Solutions for Redundancy-Free Error Correction in Quantum Channel

Laszlo Bacsardi, Laszlo Gyongyosi, and Sandor Imre

Department of Telecommunications, Budapest University of Technology and Economics,
Magyar tudosok krt. 2., H-1111 Budapest, Hungary
{bacsardi,gyongyosi,imre}@hit.bme.hu

Abstract. All free-space quantum communications require the use of a quantum channel, which transports quantum bits in such a way that the quantum mechanical states of the qubits remain preserved from one end of the channel to the other one. In quantum computing the classical error coding methods could not be used, however we can construct a classical channel with zero redundancy error correction for any unitary channel. In our basically new quantum error correction approach, the classical states are coded into the eigenvectors and unitary transformations. In this paper, we show that with our new algorithm it's possible to create redundancy-free quantum error correction. We also consider the redundancy-free implementation of a unitary error correcting operator. Our protocol achieves the redundancy-free quantum communication using local unitary operations and unitary matrices. These solutions could be useful for the free-space quantum communication.

Keywords: Quantum channel, error correction, redundancy-free.

1 Introduction

Quantum theory takes advantage of quantum mechanical principles such as the *superposition* of states and their *no-cloning* principle. Cryptography based on quantum theory principles is known as *quantum cryptography*. In the past few years, quantum key distribution systems have been undertaken a deep study. Because classical cryptographic methods in wired and *wireless security* have been found to have vulnerabilities, new methods based on *quantum mechanical* principles have been deployed.

The first protocol in *quantum cryptography* was the BB84, which however did not take advantage of the full potential of multiple superposition states. The free-space Quantum Key Distribution (QKD) [1] was first introduced over an optical path of about 30 cm in 1991. Several demonstrations increased the usability of QKD by extending it with line-of-site laser communications systems. In 1998, a research group at Los Alamos National Laboratory, New Mexico, USA developed a free-space QKD over outdoor optical paths for up to 950 m under nighttime conditions [2]. Four years later, in 2002 the researchers of the same laboratory have demonstrated that free-space QKD is possible in daylight or at night [3]. In 2006, the distance of 144 km was reached by an international research group [4]. The actual implementation of quantum cryptography

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 117–124, 2010.

systems would be invaluable, allowing for the first time the practical possibility of one-time-pad-encrypted, undecipherable communication, which will offer an essentially new degree of security in future communications.

Long distance quantum communication technologies and other quantum devices in the future will far exceed the processing capabilities of current silicon-based devices. In current network technology, in order to spread *quantum cryptography*, interfaces able to manage together the quantum and classical channel must be implemented.

In our point of view, the quantum computing algorithms can be used to affirm our free-space communication in the following four ways: [5]

1. *Open-air communication*: usually "horizontal" telecommunication that happens below 100km height. For channel, the air is used instead of optical cable.
2. *Earth-satellite communications*: it happens through greater heights than the Open-air communication, usually between 300 and 800 km altitude. Signal encoding and decoding is used to produce quantum error correction that allows operation in noisy environment.
3. *Satellite broadcast*: Quantum algorithms can improve the effective bandwidth, thus the brand is better utilized as in traditional cases.
4. *Inter-satellite communication*: the communication between satellites where the channel is the free-space. Any kind of coding and encoding can be used, to increase stability [6].

Despite the fine number of results a lot of work has to be done. The existing experiments usually use one of the easiest key distribution protocols. There is a need to trace some adoptable algorithms and apply them to communication problems between Earth and satellite and also between satellites. For this, a well-described channel model should be set up. Correct parameters to describe the noise of the different types of atmosphere should be found. As the quantum channels show few similarities with the classical ones describing those require more sophisticated approaches.

2 General Quantum Channel

A quantum bit, or a qubit is a quantum system used to store information. As opposed to a bit which can be in one of two states "0" and "1", a qubit can exist in a *continuum* of states. Moreover, we can measure the value of a bit with certainty without affecting its state, while the result of measuring a qubit is non-deterministic and the measurement alters its state. Computer and communication systems using quantum effects have remarkable properties. Quantum algorithms allow efficient factoring of large integers with applications to cryptography.

Using quantum channels, the information carrying quantum system is in interaction with the environment as an undesirable noise. This phenomena is named quantum decoherence [1]. The noise appearing from the entanglement with the environment can be observed in Figure 1.

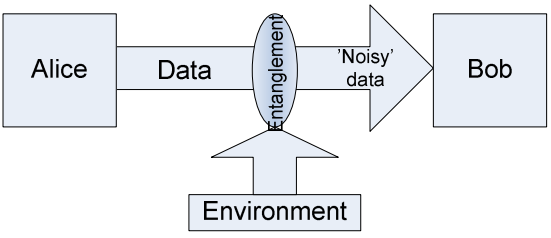

Fig. 1. General model of the quantum channel

For a well functioning communication we need a channel coding to handle the errors appearing in a communication channel. In quantum computing the classical error coding methods could not be used because of the following three reasons [7]:

1. *The errors are continuous*. The errors can results either amplitude or phase decoherence. Moreover both errors have complex coefficients which mean that their codomains are continuous.
2. *Through the No Cloning Theorem* (cloning is allowed only for the classical states e.g., 0 or 1) a simple copy-based redundancy is unadmittable.
3. There are "problems" with the *measurement* of the transmitted states. For the error correction the type of error has to be known but if the quantum bits are measured for determination of the failure then the original bits are lost.

Despite these challenges, several quantum based error correction have been published but they are based on quantum and not classical theorems [8]. In this paper we present a new redundancy-free solutions.

3 Redundancy-Free Channel

The base of our redundancy-free quantum error correction mechanism lies in the fundamental difference between classical and quantum information. In our system the noise of the quantum channel is modeled by a rotation angle. The questions are how to send over a noisy quantum channel certain amount of qubits, to provide error correction. Any physical realization of a quantum channel is likely to be susceptible to errors, because we cannot build perfect physical systems and isolate them from their environments while still maintaining control over the quantum states. We have to use quantum error correction codes to protect quantum information against such errors. The main idea in our redundancy-free theory is the engineering precision, which means that we usually don't need 100 percent perfect solution for an engineering challenge, the 99 percent perfect solution is a good solution. Of course the above described method is only in a rough state, for further use the model further investigations are needed.

The correction of the damaged quantum states is not possible in a classical representation, since the error corretion of qubits is realized by unitary rotations. Our initial assumption is that the channel rotates the qubit with an ω degree, that is consdired to be constant so far. We wish to create a system where error correction is possible. The

transmission is considered successful when at the end of the channel the qubit remains in its original state's ε environment. The main question is, whether it is possible to construct such A (and a corresponding B, which produce the inverse of matrix A) transformation in the following scheme, that the information can be processed through the channel

To achieve this we mix the qubits and send them over the channel, as shown in Figure 2. What we expect is that at the measurement, the error for one qubit is distributed among the others in its environment (its neighbors). By being so, the error remains in an ε environment for each qubit.

We use n long qubits so that $2^n = N$, where n is the length of the qubits and N is the size of the space. Let the l th qubit in the sequence sent through the channel be:

$$|\psi_l\rangle = a_l|0\rangle + b_l|1\rangle, \text{ where } |a|^2 + |b|^2 = 1. \tag{1}$$

This case the entire sequence sent through the channel can be described as:

$$|\phi\rangle = \otimes_{i=1}^{n} |\psi_l\rangle, \tag{2}$$

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \phi_i |i\rangle. \tag{3}$$

One can construct a classical channel with zero redundancy error correction for any unitary channel. Of course the information itself is classical, coded into qubits. This case the channel model is the following: The inputs and outputs are classical bits: ($|0\rangle$, $|1\rangle$). Since U is unitary, thus it can be written in the following form:

$$U = \sum_i \lambda_i |u_i\rangle, \tag{4}$$

where λ_i, $|u_i\rangle$ are the eigenvalues and the eigenvectors of matrix U and

$$\lambda_n = e^{j\alpha_n}. \tag{5}$$

Because U is unitary, it acts on each qubit and changes it as

$$|\psi\rangle = U|\psi_k\rangle. \tag{6}$$

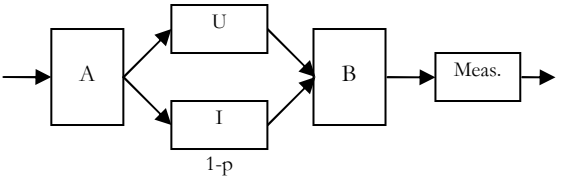

Fig. 2. Our channel model. A transforms the initial qubits into a special form. B has to produce the inverse of matrix A.

Using the eigenvalues from we get the following matrix for U

$$U_k = \begin{bmatrix} e^{j\alpha_{k1}} & 0 \\ 0 & e^{j\alpha_{k2}} \end{bmatrix}. \tag{7}$$

Because of (7) U must like

$$U = \begin{bmatrix} e^{j\pm\alpha_{k1}} & 0 \\ 0 & e^{j\pm\alpha_{k2}} \end{bmatrix}. \tag{8}$$

Now we need to do some assumptions. Let us suppose that we have two. As for the eigenvalues, we have two cases

$$\text{I. } U = \begin{bmatrix} e^{j+\alpha} & 0 \\ 0 & e^{j+\alpha} \end{bmatrix} \otimes \begin{bmatrix} e^{j+\alpha} & 0 \\ 0 & e^{j+\alpha} \end{bmatrix} = \begin{bmatrix} e^{j2\alpha} & 0 \\ 0 & e^{j2\alpha} \end{bmatrix}, \tag{9}$$

$$\text{II. } U = \begin{bmatrix} e^{j+\alpha} & 0 \\ 0 & e^{j+\alpha} \end{bmatrix} \otimes \begin{bmatrix} e^{j-\alpha} & 0 \\ 0 & e^{j-\alpha} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I. \tag{10}$$

This description lead to a redundancy-free solution because the classical states are coded into the eigenvectors of the U matrix and the eigenvalues can be written in the form shown in (5) in case of a unitary transformation.

With this model one can create redundancy-free error correction. It also works for higher dimensions, not only two. The first simulation results show that with the appropriate selection of the matrix A we can restore one quantum bit sent over the channel without any other (redundant) information.

4 Generalized Redundancy-Free Channel

In this section we consider the redundancy-free implementation of an unitary error correcting operator $\mathcal{R}_\theta$. Our protocol achieves the redundancy-free quantum communication using *local unitary operations* and *unitary matrices.*

4.1 The Redundancy-Free Error Correction

The *error* of the quantum channel is modeled by a unitary transformation, which is denoted by rotation $\mathcal{R}_\theta^\dagger$. In our model the error of the Quantum Channel is an angle $\theta_i \in [0, 2\pi)$ for every classical bit, which prepares the quantum state $|\psi_i\rangle = \cos\theta_i |0\rangle + \sin\theta_i |1\rangle$. In Figure 3. Alice's original qubit is denoted by ψ_A. At the beginning of the communication, Alice sends her quantum state ψ_A on the quantum channel, which changes to $|d\rangle = \mathcal{R}_\theta^\dagger(\psi_A)$ with given probability *p*. The error of the quantum channel is denoted by $\mathcal{R}_\theta^\dagger$.

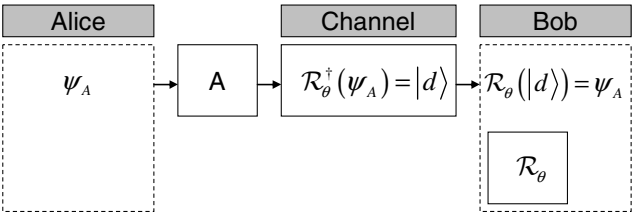

Fig. 3. Generalized channel – initial step

Let the *error-correcting* unitary operation be $\mathcal{R}_\theta \equiv e^{(i\theta\sigma_z/2)}$, for an arbitrary angle $\theta \in [0, 2\pi)$, which corresponds to an arbitrary rotation around the $\hat{z}$ -axis of a spin ½ particle. In our error-correcting process when Bob tries to read the sent quantum state, he doesn't know the effect of the quantum channel, thus the required angle state $|\theta\rangle$ nor the complex coefficients a and b.

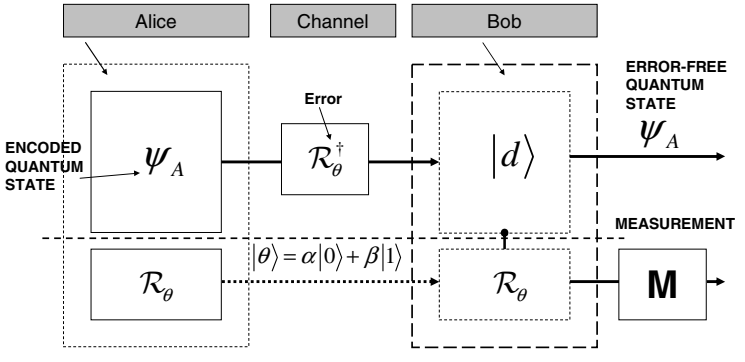

Fig. 4. Our redundancy-free coding mechanism

In Figure 4. we illustrated our redundancy-free coding mechanism, Alice initial state is ψ_A, her correction state is $\mathcal{R}_\theta$. Bob uses a CNOT to correct the error of the quantum channel.

For every quantum state, Bob measures with the projection operator $\mathcal{P} = |0\rangle\langle 0| + |1\rangle\langle 1|$. The result of the linear operator $\mathcal{P} = |0\rangle\langle 0|$ acting on an unknown $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ quantum state, projects the state $|\psi_i\rangle$ into state $|0\rangle$ with probability $|\alpha|^2$, while the linear operator $\mathcal{P} = |1\rangle\langle 1|$ projects into state $|1\rangle$ with probability $|\beta|^2$.

4.2 Probabilistic Quantum Error Correction

In our redundancy-free model, in order to read the sent quantum bits correctly, Bob must rotate the *i*-th data quantum bit by the angle θ_i in the opposite direction of what the *error of the quantum channel rotated*. The error angle $-\theta_0$ of the channel can be

corrected using the opposite direction θ_0, which is encoded by the rotation operator $\mathcal{R}(\theta_0)$. The rotation operator $\mathcal{R}(\theta_0)$ in matrix form is:

$$\mathcal{R}(\theta_0)=\begin{pmatrix}\cos\theta_0 & \sin\theta_0\\ -\sin\theta_0 & \cos\theta_0\end{pmatrix}. \tag{11}$$

We denoted the sent qubits by $\psi_A = a|0\rangle + b|1\rangle$, and the error of the quantum channel by $\mathcal{R}_{\theta_i}^{\dagger}$, and on Bob's side, the error-correcting mechanism is realized by a *unitary rotation* $\mathcal{R}(\theta_i)$. Bob has a chance *not greater* than $\varepsilon = \sin^2(\theta_i)$ to correct the sent states, because he doesn't know the original rotation angle θ_i of the quantum channel's error on the *i*-th sent qubit. The rotation operation $\mathcal{R}_\theta$ of the error correcting mechanism can be given by the angle $|\theta\rangle$, since

$$|\theta\rangle = \frac{1}{\sqrt{2}}\left(e^{i\frac{\theta}{2}}|0\rangle + e^{-i\frac{\theta}{2}}|1\rangle\right). \tag{12}$$

The error-correcting method consists of a *control qubit, which* corresponds to the damaged qubit $|d\rangle$, and a *target qubit*, which is equal to the *error-correction* angle state $|\theta\rangle$. To correct state $|d\rangle$ to ψ_A, we use a simple CNOT transformation, thus our state is transformed to

$$|d\rangle\otimes|\theta\rangle \rightarrow \frac{1}{\sqrt{2}}\left(\mathcal{R}_\theta|d\rangle\otimes|0\rangle + \mathcal{R}_\theta^{\dagger}|d\rangle\otimes|1\rangle\right), \tag{13}$$

and therefore a projective measurement in the $\{|0\rangle,|1\rangle\}$ basis of the correction-state $|\theta\rangle$ will make the damaged qubit $|d\rangle$ collapse either into the desired state $\mathcal{R}_\theta|d\rangle$ or into the wrong state $\mathcal{R}_\theta^{\dagger}|d\rangle$.

5 Conclusions

Quantum communication specifically provides a method of distributing the secret keys required to provide unconditionally secret communications and its use is guaranteed to reveal the presence of an enemy attempting to compromise the transfer. The redundancy-free channel is not only a solution for wired systems, but could be part of the wireless communication too. This method could be very useful in the long-distance aerial communication, because there would be no need to use redundant error correction codes as nowadays. This way the effective capacity of the satellite link would also be increased.

In this paper we presented a completely new method to correct quantum states. The rotation operations applied in the error correcting mechanism can be implemented with some associated error, which decreases exponentially with the number of quantum

states of the error correction state. With redundancy-free solutions we can get over some troubles issued from the atmosphere (in earth-satellite communication) and we can achieve higher bandwidth (effective one) in satellite-communication.

This paper should be also regarded as a starting point for further analysis of the properties and efficiency of our redundancy-free quantum correction system.

References

[1] Imre, S., Ferenc, B.: Quantum Computing and Communications: An Engineering Approach. Wiley, Chichester (2005)
[2] Buttler, W.T., Hughes, R.J., Kwiat, P.G., Lamoreaux, S.K., Luther, G.G., Morgan, G.L., Nordholt, J.E., Peterson, C.G., Simmons, C.M.: Practical free-space quantum key distribution over 1 km, arXiv:quant-ph/9805071
[3] Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10 km in daylight and at night. New Journal of Physics 4, 43.1–43.14 (2002)
[4] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J.G., Zeilinger, A., Weinfurter, H.: Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. Physical Review Letters PRL 98, 010504 (2007)
[5] Bacsardi, L.: Using Quantum Computing Algorithms in Future Satellite Communication. Acta Astronautica 57(2-8), 224–229 (2005)
[6] Bacsardi, L.: Satellite communication over quantum channel. Acta Astronautica 61(1-6), 151–159 (2007)
[7] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
[8] Poulin, D.: Stabilizer Formalism for Operator Quantum Error Correction (2005), Quant-ph/0508131