Quantum error correcting code for specific position errors and its application

Hiroyuki Shiraki[1] * Shogo Usami[1] Tsuyoshi Sasaki Usuda[2 3] Ichi Takumi[1]

[1] *Dept. of A.I. and Computer Science, Nagoya Institute of Technology*
Gokiso-cho, Showa-ku, Nagoya 466-8555 Japan.
TEL: 052-735-5472 FAX: 052-735-5477
[2] *Faculty of Information Science and Technology, Aichi Prefectural University,*
Kumabari, Nagakute-cho, Aichi, 480-1198 Japan.
[3] *CREST, JST*

Abstract. In this paper, we consider the quantum error correction in the case of considering security and propose quantum codes which are a different type from ordinary quantum error correcting codes. Furthermore we show performance evaluation and an example of application of the codes.

Keywords: quantum cryptography, quantum error correcting code, quantum data transmission

1 Introduction

We consider transmission and processing of quantum information. Quantum information is easily influenced by noise from environment while arbitrary states cannot be cloned [1]. Therefore based on classical coding theory, quantum error correcting code [2, 3, 4] was devised as the ways of coping.

In classical coding theory, the purpose of the coding is to reduce the error probability p close to 0 by error correction. In the error model of classical coding theory, each bit of output strings is either an error bit or a correct bit although an error may occur in any position with error probability p. For example, (3,1) classical code can correct an arbitrary single bit error completely. As we mentioned above, the theory of quantum error correcting code is also constructed as based on an assumption of such an error pattern. The five-qubit code, for example, can protect against an arbitrary single qubit error [5].

However, in almost case of sending quantum information via noisy quantum channel, all qubits of output strings are actually mixed state. It is necessary to measure quantum states in order to introduce the concept of "error". But measurement breaks quantum states. Hence we do not consider measurement. For this reason, it is difficult to consider the situation that each qubit of output strings is either an error qubit or a correct qubit. Therefore, in almost application of quantum error correcting codes, fidelity between an original qubit sequence and qubit sequence obtained by decoding is useful to evaluate codes [6, 7].

Here we consider different channel model from the model mentioned above. Our channel model consists of an unreliable channel and a reliable channel (Fig.1). The unreliable channel is a public quantum channel in which quantum information is easily influenced by a third party's eavesdropping or a heavy quantum information processing in which probability that the processing is failed is high. On the other hand, the reliable channel is a private quantum channel, a reliable quantum memory, or a quantum file server. An example of such a channel can be considered in a quantum security protocol (see Section 4). We consider the quantum error correction for such model in this paper and propose quantum codes which are a different type from ordinary quantum error correcting codes. Furthermore we show performance evaluation and an example of application of the codes.

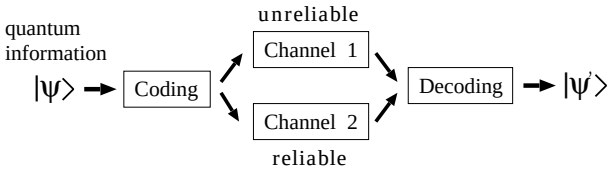

Figure 1: The model of quantum channel.

2 Error correction to specific positions

In this section, we show quantum error correcting codes for specific position error in order to apply the channel model shown in Fig.1.

2.1 The quantum error correcting code for specific position errors by $(3m, m)$ coding

We consider $(3m, m)$ quantum code which is designed as based on an assumption that a probability of arising errors from the 1st-qubit to the mth-qubit is high (sending via channel 1) and probabilities of arising errors of the other qubits are low (sending via channel 2). This code can correct errors which occur from 1st-qubit to mth-qubit.

We encode a m-qubit state $|\psi\rangle = \sum_{i=0}^{2^m-1} c_i|i\rangle$ in $3m$-qubit state as

$$|\psi\rangle \longrightarrow |\Psi_{\rm code}\rangle = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} c_j|s_j\rangle, \tag{1}$$

$$|s_j\rangle = \sum_{k=0}^{2^m-1} (-1)^{w_{\rm H}(j\cdot k)}|k\rangle|k\rangle|j\rangle, \tag{2}$$

where $w_{\rm H}(i)$ denotes Hamming weight of i in binary notation. And $j \cdot k$ means "AND" operation for each qubit when j and k are represented as binary numbers of m-digits.

2.2 The quantum error correcting code for specific position errors by $(2m+1, m)$ coding

In this subsection, we propose more efficient coding than the coding introduced in Section 2.1. This code can correct errors which occur from 1st-qubit to mth-qubit as well as the $(3m, m)$ quantum code.

*hasebon@ics.nitech.ac.jp

We encode a m-qubit state $|\psi\rangle = \sum_{i=0}^{2^m-1} c_i|i\rangle$ in $(2m+1)$-qubit state as

$$|\psi\rangle \longrightarrow |\Psi_{\rm code}\rangle = \frac{1}{\sqrt{2}} \sum_{j=0}^{2^m-1} c_j|s_j\rangle, \tag{3}$$

$$|s_j\rangle = \begin{cases} (|00\cdots0\rangle + |11\cdots1\rangle)|j\rangle \ (0 \le j \le 2^{m-1}-1), \\ (|00\cdots0\rangle - |11\cdots1\rangle)|j\rangle \ (2^{m-1} \le j \le 2^m-1), \end{cases} \tag{4}$$

where j is represented as binary numbers of m-digits.

The simplest example of the $(3m,m)$ and $(2m+1,m)$ codes is the (3,1) quantum code and we have shown that this code can correct an error of 1st qubit [8]. Moreover by making use of the stabilizer formalism it can be said that the $(3m, m)$ and $(2m+1,m)$ codes can correct errors which occur from 1st-qubit to mth-qubit .

3 Bound for the quantum error correcting code for specific position errors

In this section, we will modify the quantum Hamming bound for the codes described in Section 2, then we examine the performance limit of them by using the bound.

3.1 The quantum Hamming bound

Any quantum code encoding k qubits in n qubits in a non-degenerate way must satisfy the following inequality known as the quantum Hamming bound [9].

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \le 2^n, \tag{5}$$

where t represents the number of correctable errors.

3.2 The modified quantum Hamming bound

Here we modify the quantum Hamming bound for the codes introduced in Sectoin 2. In this case, the locations where errors may occur are specific locations in qubits. Therefore the quantum Hamming bound suitable for such codes is defined by the following inequality (6). Note that n' represents the locatons where errors may occur.

$$\sum_{j=0}^{t} \binom{n'}{j} 3^j 2^k \le 2^n. \tag{6}$$

3.3 Degenerate codes breaking the inequality (6)

We evaluate the performance limit of the code described in Equation (1) by using the inequality (6). In this case, $n'=m$, $t=m$ and $\sum_{j=0}^{t} \binom{m}{j} 3^j 2^m = (1+3)^m \cdot 2^m = 2^{3m} = 2^n$. Thus this code saturates the modified quantum Hamming bound, that is, it satisfies the inequality (6) with equality.

On the other hand, as far as the code described in Equation (3) concerned, $n'=m$, $t=m$ and $\sum_{j=0}^{t} \binom{m}{j} 3^j 2^m = 2^{3m} > 2^{2m+1} = 2^n$ $(m \ge 2)$. Therefore we can regard this code as a degenerate code which breaks the inequality (6).

4 Application to secure transmission of quantum information

Recently, a quantum cryptographic protocol with the authentication was proposed by Azuma and Ban (Azuma-Ban protocol [10]). In this section, we consider using the authentication as error detection so that if quantum information is destroyed by eavesdropping, error correction enables it to be resended.

We consider to apply the $(3m,m)$ quantum codes described in Section 2 to the Azuma-Ban protocol. In this case, a quantum channel between sender and receiver corresponds to Channel 1 shown in Fig.1 and a reliable quantum memory at the sender side corresponds to Channel 2 shown in Fig.1.

We show the schematic diagram of the protocol after application in Fig.2.

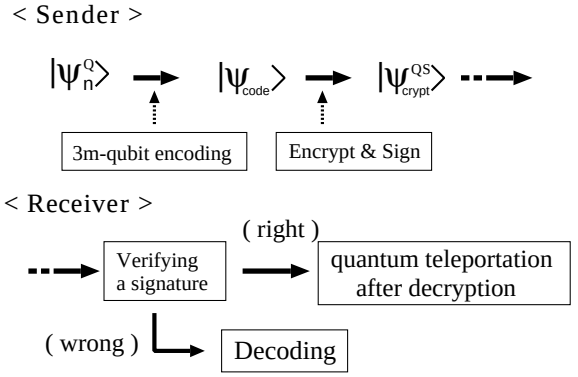

Figure 2: The schematic diagram of the protocol after application.

5 Conclusions

In this paper, we have considered quantum error correcting codes for specific position errors and their application. Moreover, we have considered the quantum Hamming bound suitable for such codes, and then we show degenerate codes as examples of breaking the bound.

As a future subject, we will consider an example of an application of the $(2m+1,m)$ codes.

Acknowledgement :
This work was partially supported by the program "R&D Support Scheme for Funding Selected IT Proposals" of MPHPT and MEXT. KAKENHI (No.15760271).

References

[1] W.K.Wootters and W.H.Zurek, Nature, **299**, pp.802-803, 1982.

[2] P.Shor, Phys. Rev. **A52**, pp.2429-2496, 1995.

[3] A.Calderbank and P.Shor, Phys. Rev. **A54**, pp.1098-1105, 1996.

[4] D.Gottesman, Phys. Rev. **A54**, pp.1862-1868, 1996.

[5] R.Laflamme, C.Miquel, J.P.Paz and W.H.Zurek, Phys. Rev. Lett. **77**, pp.198-201, 1996.

[6] E.Knill and R.Laflamme, Phys. Rev. **A55**, pp.900-911, 1997.

[7] R.Matsumoto, Phys. Rev. **A64**, 022314, 2001.

[8] H.Shiraki, S.Usami, T.S.Usuda and I.Takumi, SITA2001, pp.859-862, 2001.

[9] A.Ekert and C.Macchiavello, Phys. Rev. Lett. **77**, pp.2585-2588, 1996.

[10] H.Azuma and M.Ban, J.Phys. **A34**, pp.2723-2741, 2001.