

It is known that an arbitrary error at unknown position in the code word can be corrected by a five-qubit encoding. When the position of the error is known, so-called quantum erasure channel, an arbitrary error can be recovered by a four-qubit encoding[6]. Moreover, for an error being occurred in only one position one can encode two qubits into four. The two-to-four–qubit encoding is given by

$$\begin{aligned} |00\rangle &\mapsto (|0000\rangle + |1111\rangle)/\sqrt{2} \ , \\ |01\rangle &\mapsto (|0110\rangle + |1001\rangle)/\sqrt{2} \ , \\ |10\rangle &\mapsto (|1010\rangle + |0101\rangle)/\sqrt{2} \ , \\ |11\rangle &\mapsto (|1100\rangle + |0011\rangle)/\sqrt{2} \ . \end{aligned} \tag{2}$$

A simple quantum circuit for implementation of the encoding is depicted in Fig. 1.

Suppose now we have encoded two photons into four. In order to have any benefit from the error correction, we need to have $p_{en} > p^2$, where p_{en}

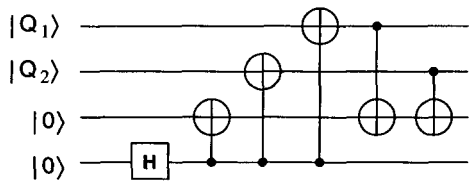

Figure 1. A quantum circuit for the two-to-four qubit encoding, which converts the input $|Q_1, Q_2\rangle$ into a four-qubit state, as is given in Eq. (2).

is the probability of success in transmission of four photons with at most one photon loss, given by $p_{en} = p^4 + 4p^3(1-p)$. This leads to a necessary condition $p > 1/3$ for the error correction doing any good. We may look at this in terms of an *effective* absorption length. Using p_{en} and inverting equation (1) we have an effective absorption length, $1/\beta$, for the QEC as

$$\begin{aligned} \beta(\alpha, d) &= -\ln(p_{en})/d \\ &= 3\alpha - \ln(4 - 3\exp(-\alpha d))/d \,. \end{aligned} \tag{3}$$

Since our QEC encodes two qubits, we compare β with 2α, to see if our code is improving the situation or not. Define the function $f(x)$ with $x \equiv \alpha d$, such that

$$\frac{\beta}{2\alpha} = \frac{3}{2} - \frac{\ln(4 - 3\exp(-x))}{2x} \equiv f(x) \,. \tag{4}$$

When $x < \ln(3) \approx 1.1$, $f(x) < 1$, our QEC is increasing the effective absorption length for the qubits we are trying to transmit. So, if we make $d < \ln(3)/\alpha$ the ECC allows us to transmit qubits with higher fidelity than is possible without it. Note that $\lim_{x\to 0} f(x) = 0$, so the absorption length can be made arbitrarily large by making d smaller. However, by decreasing d we need to introduce more gates, and the gates introduce errors.

In order to have the QEC work we need to know the position of the error, the photon loss in this case. Therefore the ability to check the absence of the photons in all four channels are necessary for the QEC. This requires a single-photon quantum nondemolition (QND) measurement.[7] Now if we only consider only one photon or none in a single quantum channel, the protocol of quantum teleportation acts as the single-photon QND device (see Fig.2). If we include the possibility that two photons are present in a channel, the teleportation does not work for single-photon QND.[8]

When single photons are present in all four channels, we can skip the correction process. Once the absence of the photon is found in one channel, a single photon is added in that channel. Whatever the quantum state of the single photon that is added, the correction process then will fix the error, since the QEC is for an arbitrary error.

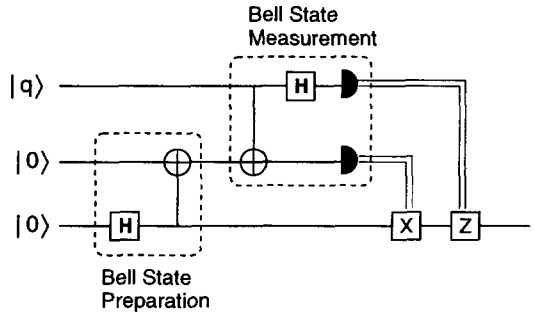

Figure 2. Single-photon quantum nondemolition measurement based on quantum teleportation. It works only if we can neglect the possibility of having two or more photons in the quantum channel. The initial Bell state is prepared by the two ancilla photons (Hadamard gate followed by a CNOT gate). The result of the Bell measurement determines the one-qubit gate on the other ancillar photon ($X, Z \equiv \sigma_x, \sigma_z$), which completes the teleportation. The absence of the photon in the qubit mode can be revealed at this measurement stage.

Including the single-photon QND, the quantum circuit for the correction process is depicted in Fig. 3. Let us consider a two-qubit input state, for example, $|\psi_{in}\rangle = |01\rangle$. The codeword is then $|\psi_{en}\rangle = \frac{1}{\sqrt{2}}(|0110\rangle + |1001\rangle)$. Suppose now that the last qubit is lost. The state of the system is given by the following density operator $\rho_1 = \frac{1}{2}(|011\rangle\langle 011| + |100\rangle\langle 100|)$, which is obtained from the initial state $|\psi_{en}\rangle$ by tracing-out the last qubit. For the sake of simplicity, let us consider the mixed state ρ_1 represented as a probability distribution over the pure states, instead of a density matrix. Thus the mixed state after the photon loss can be written as

$$\rho_1 = \{(|011\rangle, \tfrac{1}{2}), (|100\rangle, \tfrac{1}{2})\}. \tag{5}$$

The quantum nondemolition (QND) device that signals the loss of the last qubit is followed by a qubit state preparation device (a single-photon gun) that substitutes the missing qubit with a new qubit in the ground state $|0\rangle$. The new density operator is then:

$$\rho_2 = \{(|0110\rangle, \tfrac{1}{2}), (|1000\rangle, \tfrac{1}{2})\}. \tag{6}$$

Including the two ancilla bits, the total system is in the mixed state

$$\rho_3 = \rho_2 \otimes |00\rangle\langle 00| = \{(|0110\rangle|00\rangle, \tfrac{1}{2}), (|1000\rangle|00\rangle, \tfrac{1}{2})\}. \tag{7}$$

After applying the Hadamard transform on the ancilla bits, this becomes

$$\begin{aligned}\rho_4 = \big\{&\big(\tfrac{1}{2}|0110\rangle[|00\rangle + |01\rangle + |10\rangle + |11\rangle], \tfrac{1}{2}\big),\\ &\big(\tfrac{1}{2}|1000\rangle[|00\rangle + |01\rangle + |10\rangle + |11\rangle], \tfrac{1}{2}\big)\big\}.\end{aligned} \tag{8}$$

The four controlled-σ_x (CNOT) and controlled-σ_z (CZ) operations, followed by the Hadamard transform on the ancilla bits, then yields the mixed

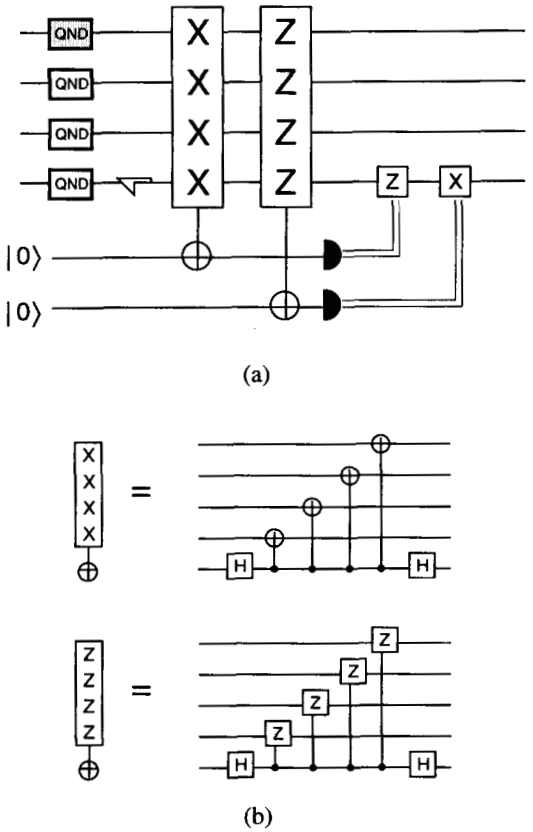

Figure 3. Quantum circuit for the error correction that recovers photon loss using two ancilla photons. (a) We assume that, for example, the loss occurred in the lower-most qubit. The QND box represents a single-photon quantum nondemolition measurement device, followed by a single-photon source. Since the code can correct an arbitrary error, the single photon from the source can be any certain qubit state. $X, Z \equiv \sigma_x, \sigma_z$, and H represents the Hadamard gate. The final one-qubit operations are for the channel where the loss has occurred, and depends on the measurement results. (b) Four CNOT (controlled by the first ancilla) and four C-σ_z (controlled by the second ancilla) gates are followed by another Hadamard gate and measurement on the computational basis for each ancilla.

state as

$$\rho_5 = \{ (\tfrac{1}{2}[(|0110\rangle + |1001\rangle)\,|00\rangle + (|0110\rangle - |1001\rangle)\,|10\rangle\,), \tfrac{1}{2}], \\ (\tfrac{1}{2}[(|1000\rangle + |0111\rangle)\,|01\rangle + (|1000\rangle - |0111\rangle)\,|11\rangle\,], \tfrac{1}{2})\}. \qquad (9)$$

The measurement outcome of the two ancillæ now determines the error-correcting operator on the last qubit. Note that the after the measurement

of the ancilla photons, the result is always a pure state. Furthermore, all the results are equally likely, so this process does not reveal any information about the original encoded state.

We have assumed so far that all the logic gates involved in the error correction are perfect. Obviously, when these gate operations are imperfect, the effective absorption length is degraded. In linear optical quantum computing the two-qubit gates are intrinsically imperfect since they are nondeterministic[9,10]. The probability of success for the non-deterministic two-qubit gate (CZ gate) introduced by Knill, Laflamme, and Milburn, for example, is given by $n^2/(n+1)^2$, where n is the number of ancilla photons. Of course, the intrinsic imperfection of the gate operation can be made small as possible as we increase the number of ancillar photons. However, it requires increased number of photodetectors and the finite quantum efficiency of the photodetectors again degrades the quality of the QEC. In our recent work, we have analyzed the optimal number of anillar photons to maximize the effective absorption length of the quantum channel.[11]

This quantum error-correction scheme for photon loss can provide a cyclic quantum memory when inserted in a delay-line loop. Recently, Pittman and Franson developed a cyclic quantum memory device for photons using a Sagnac interferometer. This device can fix the error caused by the dephasing, but the photon loss in the optical fiber still limits the storage time.

To summarize, a quantum repeater is a device to achieving remote, shared, entanglement by using quantum purification and swapping protocols. Our scheme, on the other hand, utilizes quantum error correction to relay an unknown quantum state with high fidelity down a quantum channel, and can be named as a "quantum transponder" or a quantum relay[12]. For quantum key distribution schemes such as BB84, only a transponder is required for long-distance key transfer. Furthermore, if the fidelity of the transponder is sufficiently high, one can also use it to distribute entanglement by relaying, say, one half of an entangled pair.

Acknowledgments

This work was carried out by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. We wish to thank J. D. Franson, G. J. Milburn, T. C. Ralph, and C. P. Williams, for stimulating discussions. We would like to acknowledge support from the ONR, ARDA, NSA, and DARPA. R.M.G. would also like to acknowledge the National Research Council.

References

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

2. J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger Nature, **410**, 1067 (2001).
3. L.-M. Duan, M.D. Lukin, J.I. Cirac, and P. Zoller, Nature, **414**, 413 (2001).
4. P. Kok, C.P. Williams, and J.P. Dowling, Phys. Rev. A **68**, 022301 (2003).
5. C.H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, 175 (IEEE, New York, NY, 1984).
6. M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
7. G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J.M. Raimond, and S. Haroche, Nature **400**, 239 (1999).
8. P. Kok, H. Lee, and J.P. Dowling, Phys. Rev. A **66**, 063814 (2002).
9. E. Knill, R. Laflamme, and G.J. Milburn, Nature, **409**, 46 (2001).
10. J.D. Franson, M.M. Donegan, M.J. Fitch, B.C. Jacobs, and T.B. Pittman, Phys. Rev. Lett. **89**, 137901 (2002).
11. R.M. Gingrich, P. Kok, H. Lee, F. Vatan, and J.P. Dowling, quant-ph/0306098.
12. B.C. Jacobs, T.B. Pittman, and J.D. Franson, Phys. Rev. A **66**, 052307 (2002).