IAC-08-B2.4.8

REDUNDANCY-FREE QUANTUM THEORY BASED ERROR CORRECTION METHOD IN LONG DISTANCE AERIAL COMMUNICATION

Laszlo Bacsardi
Department of Telecommunications, Budapest University of Technology and Economics, Hungary
bacsardi@hit.bme.hu

Marton Berces, Sandor Imre
Department of Telecommunications, Budapest University of Technology and Economics, Hungary
{berces; imre}@hit.bme.hu

ABSTRACT

Quantum computing has a shorter history than satellites. From the engineering point of view, a quantum computing system may represent the highest level of information processing—a system where the physical layer is based on quantum mechanics. Although quantum computers are not to exist in the near future, the results of quantum computing are unquestionable: teleportation, O(n^1/2) search in an unsorted database, practically unbreakable key distribution and many more. Previous studies show that it is to mix satellite communication (a profitable business) and quantum computing (a new technology). Although there are recent studies about the physical solutions of the quantum-based communication, it is worth to examine the efficiency of this type of communication. Our primary goal is to create a quantum computing based redundancy-free error correction method that can be used over long distance aerial communication (such as earth-satellite). In this paper we present a theoretical study. The initial problem to solve is how to send certain amount of quantum bits over a noisy quantum channel, how to provide error correction. Solving this problem, the used 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.

FULL TEXT

I. INTRODUCTION

The telecommunication and the satellite communication always have been a pulling force either in the military or in the civil environment. For an improved telecommunication system we need better hardware, better software and better solution for the transmission - irrespectively of what better means. Due to a convergence between the different technologies, there are a lot of solutions in telecommunications which are coming from other fields like information theory or computer studies. One of the main problems in the field of computer technology is the decreasing size of transistors used during the manufacturing process of the computers. According to engineer Gordon Moore we already now from the 60's, that the size of the microchips reduce to half in about every 18 months. This will cause some problems in creating the atomic-size transistors and handling their egress. But it could be a beginning of a new technology called quantum computing [1]. Since 1980 recent studies have been dealing with this technology, and from the 90's this way of the technology seem to be an efficient tool in telecommunication and even in satellite communication.

Despite of the many theoretical results there are significant problems in the practical realization. Thousands of mathematicians, physicists and engineers are working to create a faster and more reliable communication system, and the results of quantum information theory can be used in factorizing and cryptography, in the

searching in a sorted or unsorted database etc. But one of the main fields where existing solutions can be found is communication. After successful wire-based experiments—some kind of quantum products are already in commercial trade—the interest of researches turned to the wireless solutions, and the convergence with satellite communication started.

Our study deals with the quantum based communication which can be used either in the earth-satellite (satellite-earth) or satellite-satellite communication. This is a theoretical study with practical results presented in the second section.

There is no doubt it that we could be able to communicate with satellite from the surface of the Earth using quantum based algorithms, because there are recent studies proving that it is possible. The question investigated in our paper is that how can it be done most effectively.

II. QUANTUM COMMUNICATION

Classical communication occurs between two or more parties on a channel with the interference of the environment (called noise in the literature). In computer science the sender usually sends bits and the recipient digests those. In quantum computing qubits are used for exchanging information. The main question is: can quantum communication be more effective than classical ones? Holevo's theorem [2] states that for sending n classical bits n qubits are required no matter what kind of coding we use. If the participants share entangled pairs in advance then twice as many bits can be sent, not more.

2.1 Moore-law

As the experimental observation by Gordon Moore—stating that in every two year the number of transistors built on unit surface doubles—described in 1965 is still true, industry will face a limit in the transistor miniaturization. Researchers need to look for other methods to increase computing capacities of computers. One way is to design new architectures that suite applications more effectively. The other is to create a general computing architecture that is more powerful than the previous one. Industry goes this second way, but the boundaries of classical physics will sooner or later arise. At that point quantum based computation devices (quantum computers) can solve humanity's need for computing capacity.

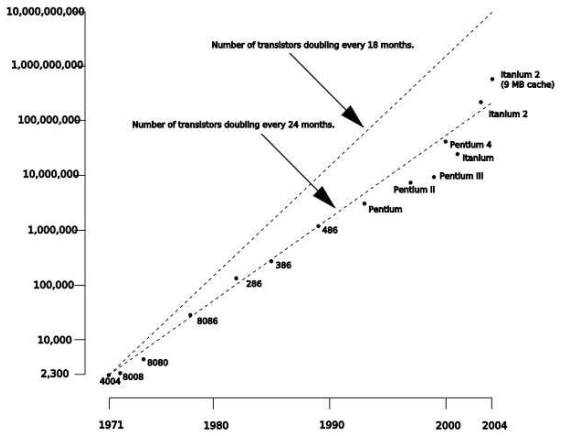

Fig 1.: Graphical representation of the Moore-law. Horizontaly the years, vertically number of transistors on an integrated circuits are represented.

2.2 Quantum bit

A quantum bit (that is often called a qubit) is a unit long two-dimensional complex vector. Every closed system can be described with this method. It can be imagined as if it was a coin flipping in the air. While in air, its state is undecided, it is in the superposition of the two sides (base states). When it is settled on the ground, it is in a definite state; either head or number. More detailed description is provided below.

2.3 Postulates

1) Each state of a closed system can be described by means of a vector in a Hilbert space [1]. In quantum computing the state vectors are denoted as $|\varphi\rangle$ (say 'ket phi' according to Dirac). The coordinates of $|\varphi\rangle$ are complex numbers and each of them refers to the probability amplitude of the associated basis (classical) state. The simplest quantum system is the so called qubit which replaces in the quantum world the classical information bearing unit, the bit. A qubit can be prepared in a two dimensional superposition of both classical bit values (0 and 1) as

$$|\varphi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = a|0\rangle + b|1\rangle;\ a,b \in \mathbb{C}, \qquad (1)$$

where $|a|^2$ and $|b|^2$ represent the probabilities of getting the classical bit values (orthonormal basis states) $|0\rangle$ and $|1\rangle$ as the result of measuring the qubit respectively. Of course $|a|^2 + |b|^2 = 1$ shall be fulfilled because of the complete probability law of probability theory (i.e., only unit length vectors are allowed). The conjugate transpose of $|\varphi\rangle$ is denoted by $\langle\varphi| = (|\varphi\rangle^*)^T = \begin{bmatrix} a^* & b^* \end{bmatrix}$.

Generalizing the above set of definitions a quregister consisting of n qubits is described as

$$|\varphi\rangle = \begin{bmatrix} \varphi_0 \\ \varphi_1 \\ \vdots \\ \varphi_{2^n-1} \end{bmatrix} = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle, \qquad (2)$$

Based on (2) we emphasize that the above quregister contains all the $2^n - 1$ basis states (i.e., classical integer number) at the same time, which can be regarded as the source of quantum parallelism.

The inner (scalar) product of two states is denoted and defined as

$$\langle\varphi|\psi\rangle = \sum_{i=0}^{2^n-1} \varphi_i^* \cdot \psi_i \,. \qquad (3)$$

Two vectors are orthogonal if and only if $\langle\varphi|\psi\rangle = 0$ and are identical if and only if $\langle\varphi|\psi\rangle = 1$.

The outer (matrix) product of two states is denoted and defined as

$$|\varphi\rangle\langle\psi| = A = \begin{bmatrix} A_{00} & \cdots & A_{0(2^n-1)} \\ \vdots & \ddots & \vdots \\ A_{(2^n-1)0} & \cdots & A_{(2^n-1)(2^n-1)} \end{bmatrix}, \; A_{ij} = \varphi_i \cdot \psi_j^*, \qquad (4)$$

2) Having explained how to describe the system, now we present how to calculate its evolution. In quantum computing only a special type of linear operators can be used, namely the unitary operator i.e., the inverse of its matrix equals its adjoint (conjugate transpose) $U^{-1} = U^+$. So each quantum gate can be handled as an $n \times n$ matrix and the state of the system at the output of the gate $|\varphi_{out}\rangle = U|\varphi_{in}\rangle$.

3) The only exception from the unitarity principle of quantum gates is the measurement device which does not suffer from this restriction. Each measurement can be defined by means of a set of measurement operators $\{M_m\}$, where m refers to the different measurement outcomes. These operators can be imagined as they were in the same "gate or box" and all of them act upon measurement. Then the measured system evolves into its next state according to the measurement probabilities. Hence the mathematical representation of a measurement operator is not always unitary the measurement is not always reversible. The probability of getting a measurement result m assuming $|\varphi_{in}\rangle$ as an input state equals to

$$P(m) = \langle \varphi_{in} M_m^{\uparrow} | M_m \varphi_{in} \rangle, \qquad (5)$$

and the state of the system after the measurement is

$$|\varphi_{out}\rangle = \frac{M_m |\varphi_{in}\rangle}{\sqrt{\langle \varphi_{in} M_m^{\uparrow} | M_m \varphi_{in} \rangle}}, \qquad (6)$$

The measurement operator set needs to fulfill the following condition too:

$$\sum_m M_m^{\uparrow} M_m = I, \qquad (7)$$

So the measured system will not disappear we will know its state after measurement with certain probability.

4) The last rule provides how to merge quantum systems (e.g., qubits into a quregister) together. We shall use the tensor product (⊗) between the state vectors of the individual systems. Let us suppose we have two qubits $|\varphi_1\rangle = a_1|0\rangle + b_1|1\rangle$ and $|\varphi_2\rangle = a_2|0\rangle + b_2|1\rangle$. Then the state of the quregister consisting of these two qubits is

$$|\varphi_1\varphi_2\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle = a_1a_2|00\rangle + b_1a_2|10\rangle + a_1b_2|01\rangle + b_1b_2|11\rangle. \qquad (8)$$

The tensor product preserves the unit length for the qregister in accordance with Postulate 1. The notation ⊗ is often omitted or replaced with '·'.

2.4 Some applications

Today, the most important applications of quantum communication is Quantum based Key Distribution systems (QKDs). These devices provide both theoretically and practically unbreakable key distribution via optical cable. The devices can be bought and mostly use the BB84 protocol to operate. Of course there are several other aspects of quantum computing and computation, some mentioned below.

One of the most referred result is the search for a marked item in an unsorted database. That is called the Grover algorithm. This gives the result after $\Theta(\sqrt{N})$ iteration where N is the number of elements in the database.

Another further application could be the teleportation. To do that a classical channel is used to create a particle that has the same properties as the one on the "sender" side.

III. CHANNEL CODING

3. 1 Quantum channel

One of the major differences between the classical and quantum channels that in the second one the information carrying quantum system is in interaction with the environment as an undesirable noise. This phenomena is named quantum decoherence. The noise appearing from the entanglement with the environment can be observed in Fig 2.

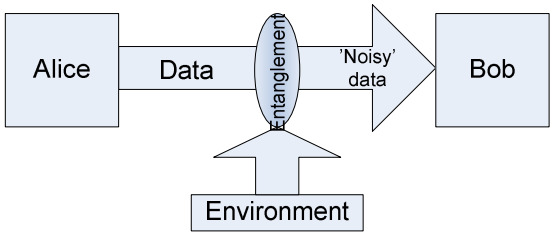

Fig 2.: General model of the quantum channel

3.2 Free-space channel

The free-space Quantum Key Distribution (QKD) [3_1] was first introduced over an optical path of about 30 cm in 1991. Several demonstrations (indoor optical paths of 205 m and outdoor optical paths of 75 m) increased the usability of QKD by extending it with line-of-site laser communications systems. There are certain key distribution problems in this category for what free-space QKD would have definite practical advantages (for example, it is not practical to send a courier to a satellite).

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 [3]. Four years later, in 2002 the researchers of the same laboratory have demonstrated that free-space QKD is possible in daylight or at night [4]. In 2006, the distance of 144 km was reached by an international research group [5].

In our point of view, the quantum computing algorithms can be used to affirm our communication in following four ways: [6]

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: the broadcast satellite is in orbit at 36,000 km using 27 MHz frequency for signalling. In the Quadrature Phase Shift Keying (QPSK) every symbol contains two bits, this is why the bit speed is 54 Mbs. Half the bits are used for error-correction, so at most we have 38 Mbs, but in common solutions there are only 27-28 Mbs, in which usually 5-6 TV-channels is stored with a bandwidth of 2-5 Mbs each. 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 [7].

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.

3.3 Channel coding

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 [8]:
1. The errors are continuous. The errors can results either amplitude or phase decoherence. Moreover both errors have complex coefficients which means 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 transmited 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 [9]. The simplest one is the 3-qubit bit-flip code which can correct one bit-flip error in a channel similarly to the classical binary symmetric channel. Without any deep mathematical details the main points of this error coding algorithm is described below. The two communication parties are called Alice and Bob. The initial quantum bit is not copied but Alice code it in a three bit length quantum bit. At the output we detect a syndrome vector. It's important that the qubits are not measured by Bob he examined only the equation of the three qubits without any information about their content. The table of syndromes shows what kind of correction has to be done for achieving the correct information.

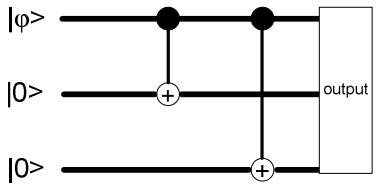

Fig 3.: Initial linear transformation for 3 qubit bit-flip code

The 3-qubit phase-flip code can correct one phase-flip error (there is no similar failure in the classical world). The procedure for this correction is similar as in the 3-qubit bit-flip code, but we use other initial coding process and other

The Shor-code presented by Peter Shor was the first code for correcting an arbitrary quantum bit error (either a bit-flip or phase-flip error) [REF]. Unfortunately the correction system requires large overhead – for sending one quantum bit we need to handle 17 qubits.

Now for the better error correction we have Calderbank-Shor-Steane codes, stabilizer codes etc. [8] The basic idea of the Steane-code is that the correction of the bit-flip errors is similar to the classical cases, the correction of the phase-flip errors are traced back with a quantum transformation to the case of the bit-flip errors. This code is a short one, but the main advantage is that the size of the circuit needed for error detection and correction is linear to the size of the code (and not exponential one like at the 3-bit bit-flip or phase-flip code.

IV. REDUNDANCY-FREE QUANTUM CHANNEL

4. 1 Redundancy-free channel

One of the most exciting questions in the field of quantum communictaion is the following: How to send over a noisy quantum channel certain amount of qubits, to provide error correction? The qubits are independent, each contains information that needs to be processed.

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. By this, not a complete restoration is meant. 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?

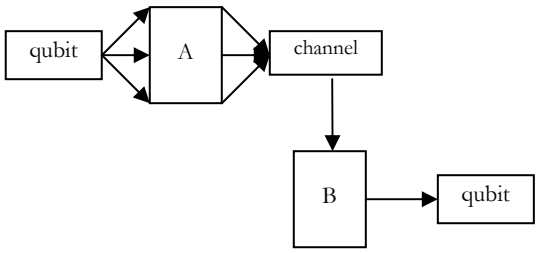

Fig 4.: Initial channel model. A transforms the initial qubits into a special form. B has to produce the inverse of matrix A.

To achieve this we mix the qubits and send them over the channel, as shown in Figure 4. 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 remaind 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. 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:

$$U = \sum_i \lambda_i |u_i\rangle \qquad (9)$$

where λ_i, u_i are the eigenvalues and the eigenvectors of matrix U and

$$\lambda_n = e^{j\alpha_n} \qquad (10)$$

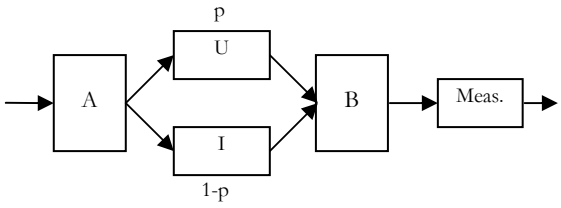

Figure 5.: Generalized channel model

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 (10) 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. 2 Using a redundancy-free channel in long distance communication

As discussed before, the free-space quantum channel could be used in least four different ways in satellite communication. The redundancy-free channel is not only a solution for wired systems, but could be part of the wireless communicaton 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

With redundancy-free solutions we can get over the troubles issued from the atmosphere (in earth-satellite communication) and we can achive higher bandwidth (effective one) in stallite-satellite communiction.

The main idea in our redundancy-free theory is the engineering precision which mean 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.

If we allow a little variance from the beginning we can manage a well operating system for quantum based communication.

V. CONCLUSION

In this paper some possible advantages of the redundancy-free quantum channel are examined, and a solution is presented for creating this kind of channel.
The long-distance redundancy-free aerial communication can be used in other earth-based application illustrating well that the results of the space research come over to the everydays life. It can be used in applications where the information dissemination is important but 100 percent solution is not neccessary and cable-based solution does not exists.
The redundancy-free quantum correction method can be a new tools either for the existing or the planned quantum space applications.

REFERENCES

[1] S. Imre, B. Ferenc, 'Quantum Computing and Communications: An Engineering Approach', (Wiley, 2005)

[2] A. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel", Problemy Peredachi Informatsii, Vol. 9, no. 3, 1973, pp. 3 – 11. English translation in Problems of Information Transmission, Vol. 9, 1973, pp. 177 – 183

[3] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, 'Practical free-space quantum key distribution over 1 km' (arXiv:quant-ph/9805071)

[4] Richard J Hughes, Jane E Nordholt, Derek Derkacs and Charles G Peterson, 'Practical free-space quantum key distribution over 10 km in daylight and at night', (New Journal of Physics 4 (2002) 43.1–43.14)

[5] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter,

'Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km', (Physical Review Letters, 2007, PRL 98, 010504 [2007])

[6] L. Bacsardi, Using Quantum Computing Algorithms in Future Satellite Communication, (Acta Astronautica, Vol 57. Issue 2-8., pp 224-229. [2005])

[7] L. Bacsardi, Satellite communication over quantum channel (Acta Astronautica, Volume 61, Issues 1-6, June-August 2007, p 151-159)

[8] Michael A. Nielsen, Isaac L. Chuang: Quantum Computation and Quantum Information, (Cambridge University Press, [2000])

[9] David Poulin, Stabilizer Formalism for Operator Quantum Error Correction, (Quant-ph/0508131, [2005])