Analytical technique for simplification of the encoder–decoder circuit for a perfect five-qubit error correction

2006 New J. Phys. 8 80

(http://iopscience.iop.org/1367-2630/8/5/080)

New Journal of Physics
The open–access journal for physics

Analytical technique for simplification of the encoder–decoder circuit for a perfect five-qubit error correction

Jin-Yuan Hsieh[1], **Che-Ming Li**[2] **and Der-San Chuu**[2]

[1] Department of Mechanical Engineering, Ming Hsin University of Science and Technology, Hsinchu, 30401, Taiwan

[2] Institute and Department of Electrophysics, National Chiao Tung University, Hsinchu, 30050, Taiwan

E-mail: jyhsieh@must.edu.tw

New Journal of Physics **8** (2006) 80
Received 28 December 2005
Published 30 May 2006
Online at http://www.njp.org/
doi:10.1088/1367-2630/8/5/080

Abstract. Simpler encoding and decoding networks are necessary for more reliable quantum error-correcting codes (QECCs). The simplification of the encoder–decoder circuit for a perfect five-qubit QECC can be derived analytically if the QECC is converted from its equivalent one-way entanglement purification protocol. In this work, the analytical method to simplify the encoder–decoder circuit is introduced and a circuit that is as simple as the existing simplest circuits is presented as an example. The encoder–decoder circuit presented here involves nine single- and two-qubit unitary operations, only six of which are controlled-NOT gates.

PII: S1367-2630(06)15767-5

Contents

1. Introduction

The unique feature of quantum correlation and quantum interference has stimulated ingenious scenarios to exhibit the power of quantum information processing [1]. Quantum states can be encoded into qubits through quantum error-correcting codes (QECCs). With the introduction of redundancy, the encoded data can tolerate small errors which are due to decoherence in some individual qubits. Then, QECCs play a crucial role in scalable quantum computation and communication to preserve the gain in computational time and in security.

The five-qubit QECC that protects a qubit of information against general one-qubit errors is one of special interest for quantum computations. It has been proven to be the best and smallest block code [2]. It is also a perfect non-degenerate code because it saturates the quantum Hamming bound [3] and thus is capable of correcting all one-qubit errors with a minimum number of extra qubits. Laflamme *et al* [4] and Bennett *et al* [5] independently showed the first five-qubit QECCs. Recent developments of most QECCs are attributed to stabilizer formalisms [6, 7]. In the work of Laflamme *et al* [4], the five-qubit error correction is shown to perform in a rather simple procedure. The initial one-qubit information, as accompanied with four extra qubits in the state $|0\rangle$, is encoded by a circuit representing a sequence of single-qubit Pauli operations and two-qubit controlled Pauli operations. Then, after the interaction of the environment that causes generic one-qubit errors, the polluted five-qubit state is decoded by running the same encoder circuit in reverse order. Eventually, the tensor product state of the four extra qubits is measured in the computational basis ($|0\rangle$ and $|1\rangle$) to decide the corresponding final Pauli operation for recovering the original state of the information carried qubit. By computer search, Braunstein and Smolin [8] found a simplified encoder circuit which can encode the one-qubit information in 24 laser pulses. For the stabilizer code, however, the initial one-qubit information is encoded by the actions of all the operators belonging to the group generated by the stabilizers. The encoded five-qubit state is then allowed to be affected by generic one-qubit errors followed by measurements of the stabilizer observables to detect and correct the qubit on which the error has occurred. The five-qubit stabilizer code has been experimentally implemented using nuclear magnetic resonance by Knill *et al* [9]. The five-qubit QECC introduced by Bennett *et al* [5] was derived from a restricted one-way entanglement purification protocol (1-EPP) which purifies one good Bell state from a noisy block of five Bell states. In fact, it can be shown that the Bennett *et al* protocol is equivalent to the error correction of Laflamme *et al*. However, the QECC of Bennett *et al*

can be well derived so that it requires a simpler network for both encoding and decoding than the original one reported by Laflamme *et al* Bennett *et al* suggested, i.e. to use a Monte Carlo search program for deriving the QECC.

In realistic situations, to reduce the number of two-qubit gates necessary in the encoder–decoder circuit is significantly important for reliable five-qubit QECCs because two-qubit operations could be the more difficult ones to be implemented in a physical apparatus [10]. This work thus is motivated to derive five-qubit, single-error corrections which can be performed by using the least number of two-qubit operations in their encoder–decoder networks. The QECC presented as an example herein is derived analytically from the restricted 1-EPP proposed by Bennett *et al* [5] and its encoder–decoder network contains only six controlled-NOT (CNOT) gates and three single-qubit operations. The restricted 1-EPP therefore is depicted first in section 2. In section 3, we describe the systematic method for deriving 1-EPP in detail. A concrete example for the simplest quantum gate array then will be given to show the capacity of the present method. In section 4, we present the coding circuit which is converted directly from the 1-EPP and compare its efficiency with those of several existent encoder–decoder circuits. A conclusion is given in section 5.

2. The 5-EPR-pair single-error-correcting code[3]

Suppose there exists a finite block-size 1-EPP which distills one good pair of spins in a specific Bell state from a block of five pairs, and no more than one of the five pairs is subjected to noise. When this 1-EPP is combined with a teleportation protocol, two parties, Alice and Bob, can transmit quantum states reliably from one to the other. The combination of the 1-EPP and teleportation protocol therefore is equivalent to a QECC. The 1-EPP considered herein is schematically depicted in figure 1. Suppose Alice is the encoder, Bob the decoder, and the Bell state $\Phi^+ = (|00\rangle + |11\rangle)/\sqrt{2}$ is the good state to be purified. Alice and Bob are supposed to be provided with five pairs of spins in the state Φ^+ by a quantum source (QS). However, they actually share five Bell states in which generic errors have or have not occurred on at most one Bell state due to the presence of noise N_B in the quantum channel via which the pairs are transmitted. The noise models are assumed to be one-sided [5] and can cause the good Bell state Φ^+ to become one of the incorrect Bell states

$$\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \qquad \Psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{1}$$

The good Bell state Φ^+ can become one of the erroneous Bell states expressed in (1) if it is subjected to either a phase error ($\Phi^+ \to \Phi^-$), an amplitude error ($\Phi^+ \to \Psi^+$), or both ($\Phi^+ \to \Psi^-$) [2, 11]. When performing the 1-EPP, Alice and Bob have a total of 16 error syndromes to deal with. The collection of error syndromes includes the case that none of the five pairs has been subjected to errors and the 15 cases in which one of the five pairs has been subjected to one of the three types of error. The strategy of Alice and Bob is to perform a sequence of unilateral and bilateral unitary operations (as shown in figure 1, U_1 and U_2 performed by Alice and Bob, respectively) to transform the collection of the 16 error syndromes to another collection that can provide information about the errors subjected by their particles. Suppose the state of the first

[3] EPR: Einstein–Podolsky–Rosen.

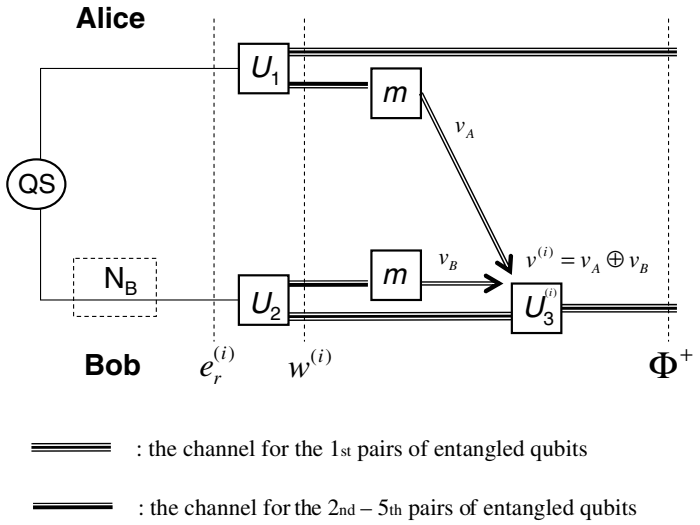


Figure 1. The 1-EPP with notations used in the context. Alice performs U_1 and m and then sends her classical result (v_A) to Bob. Bob performs U_2 and m, and then combines his own result (v_B) and Alice's to control a final operation $U_3^{(i)}$. QS, quantum source.

pair in the block is to be recovered. After performing the sequence of their operations (U_1 and U_2, respectively), Alice and Bob should then perform local measurements on their respective halves of the second to fifth pairs. Alice sends her result via classical channels to Bob who then performs the Pauli operation U_3 to recover the original state of the first pair conditionally on both Alice's and his results. The ultimate requirement of these results of final measurement is that each and every one of them should be distinguishable from the others. In other words, there should be 16 distinct measurements obtained from the aforementioned transformation of the error syndrome. The main issue now is that the sequence of unilateral and bilateral unitary operations performed by the two parties to transform the error syndrome should be well designed so the requirement just mentioned can be fulfilled.

To arrange the sequence of operations, basic concepts of linear algebra are used. The four Bell states $\Phi^{\pm}$ and $\Psi^{\pm}$ are first labelled by two classical bits, namely,

$$\Phi^+ = 00, \qquad \Phi^- = 10, \qquad \Psi^+ = 01, \qquad \Psi^- = 11. \tag{2}$$

The right, low-order or amplitude bit identifies the Φ/Ψ property of the Bell state, while the left, high-order or phase bit identifies the $+/-$ property. Note that the combined result of the local measurements obtained by Alice and Bob on a Bell state is revealed by the Bell state's low or amplitude bit. In the representation of the high–low bits, each error syndrome thus is expressed as a ten-bit codeword, e.g., the error syndrome $\Phi^+\Psi^-\Phi^+\Phi^+\Phi^+$ is written as 00 11 00 00 00. Codewords of the error syndrome, denoted by $e_r^{(i)}$, $i = 0, 1, \ldots, 15$, are listed in table 1. The effect of the sequence of unilateral and bilateral unitary operations performed by Alice and Bob is to map the codewords $e_r^{(i)}$ onto another collection of ten-bit codewords $w^{(i)}$. If both the codewords, $e_r^{(i)}$ and $w^{(i)}$ are written as column vectors in the ten-dimensional Boolean-valued ($\in \{0, 1\}$) space, then the mapping $e_r^{(i)} \rightarrow w^{(i)}$ can be simply expressed by a

Table 1. The correspondence among the error syndrome $e_r^{(i)}$ ($E_r^{(i)}$), the codeword $w^{(i)}$ ($W^{(i)}$), the measurement result $v^{(i)}$ and the Pauli operation $U_3^{(i)}$ controlled by the measurement result in the restricted 1-EPP (five-qubit QECC) applying the encoder–decoder circuit shown in figure 3 (figure 4).

i	$e_r^{(i)}$, $E_r^{(i)}$	$w^{(i)}$, $W^{(i)}$	$v^{(i)}$	$U_3^{(i)}$
0	00 00 00 00 00	00 00 00 00 00	0000	**I**
1	10 00 00 00 00	11 00 00 01 01	0011	σ_y
2	01 00 00 00 00	01 00 01 01 00	0110	σ_x
3	11 00 00 00 00	10 00 01 00 01	0101	σ_z
4	00 10 00 00 00	00 01 00 00 01	1001	**I**
5	00 01 00 00 00	00 11 01 01 00	1110	**I**
6	00 11 00 00 00	00 10 01 01 01	0111	**I**
7	00 00 10 00 00	11 01 10 01 01	1011	σ_y
8	00 00 01 00 00	00 00 01 00 00	0100	**I**
9	00 00 11 00 00	11 01 11 01 01	1111	σ_y
10	00 00 00 10 00	10 01 00 10 00	1000	σ_z
11	00 00 00 01 00	00 00 00 01 00	0010	**I**
12	00 00 00 11 00	10 01 00 11 00	1010	σ_z
13	00 00 00 00 10	00 00 00 00 01	0001	**I**
14	00 00 00 00 01	01 11 01 00 10	1100	σ_x
15	00 00 00 00 11	01 11 01 00 11	1101	σ_x

matrix equation

$$w^{(i)} = \mathbf{M} e_r^{(i)}, \tag{3}$$

provided that the mapping is confined to $w^{(0)} = e_r^{(0)} (= 00\,00\,00\,00\,00)$. The four error syndromes, $e_r^{(3k)}$, $e_r^{(3k-1)}$, $e_r^{(3k-2)}$ and $e_r^{(0)}$, corresponding to a common erroneous pair, form a group and are characterized by

$$e_r^{(3k-2)} \oplus e_r^{(3k-1)} = e_r^{(3k)}, \qquad k = 1, 2, \ldots, 5, \tag{4}$$

where k enumerates the erroneous pair and $\oplus$ is the addition modulo 2. Accordingly, the 16 codewords $w^{(i)}$ should be subdivided into five corresponding groups, each of which has $w^{(3k)}$, $w^{(3k-1)}$, $w^{(3k-2)}$ and $w^{(0)}$, and holds the relation

$$w^{(3k-2)} \oplus w^{(3k-1)} = w^{(3k)}, \qquad k = 1, 2, \ldots, 5. \tag{5}$$

Therefore the matrix $\mathbf{M}$ can be simply expressed by a 10×10 matrix, such as

$$\mathbf{M} = \left[w^{(1)} w^{(2)} w^{(4)} w^{(5)} w^{(7)} w^{(8)} w^{(10)} w^{(11)} w^{(13)} w^{(14)} \right], \tag{6}$$

in accordance with the arrangement of error syndromes listed in table 1. The first two rows of $\mathbf{M}$ represent the states of the pair to be recovered, and the 4th, 6th, 8th and 10th rows represent

the low bits of the second to fifth Bell states and thus construct the four-bit codewords for the measurement results $v^{(i)}$. The measurement result $v^{(i)}$ of course is also characterized by

$$v^{(3k-2)} \oplus v^{(3k-1)} = v^{(3k)}, \qquad k = 1, 2, \ldots, 5, \tag{7}$$

in accordance with relations (4) and (5). In the language of linear algebra, the action of the sequence of unilateral and bilateral unitary operations that accounts for the mapping $e_r^{(i)} \rightarrow w^{(i)}$ is to perform a sequence of elementary row operations on the 10×10 identity matrix $\mathbf{1}$ to reduce it to the matrix $\mathbf{M}$. In this spirit, Bennett *et al* [5] have undertaken a Monte Carlo numerical search program to find suitable solutions for matrix $\mathbf{M}$ and their corresponding encoder–decoder networks. Basically, the approach implemented by Bennett *et al* is a tedious numerical method of trial and error performing the transformation $\mathbf{1} \rightarrow \mathbf{M}$ subjected to a 'forward' sequence of local operations. In this work, we will present an analytical method for creating $\mathbf{M}$ implemented in the present QECC. The present method will be described in detail in section 3.

3. The present method

3.1. Theory

The unilateral and bilateral unitary operations performed in the 1-EPP in fact are their own inverse transformations, so if the sequence of operations is run in the reverse order, then the inverse transformations $\mathbf{M} \rightarrow \mathbf{1}$ are accomplished. In the spirit of inverse transformation, it thus allows us to derive all appropriate versions of $\mathbf{M}$ and the corresponding encoder–decoder networks by following an analytical way. More importantly, for a derived $\mathbf{M}$, rearranging the sequence of row operations on the same inverse transformation $\mathbf{M} \rightarrow \mathbf{1}$ will help in constructing its simplest encoder–decoder network.

An elementary row operation corresponds to a basic unilateral or bilateral unitary operation. In the present protocol, Alice and Bob are confined to perform only three basic unitary operations because these operations are necessary and sufficient for the elementary row operations needed to achieve the mapping $\mathbf{M} \rightarrow \mathbf{1}$, and vice versa. These basic operations are: (i) a bilateral CNOT (BXOR), which performs the bit change $(x_S,\ y_S)(x_T, y_T) \rightarrow (x_S \oplus x_T,\ y_S)(x_T, y_S \oplus y_T)$, where the subscripts S and T denote the source and target pairs, respectively; (ii) a bilateral $\pi/2$-rotation B_y, which performs $(x,\ y) \rightarrow (y, x)$; and (iii) a composite operation $\sigma_x B_x$, which performs $(x,\ y) \rightarrow (x, x \oplus y)$. The unitary Pauli operation σ_x performs a π-rotation of Alice or Bob's spin about the x-axis, while the bilateral operation B_x (B_y) performs a $\pi/2$-rotation of both Alice and Bob's spins about the x (y)-axis. The unilateral operations are defined as those operators performed by Alice or Bob but not both. The bilateral operations are represented by a tensor product of one part of Bob and the same part of Alice. Note that the bilateral CNOT is performed such that the source qubits of Alice and Bob belong to a common pair, and the target qubits belong to another common pair.

The information obtained through local measurements and one-way communications can only deduce the low bit of a Bell pair, and the original state of the first Bell pair can only be recovered by the low-bit information. Then, for a successful 1-EPP, or its equivalent QECC, each and every measurement result $v^{(i)}$ is required to be distinguishable from the others, so

the collection of $v^{(i)}$ in fact should contain all elements in the four-dimensional Boolean-valued space. To perform the aforementioned inverse transformation $\mathbf{M} \to \mathbf{1}$, the codewords of measurement result are first arranged according to relations (7) and the matrix $\mathbf{M}$ can be assumed as

$$\mathbf{M} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 & c_{10} \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_9 & f_{10} \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{8}$$

It should be noted that the arrangement of the results of measurements shown in the above matrix is only one of the possible choices. By performing a sequence of row operations corresponding to the basic unitary operations, the assumed matrix $\mathbf{M}$ (8) actually is allowed to be reduced to one of all the alternatives akin to the identity matrix $\mathbf{1}$, and a suitable encoder–decoder network is constructed accordingly. The alternatives akin to the identity $\mathbf{1}$ are those obtained by (1) permuting column vectors within one of the five sets of two column vectors ($x^{(3k-2)}$ and $x^{(3k-1)}$, $k = 1, 2, \ldots, 5$), or (2) adding one column to the other within each of the groups, or (3) performing both actions. For example, an alternative could be

$$\mathbf{1}_{\text{akin}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{9}$$

When the derivation of $\mathbf{M}$ is done, the alternative akin to $\mathbf{1}$ is then converted back to the identity $\mathbf{1}$ by well rearranging its columns and the derived $\mathbf{M}$ is adjusted via the same column changes, in order to conform to equation (3). The procedure of reducing the matrix $\mathbf{M}$ to the alternative akin to the identity $\mathbf{1}$ is similar to the Gauss–Jordan elimination method for solving systems of linear equations. During the procedure of row operations, all the unknowns appearing in the assumed matrix $\mathbf{M}$ (8) are given or solved according to the structure of the alternative akin to $\mathbf{1}$. Details of the derivation can be found in [12].

3.2. A systematic scenario example

There are so many solutions for the assumed **M** which are all suitable for the 1-EPP; however, only one of them has been adjusted and presented as:

$$\mathbf{M_1} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & b_9 & b_{10} \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 & c_{10} \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8 & d_9 & d_{10} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_9 & f_{10} \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{10}$$

Let us show the systematic scenario for accomplishing the transformation $\mathbf{M_1} \to \mathbf{1}$ by one of the simplest networks. The matrix $\mathbf{M_1}$ can be rephrased as

$$\mathbf{M_1} = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{15} \\ m_{21} & m_{22} & \cdots & m_{25} \\ \vdots & \vdots & & \vdots \\ m_{51} & m_{52} & \cdots & m_{55} \end{bmatrix}, \tag{11a}$$

where the matrix elements $m_{\alpha\beta}$ denote the 2×2 matrices:

$$m_{11} = \begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}, \qquad m_{21} = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}, \ldots, \tag{11b}$$

and so forth. The next step of our method is a procedure of elementary row operations on the matrix $\mathbf{M_1}$ (10) subjected to a suitable sequence of the basic operations. When the assumed matrix $\mathbf{M_1}$ is transformed into the identity matrix **1** under the series of row operations, the unknowns a_r, $b_r, \ldots, f_r$ will be solved stepwise in accordance with the structure of **1**. It is easy to show that a sequence of row operations can do the transformation on two Bell states α and β in a group enumerated by γ, namely,

$$\begin{bmatrix} m_{\alpha\gamma} \\ m_{\beta\gamma} \end{bmatrix} \to \begin{bmatrix} \mathbf{I} \\ 0 \end{bmatrix}, \tag{12}$$

provided that $\det(m_{\alpha\gamma}) = 1$ and $\det(m_{\beta\gamma}) = 0$. Here $\mathbf{I}$ denotes the 2×2 identity matrix. For example, the consecutive transformation

$$\begin{bmatrix} m_{\alpha\gamma} \\ m_{\beta\gamma} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

can be accomplished if the operation B_y is first performed on Bell state β, then a $\sigma_x B_x$ is performed on Bell state α followed by a BXOR performed on both states, as Bell state α being the source and Bell state β being the target. It can be found in what follows that the unknowns assumed in the matrix $\mathbf{M_1}$ either will be given based on the requirement for the transformation described in (13), or will be determined according to the unique structure of the identity matrix $\mathbf{1}$.

In the first stage of row operations, we are confined to performing a transformation of the matrix $\mathbf{M_1}$ (11a) such that $m_{44} \to \mathbf{I}$ and $m_{4k}, m_{k4} \to 0$, for $k = 1, 2, 3$ and 5, according to the structure of $\mathbf{1}$. Let $\det(m_{44}) = 1$ and $\det(m_{14}) = \cdots = \det(m_{54}) = 0$, which imply

$$a_7 b_8 \oplus a_8 b_7 = 0, \qquad c_8 = 0, \qquad e_7 = 1; \qquad c_7, d_7, d_8, e_8, f_7, f_8 \in \{0, 1\}. \tag{13}$$

Clearly, there are totally 640 solutions for the unknowns appearing in (10) to be considered in this stage (ten for the condition $a_7 b_8 \oplus a_8 b_7 = 0$, two for each of the six arbitrary Boolean valued unknowns, and thus totally $10 \times 2^6 = 640$ solutions). To illustrate the simplest way of creating Boolean functions, however, only one among these 640 cases is considered. Let us consider the case in which

$$a_7 = 1, \qquad b_7 = a_8 = b_8 = c_7 = d_7 = d_8 = e_8 = f_7 = f_8 = 0. \tag{14}$$

Then, by performing the operations shown in figure 2(a), we have the transformation $\mathbf{M_1} \to \mathbf{M_1'}$,

$$\mathbf{M_1'} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 & 0 & a_9 & a_{10} \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & 0 & 0 & d_9 & d_{10} \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & 0 & 0 & f_9 & f_{10} \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} m_{11}' & m_{12}' & m_{13}' & 0 & m_{14}' \\ m_{21}' & m_{22}' & m_{23}' & 0 & m_{25}' \\ m_{31}' & m_{32}' & m_{33}' & 0 & m_{35}' \\ 0 & 0 & 0 & \mathbf{I} & 0 \\ m_{51}' & m_{52}' & m_{53}' & 0 & m_{55}' \end{bmatrix}, \tag{15}$$

in which we have chosen the following setting for the unknowns:

$$\begin{aligned} &b_1 = 1, \quad b_2 = 1, \quad b_3 = 0, \quad b_4 = 0, \quad b_5 = 1, \quad b_6 = b_9 = 0, \quad b_{10} = 1, \\ &c_1 = 0, \quad c_2 = c_3 = 0, \quad c_4 = 1, \quad c_5 = c_6 = c_9 = 0, \quad c_{10} = 1, \text{ and} \\ &e_1 = e_2 = e_3 = e_4 = e_5 = e_6 = e_9 = e_{10} = 0. \end{aligned} \tag{16}$$

Let us proceed to apply the second series of operations, as depicted in figure 2(b), to perform the transformations $m_{22}' \to \mathbf{I}$ and $m_{2k}', m_{k2}' \to 0$, for $k = 1$, 3 and 5. As a result, we have

$$\begin{aligned} &d_1 = f_1 = d_2 = f_2 = 0, \qquad d_3 = d_4 = f_3 = f_4 = 0, \qquad d_5 = 1, \\ &d_6 = 0 = f_5 = f_6 = 0, \qquad d_9 = f_9 = d_{10} = 0, \qquad f_{10} = 1, \qquad a_3 = a_4 = 0. \end{aligned} \tag{17}$$

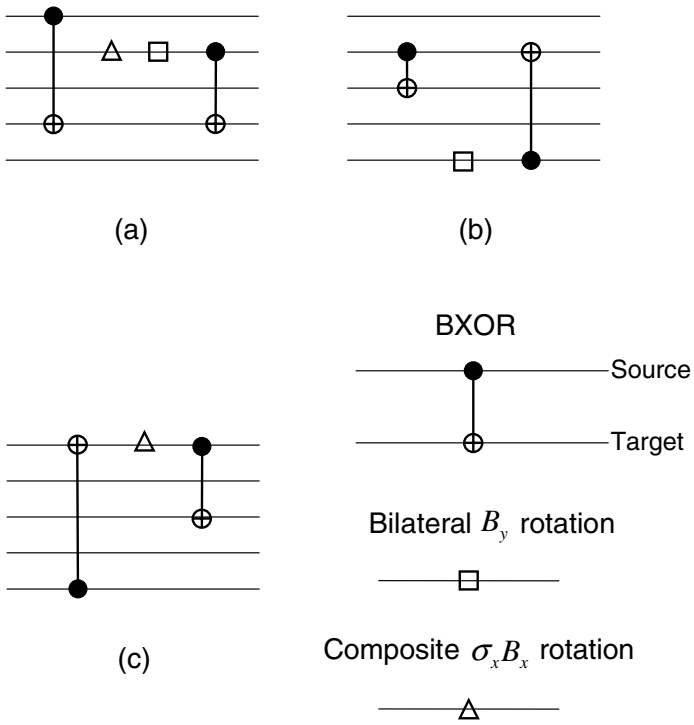


Figure 2. The three quantum gate arrays performed in the stage of row operations: (a) for $\mathbf{M_1} \rightarrow \mathbf{M_1'}$; (b) for $\mathbf{M_1'} \rightarrow \mathbf{M_1''}$; and (c) for $\mathbf{M_1''} \rightarrow \mathbf{1}$.

Note that according to the requirements $\det(m'_{2k}) = 0$ and $\det(m'_{k2}) = 0$, $a_3 = a_4 = 0$ is only one of the suitable choices and $d_3 = d_4 = 0$ is the only choice. Therefore, the $\mathbf{M_1'}$ is transformed into $\mathbf{M_1''}$:

$$\mathbf{M_1''} = \begin{bmatrix} a_1 & a_2 & 0 & 0 & a_5 & a_6 & 0 & 0 & a_9 & a_{10} \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} m''_{11} & 0 & m''_{13} & 0 & m''_{14} \\ 0 & \mathbf{I} & 0 & 0 & 0 \\ m''_{31} & 0 & m''_{33} & 0 & m''_{35} \\ 0 & 0 & 0 & \mathbf{I} & 0 \\ m''_{51} & 0 & m''_{53} & 0 & m''_{55} \end{bmatrix}. \tag{18}$$

Finally, if the matrix $\mathbf{M_1''}$ is transformed through additional two BXOR and one $\sigma_x B_x$ operations, as shown in figure 2(c), it results in the identity matrix $\mathbf{1}$. In this stage, we have set the rest of the unknowns to be one of the alternatives: $a_1 = 1$, $a_2 = 0$, $a_5 = 1$, $a_6 = 0$, $a_9 = 0$ and $a_{10} = 0$. The whole sequence of basic operations, as shown in figure 3, is obtained by combining the three subsequences as shown in figures 2(a)–(c). It will transform the matrix $\mathbf{M_1}$ into the identity matrix $\mathbf{1}$. This network is the simplest one since it involves only six BXORs,

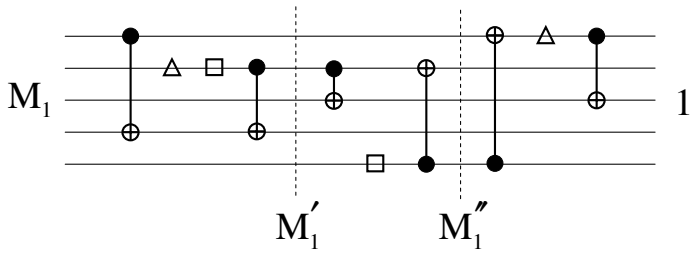


Figure 3. The gate array for the transformation $\mathbf{M}_1 \rightarrow \mathbf{1}$. The basic unitary operations are performed in the order from left to right, while if they are performed from right to left, then the inverse transformation $\mathbf{M_1} \rightarrow \mathbf{1}$ is accomplished.

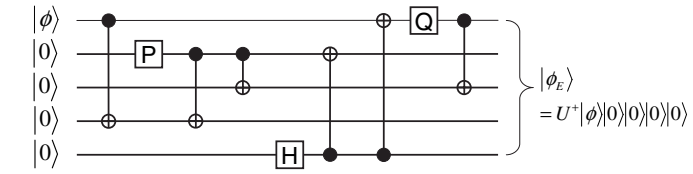
and the corresponding matrix reads

$$\mathbf{M_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{19}$$

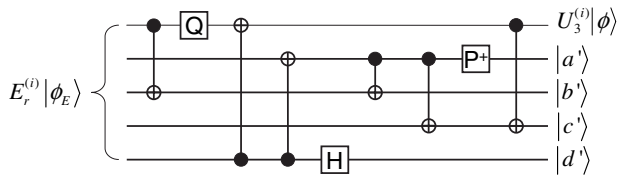
Performed by this network, the correspondence between the error syndromes $e_r^{(i)}$ and the combined measurement results $v_r^{(i)}$ is also listed in table 1. Referring to table 1, or the matrix $\mathbf{M}_1$, when Bob obtains the measurement result $v^{(2)}(= 0110)$, for example, he knows the pair to be purified is in the state $\Psi^+(= 01)$ and thus simply performs the Pauli operation $U_3^{(2)} = \sigma_x$ to recover it to the good state Φ^+.

4. The encoder–decoder circuit for a perfect five-qubit error correction

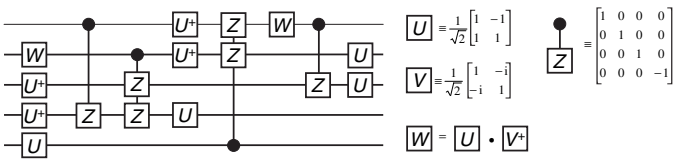
The 1-EPP depicted above can be directly converted to a five-qubit QECC whose encoder–decoder circuit has the same configuration as the one shown in figure 4. However, in the language of QECC, the classical high–low or phase–amplitude bits used to code the Bell state in the 1-EPP are now used to code operators belonging to the Pauli group, namely, $\mathbf{I} = 00$, $\sigma_x = 01$, $\sigma_z = 10$, $\sigma_y = 11$. When acting on a single qubit, the Pauli operator produces either no error (by $\mathbf{I}$), a bit flip error (by σ_x), a phase flip error (by σ_z), or a bit-phase flip error (by σ_y). Therefore, such a code is convenient because the codewords $e_r^{(i)}$ are now replaced by $E_r^{(i)}$, which represent the 16 error syndromes described by five-Pauli-operartor tensor products. Furthermore, the transformation described by the matrix equation (3) is now replaced by the similarity transformation of operators described as: $W^{(i)} = UE_r^{(i)}U^+$, where U (U^+) represents the sequence of the basic operations performed in the decoder (encoder) circuit. Clearly, both the encoder and decoder circuits have exactly the same quantum gate arrangement but they



(a) The operation of encoder circuit



(b) The operation of decoder circuit



(c) The operation of encoder circuit for ion-trap quantum computers

Figure 4. The perfect five-qubit error correction. (a) The initial tensor product state is encoded to an entangled state $|\phi_E\rangle$. (b) After suffering from the single-qubit error, the state $E_r^{(i)}|\phi_E\rangle$ is then decoded, resulting in the final tensor product state $(U_3^{(i)}|\phi\rangle)|a'b'c'd'\rangle$. Here, $\mathbf{P} = HQ$, $\mathbf{P}^+ = QH$. (c) The encoder circuit from (a) is rewritten in terms of the gate primitives of an ion-trap quantum computer.

should be run in opposite orders. In order to perform the transformation mentioned above, this time the single-qubit Hadamard transformation: $H = H^+ = (\sigma_x + \sigma_z)/\sqrt{2}$, is used to perform the bit change $H(x, y)H^+ \rightarrow (y, x)$, the single-qubit transformation: $Q = Q^+ = (\sigma_y + \sigma_z)/\sqrt{2}$, is used to perform $Q(x, y)Q^+ \rightarrow (x, x \oplus y)$, and the two-qubit CNOT gate is used to perform $(\mathrm{CNOT})(x_\mathrm{S}, y_\mathrm{S})(x_\mathrm{T}, y_\mathrm{T})(\mathrm{CNOT})^+ \rightarrow (x_\mathrm{S} \oplus x_\mathrm{T}, y_\mathrm{S})(x_\mathrm{T}, y_\mathrm{S} \oplus y_\mathrm{T})$, respectively. That is, in the five-qubit QECC to be presented, the basic single- and two-qubit operations needed to be implemented are H, Q and CNOT.

For the present five-qubit QECC, the correspondence between the codewords $W^{(i)}$ and $E_r^{(i)}$ is exactly the same as that between the derived matrix $\mathbf{M}_1$ given in (9) and the identity $\mathbf{1}$. The QECC is performed as follows. If a state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ is to be protected in a quantum computation, it is first accompanied with four extra qubits in the state $|0\rangle$. Then the five-qubit state $|\phi\rangle|0\rangle|0\rangle|0\rangle|0\rangle$ is encoded by the performance of U^+. After the encoded state is subjected to $E_r^{(i)}$, the erroneous state then is decoded by the implementation of U. The resulting state turns out to be

$$\left|\phi_r^{(i)}\right\rangle = UE_r^{(i)}U^+(|\phi\rangle|0\rangle|0\rangle|0\rangle|0\rangle) = W^{(i)}(|\phi\rangle|0\rangle|0\rangle|0\rangle|0\rangle) = (U_3^{(i)}|\phi\rangle)\left|a'\right\rangle\left|b'\right\rangle\left|c'\right\rangle\left|d'\right\rangle, \tag{20}$$

where $U_3^{(i)}$ is the single-qubit Pauli operation acting on the first qubit and is dependent on the measurement result on the four extra qubits. When the extra qubits are measured in

the computational basis, the measurement result $v^{(i)} = a'b'c'd'$ is obtained. Eventually, the corresponding Pauli operation $U_3^{(i)}$ is performed on the remaining qubit, which is in the state $U_3^{(i)}|\phi\rangle$, to recover the initial state $|\phi\rangle$. The procedure of performing the five-qubit QECC is quite simple, same as the one reported by Laflamme *et al* [4], and is displayed schematically in figure 4. The present QECC is equivalent to the aforementioned 1-EPP, which adopts the network shown in figure 4, so table 1 is also useful to it. As a result, when referring to table 1 again, if the measurement result $v^{(2)} = 0110$ is read, then $U_3^{(2)} = \sigma_x$ is performed to recover the initial state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. The encoder–decoder circuit required to perform the present QECC, as shown in figures 4(a) and (b), is rather simple; it contains nine operations, in which only six CNOTs are required. As a matter of fact, this circuit is one of the simplest ones derived so far. The other best known circuit is the one presented by Braunstein and Smolin [8] and its corresponding matrix is

$$\mathbf{M}_{\mathrm{BS}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{21}$$

The efficiency of a coding scheme can be characterized by the shortness of the encoder–decoder circuit. The shortness criterion is based on the fewest total operations or the fewest CNOT operations [5]. The total operations include one-qubit rotations and CNOTs. It is equivalent to determine the minimum experimental efforts for implementing the shortest coding circuit on a quantum computer. The number of laser pulses required to perform an encoder–decoder circuit is a reasonable measure of the efficiency for ion-trap computers [8, 13]. A qubit is coded through the ground state and the long-lived excited state of an ion in an ion-trap quantum computer [14]. The physical states are driven by laser beams to implement the quantum logic gates further. To count the number of laser pulses, the encoder circuit from figure 4(a) is rewritten in terms of the gate primitives of an ion-trap quantum computer and shown in figure 4(c). It is interesting to observe that two pairs of CNOTs (the 2nd and 3rd and the 4th and 5th ones) in the present circuit can be combined as two three-qubit gates and can be implemented as single element. Besides, the functions of operators U and V implemented on an ion-trap quantum computer are equivalent to the ones of operators H and Q, respectively. Since each single-qubit operation requires one laser pulse, the two-qubit gate needs three pulses, and the three-qubit gate requires four laser pulses, the present circuit also requires only 24 laser pulses if it is implemented on an ion-trap quantum computer, same as the Braunstein and Smolin circuit. The numbers of total operations, CNOTs, and laser pulses for the circuits presented by Bennett *et al* [5] and Braunstein and Smolin [8] have also been summarized in table 2.

Table 2. Three efficiency criteria and the corresponding costs for four circuits have been presented. Circuit 1 is given by Bennett *et al* (figure 18 in [5]) and is unoptimized. The optimized circuit of Bennett *et al* denoted by Circuit 2, mentioned in [5], consists of six two-qubit controlled-NOT gates only. Since the number of laser pulses depends on the detailed structure of the circuit, it is not shown here for laking the detailed information. Circuit 3 is the simplification of the coding circuit of Laflamme *et al* proposed by Braunstein and Smolin (figure 1 in [8]). One can find that the original circuit of Laflamme *et al* (figure 1 in [4]) is more complicated and requires 41 laser pulses. Circuit 4 denotes the simpest circuit which has been found by computer search (figure 3 in [8]) and by the systematic method presented in this work.

Criteria	Circuit 1	Circuit 2	Circuit 3	Circuit 4
Total number of operations	12	11	10	9
Number of CNOTs	7	6	7	6
Number of laser pulses	35	—	26	24

5. Conclusion

This work has presented a rather simple encoder–decoder circuit to perform the five-qubit, single-error correction protocol. The QECC derived herein is converted directly from the restricted 1-EPP depicted above, so a major part of this work is dedicated to the depiction of the 1-EPP. The present encoder–decoder circuit is the simplest one corresponding to the derived matrix $\mathbf{M_1}$ given in (20), which is derived via an analytical approach [12]. This analytical approach, as shown, can help in deriving not only the suitable matrix $\mathbf{M}$ for the five-qubit QECC but also the simplest version of encoder–decoder network corresponding to the derived matrix. However, many possible matrices $\mathbf{M}$ suitable for the QECC remain to be discovered analytically and, thus, so many candidates of encoder–decoder circuit that require only six CNOTs. The simplest network that is even simpler than the present one and the Braunstein and Smolin circuit [8] might not be found from these candidates. However, a more convincing proof which could be a numerical approach based on the analytical approach introduced in [12] is required in future work.

Acknowledgments

This work is supported partially by the National Science Council, Taiwan under the grant numbers NSC 94-2212-E-159-002 and NSC 94-2112-M-009-024.

References

[1] Bennett C H and DiVincenzo D P 2000 *Nature* (London) **404** 247
Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Knill E and Laflamme R 1997 *Phys. Rev.* A **55** 900
[3] Ekert A and Macchiavello C 1996 *Phys. Rev. Lett.* **77** 2585

[4] Laflamme R, Miquel C, Paz J P and Zurek W H 1996 *Phys. Rev. Lett.* **77** 198
[5] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 *Phys. Rev.* A **54** 3824
[6] Gottesman D 1996 *Phys. Rev.* A **54** 1826
Gottesman D 1997 *PhD Thesis* California Institute of Technology, Pasadena, CA
[7] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1997 *Phys. Rev. Lett.* **78** 405
[8] Braunstein S L and Smolin J A 1997 *Phys. Rev.* A **55** 945
[9] Knill E, Lafamme R, Matrtinez R and Negrevergne C 2001 *Phys. Rev. Lett.* **86** 5811
[10] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H 1995 *Phys. Rev.* A **52** 3457
[11] Steane A M 1996 *Phys. Rev. Lett.* **76** 793
[12] Hsieh J-Y and Li C-M 2004 *Preprint* quant-ph/0405038
[13] Beckman D, Chari A N, Devabhaktuni S and Preskill J 1996 *Phys. Rev.* A **54** 1034
[14] Cirac J I and Zoller P 1995 *Phys. Rev. Lett.* **74** 4091