IMPLEMENTATION OF UNITARY QUANTUM ERROR CORRECTION

HIROYUKI TOMITA

Research Center for Quantum Computing, Kinki University,
Higashi-Osaka, 577-8502, Japan
E-mail: tomita@alice.math.kindai.ac.jp

A short survey on quantum error correction (QEC) except for the recent fashion such as so-called surface-code is presented. Most of the standard QEC theory developed in the last twenty years have features of the process of error syndrome measurements with use of subsidiary ancilla qubits and non-unitary correcting process. Recently, we re-discovered a unitary error correction without error syndrome detection scheme.[1,2] Though this method is found in the earlier works on QEC,[3,4] it has not been referred in most of the textbooks on QEC.[5–8] Of course, if this unitary QEC system can actually be implemented with simple physical circuits, this must be advantageous for the usual syndrome detecting method. Its usefulness is shown by applying it to a fully correlated error.

Keywords: Quantum error correction; Unitary correction

1. Classical Error Correction (CEC)

The bit-flip error $(0 \leftrightarrow 1)$ on a classical bit is corrected by encoding it together with some redundant ancilla bits and decoding the error code based on the *majority* principle. Assuming the bit-flip error occurs with a small probability p on at most only one bit in the encoded assembly of the data bit and the ancilla bits, a codeword composed with three bits is sufficient to correct it. An example of the simplest codeword to realize this correction process is given as follows:

$$\begin{array}{ccccccccc} \text{data-bit} & & \text{encode} & & \text{error-code} & & \text{majority-rule} & & \text{decode} \\ 0 & \rightarrow & 000 & \rightarrow & \{100,\ 010,\ 001\} & \rightarrow & 000 & \rightarrow & 0 \\ 1 & \rightarrow & 111 & \rightarrow & \{011,\ 101,\ 110\} & \rightarrow & 111 & \rightarrow & 1 \end{array}$$

Thus it is clear that three-bit encoding is enough so that the sets of error codes originated from the initial data bit 0 or 1 are completely separated and can be corrected with accuracy of $O(p^2)$ by using the majority rule.

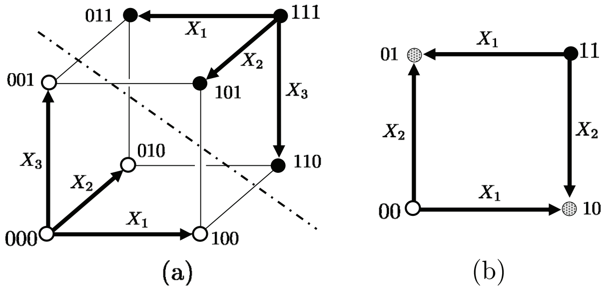

Fig. 1. (a)An image[5] of the Hamming distance (=3) of the 3-bit encoding system for the bit-flip error, where X_i denotes the bit-flip error on the i-th bit. (b)Two-bit encoding does not have a sufficient distance for the error codes to be separated.

It can be shown that an n-bit codeword is sufficient for k data bits to be corrected, where n must satisfy the condition $2^n \geq 2^k(n+1)$. Here, 2^k is the number of independent binary states of k classical bits and $n+1$ is the number of distinguishable errors including 'no-error'. Generally if the error occurs on at most m bits, we need $2^n \geq 2^k \sum_{i=0}^{m} {}_iC_n$. For example, we need $n = 2m+1$ to correct one data bit ($k=1$) by using the majority rule. The minimal condition for the correctable codeword is expressed by the Hamming distance (Fig.1).

2. Quantum Error Correction (QEC)

The principle of conventional QEC is almost the same as that of CEC, if we interpret the classical bit 0 or 1 as the qubit state $|0\rangle$ or $|1\rangle$, respectively, except for the following facts:

1) A superposed input data of $|0\rangle$ and $|1\rangle$ is acceptable in QEC.
2) Then, any observation destroying the superposed state is not permitted in encoding and decoding (or correcting) processes.
3) There is a phase-flip error peculiar to the quantum system in addition to the bit-flip error.

2.1. *Quantum bit-flip error*

The quantum bit-flip operation is defined by

$$X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle,$$

that is, the NOT operation described by a Pauli matrix,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let us denote this bit-flip operator acting on the i-th qubit by X_i. For example,

$$X_1 = X \otimes I \otimes I,\ X_2 = I \otimes X \otimes I,\ X_3 = I \otimes I \otimes X,$$

for the three qubit system, where I is the 2-dimensional identity matrix I_2.

The Hamming distance is just the same as that in CEC, i.e. we need three qubits for the bit-flip error correction of one data-qubit. The encoding process is given by

$$|0\rangle \to |000\rangle \quad \text{and} \quad |1\rangle \to |111\rangle. \tag{1}$$

The encoded pair are called the *logical qubits* and denoted as

$$|0\rangle_{\mathrm{L}} = |000\rangle \quad \text{and} \quad |1\rangle_{\mathrm{L}} = |111\rangle, \tag{2}$$

supposing that a error correctable quantum logical circuits is constructed with them.

In QEC we have to encode without observing the input state $|0\rangle$ or $|1\rangle$, so that a superposed state such as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $(\alpha, \beta \in \mathbb{C})$ is acceptable as an input state, i.e.

$$|\psi\rangle \otimes |00\rangle = \alpha|000\rangle + \beta|100\rangle \to |\Psi\rangle = \alpha|000\rangle + \beta|111\rangle. \tag{3}$$

Note that the encoded state is *entangled*. This encoding process is performed by a unitary operation without any observation in QEC,[7] i.e. two controlled-NOT (CNOT) gates shown in Fig.2.

The encoding operation U_{E}(=CNOTNOT gate) is clear, if it is understood after the classical meaning, i.e. 'If the input state is $|1\rangle$, reverse the

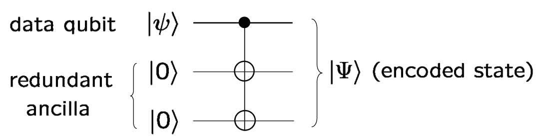

Fig. 2. Unitary encoding operation U_{E} without observation. The small filled circle denotes the controlled qubit, i.e. 'if $|1\rangle$', and the large open circle the NOT operation X on the corresponding qubits.

ancillary qubits state $|00\rangle$ to $|11\rangle$'. In the quantum circuit this logical process is performed without any observation, i.e. as a unitary transformation,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ \beta \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{pmatrix}. \tag{4}$$

That is, the encoding gate is a generator of the logical qubits of Eq.(2). The column vectors of its matrix form except for the first and fifth are arbitrary, at least if the matrix itself is unitary.

Each bit-flip error X_i is a unitary operation acting on the encoded state $|\Psi\rangle$ as $X_i|\Psi\rangle = |\Psi'\rangle$ including the no-error case $X_0 = I_8$. The output state $|\Psi'\rangle$ is given by

$$|\Psi'\rangle = \begin{cases} \alpha|000\rangle + \beta|111\rangle & \text{for } X_0 \text{ (no error)}, \\ \alpha|100\rangle + \beta|011\rangle & \text{for } X_1, \\ \alpha|010\rangle + \beta|101\rangle & \text{for } X_2, \\ \alpha|001\rangle + \beta|110\rangle & \text{for } X_3. \end{cases} \tag{5}$$

However, which error occurred, if any, is unknown. That is, the error channel is described as a stochastic process with probability $\{p_i\}$ and its output is a mixed state in general. Error correction is performed by detecting the

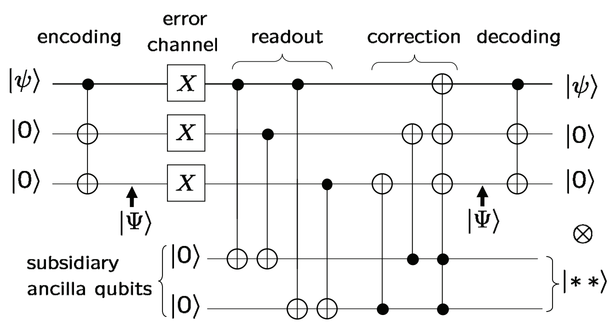

Fig. 3. A standard bit-flip error correction process with detecting the error states.[7] The correction process may be replaced by a physical measurement of the ancilla states and surgery on the above three qubits referring the measured value.

output state $|\Psi'\rangle$ with the use of subsidiary ancilla qubits for readout as is shown in Fig.3. The error syndrome of the subsidiary ancilla states shown by $|**\rangle$ in Fig.3 after readout of $|\Psi'\rangle$ is given by

$$\begin{array}{lll} |00\rangle & \text{for} & \alpha|000\rangle + \beta|111\rangle \quad \text{(no error)}, \\ |11\rangle & \text{for} & \alpha|100\rangle + \beta|011\rangle, \\ |10\rangle & \text{for} & \alpha|010\rangle + \beta|101\rangle, \\ |01\rangle & \text{for} & \alpha|001\rangle + \beta|110\rangle, \end{array} \tag{6}$$

respectively. The state of the subsidiary ancillae can be any one of these four with some probability, and *not* a superposed state. Note that this readout process itself never spoils the superposition brought by the input state $|\psi\rangle$.

Now let us introduce a unitary correction without detecting the error syndrome. First, if we operate the decoding operator, i.e. the inverse of the encoding operator U_{E}(=CNOTNOT), on the error state $|\Psi'\rangle$ given by Eq.(5), it can be easily found that

$$|\Psi'\rangle = \begin{cases} \alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|000\rangle + \beta|100\rangle, \\ \alpha|100\rangle + \beta|011\rangle \rightarrow \alpha|111\rangle + \beta|011\rangle, \\ \alpha|010\rangle + \beta|101\rangle \rightarrow \alpha|010\rangle + \beta|110\rangle, \\ \alpha|001\rangle + \beta|110\rangle \rightarrow \alpha|001\rangle + \beta|101\rangle. \end{cases} \tag{7}$$

Note that the decoded states have no entanglement now, though the first qubit is reversed in the second line (the case of X_1-error) yet. This mismatch can be corrected by a NOT-controlled-controlled gate, i.e. 'Flip the first qubit, only if the second and the third qubit state is $|11\rangle$'. This operation is performed by a CCNOT gate (Fig.4), a kind of the so-called *Toffoli* gate.

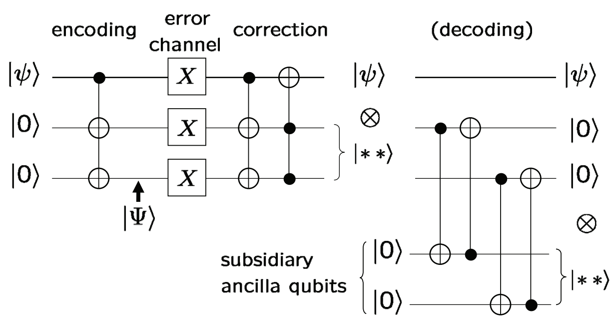

Fig. 4. A unitary error correction without detecting the error syndrome. If we need the complete initial states, we may use the subsidiary ancillae to reset the encoding ancillae by swapping. Then we obtain the same final state as Fig.3.

After this CCNOT operation we find,

$$|\Psi'\rangle \;\rightarrow\; |\psi\rangle \otimes |**\rangle. \tag{8}$$

The data qubit has been recovered in all cases. The ancilla state $|**\rangle$ represents the error syndrome depending on where the bit-flip error occurred (or did not occur), which was detected by using the subsidiary ancilla in the previous method. Some non-unitary process is necessary to recover it to the initial state. However, we need not to know it at least for the purpose of error correction of the data qubit, because Eq.(8) has a direct product form and the data qubit state can be extracted safely discarding the ancilla. [a]

The advantages of the unitary correction become clearer if we use the operator QEC formulation.[1,2] In this formulation the initial and the encoded states are given by density operators,

$$\rho_0 = |\psi\rangle\langle\psi| \otimes |00\rangle\langle 00|, \quad (\ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle\ ), \tag{9}$$

and

$$\rho = U_{\mathrm{E}}\rho_0 U_{\mathrm{E}}^{-1} = (\alpha|000\rangle + \beta|111\rangle)(\alpha^*\langle 000| + \beta^*\langle 111|), \tag{10}$$

respectively. Note that both are pure states and the latter is entangled. The stochastic noisy error channel is defined by a superoperator form,

$$\rho' = \sum_{i=0}^{3} p_i (X_i \rho X_i), \tag{11}$$

where $X_0 (= I)$ denotes 'no error' and $p_0 = 1 - \sum_{i=1}^{3} p_i$, if we assume the bit-flip error occurs on at most only one qubit. Thus the error state is a mixed state in general. Let us denote the recovery operator composed with a CNOTNOT gate and a CCNOT gate by U_{R}. Then the corrected state is given by a tensor product form,

$$\tilde{\rho} = U_{\mathrm{R}}\rho' U_{\mathrm{R}}^{-1} = |\psi\rangle\langle\psi| \otimes \rho'_{\mathrm{a}}, \tag{12}$$

where

$$\begin{aligned} \rho'_{\mathrm{a}} &= p_0|00\rangle\langle 00| + p_1|11\rangle\langle 11| + p_2|10\rangle\langle 10| + p_3|01\rangle\langle 01| \\ &= \begin{pmatrix} p_0 & 0 & 0 & 0 \\ 0 & p_3 & 0 & 0 \\ 0 & 0 & p_2 & 0 \\ 0 & 0 & 0 & p_1 \end{pmatrix}. \end{aligned} \tag{13}$$

[a] If we want to recover the complete initial state including the encoding ancilla, we may use the two subsidiary ancilla set $|00\rangle$ to reset the encoding ancilla as is shown in the right-half part of Fig.4, and encode it again if the encoded state $|\Psi\rangle$ is wanted.

Extracting the data qubit state means merely computing the partial trace over the ancilla states using $\mathrm{Tr}\rho'_{\mathrm{a}} = 1$ in this formulation. The process of partial trace is a kind of projection and is non-unitary.

2.2. *Phase-flip error*

There are other types of error on the qubit, i.e. the phase-flip error and the bit-and-phase-flip error. These operations are defined by

$$Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle \ \text{ and } \ Y|0\rangle = |1\rangle,\ Y|1\rangle = -|0\rangle.$$

They are also described by Pauli matrices as

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ \text{ and } \ Y = -i\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

respectively. Note that $Y = XZ$. The notations $\{Z_i\}$ and $\{Y_i\}$ are used in the same meaning as $\{X_i\}$.

In the case of the phase-flip errors only, the process of encoding and correction is almost the same as that for the bit-flip case, if one uses the Hadamard transformations, $HZH = X$ (and $HYH = -Y$), where H is the Hadamard operator given by

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Application of this fact to the general case of (X, Y, Z)-error is straightforward in Shor's nine-qubit QEC.[9] The details are skipped and shown in Fig.6 only. After the bit-flip correction the entanglement within each three qubit group is coming untied and a direct product state $|\Psi_{147}\rangle \otimes |{*}{*}{*}{*}{*}{*}\rangle$ is resulted, where $|\Psi_{147}\rangle$ is an entangled state of the 1^{st}, 4^{th} and 7^{th} qubits.

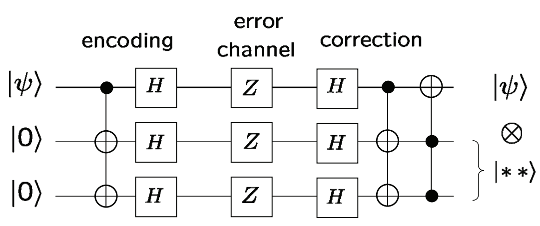

Fig. 5. The phase-flip error correction.[3]

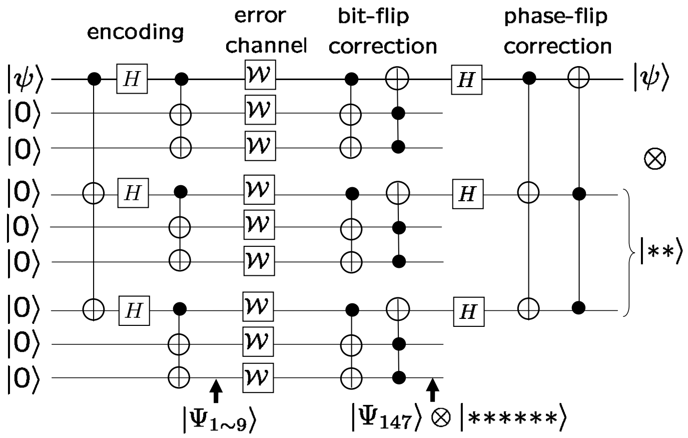

Fig. 6. The unitary version[1] of Shor's 9-qubit QEC for the general (X, Y, Z)-error. The notation $\mathcal{W}$ denotes one of the X, Y and Z operations. We assume again an error occurs on at most one of nine qubits. The encoded state $|\Psi_{1\sim 9}\rangle$ is an entangled state over all nine qubits and $|\Psi_{147}\rangle$ is that over the $1^{\rm st}$,$4^{\rm th}$ and $7^{\rm th}$ qubits.

2.3. *The method of stabilizer*

The sufficient Hamming distance is realized with $n = 5$ for the general (X, Y, Z)-error, because $2^n \geq 2^k(3n + 1)$ gives $n \geq 5$ for $k = 1$, where $3n$ is the number of distinguishable errors in this case. However, how to encode the logical qubits is not so trivial compared with the bit-flip error. We have a powerful tool, the so called *stabilizer* method applicable for this purpose.

Let $\{W_k\}$ be the set of error operators concerned in a given qubit system. A set of commutative operators $\{S_j\}$ satisfying the following properties is called a stabilizer set for QEC:

1. Each S_j satisfies $S_j^2 = I$, i.e. its eigenvalues are ± 1.
2. Each W_k is either commutative or anti-commutative with all $\{S_j\}$, and anti-commutative with at least one member S_j. And $\{W_k\}$ can be discriminated from one another by this commutativity relations.
3. All $\{S_j\}$ have simultaneous eigenstate(s) with eigenvalue $+1$.

The property 3 corresponds to the logical qubit(s), i.e. the equations

$$S_j|0\rangle_{\rm L} = |0\rangle_{\rm L},\ S_j|1\rangle_{\rm L} = |1\rangle_{\rm L},\ ...., \tag{14}$$

for all S_j characterize the set of logical qubits. From this property the *operator* set composed of $\{S_j\}$ is called a stabilizer set and used as an equivalent substitute for the set of *states* of the logical qubits.

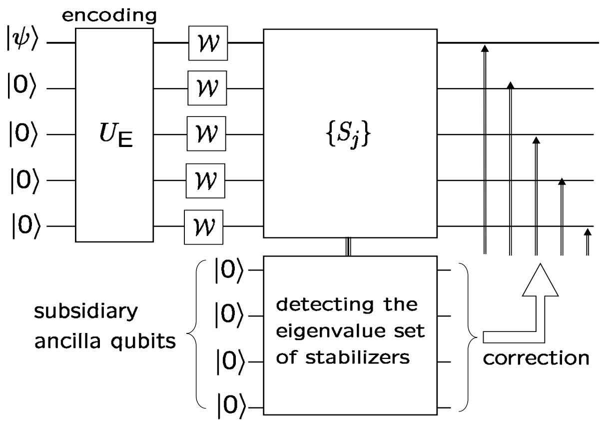

Fig. 7. Five qubit QEC using a stabilizer. The encoding operator $U_{\rm E}$ may be composed by using the stabilizer set so that the corresponding logical qubits are created.

If W_k is anti-commutative with S_j, we have

$$S_j W_k |0\rangle_{\rm L} = -W_k S_j |0\rangle_{\rm L} = -W_k |0\rangle_{\rm L}, \tag{15}$$

and the same relation for $|1\rangle_{\rm L}$. Then the error state $W_k(\alpha|0\rangle_{\rm L} + \beta|1\rangle_{\rm L})$ is an eigenstate of S_j with eigenvalue -1. To the contrary if commutative, the eigenvalue is $+1$. Thus all error states can be discriminated from each other according to the pattern of the eigenvalue set $\{\pm1, \pm1, ...\}$ of the stabilizers and the sufficient Hamming distance is realized automatically.

To ascertain the effect of the stabilizer let us consider the 3-qubit bit-flip QEC, i.e. $\{W_k\} = \{X_1, X_2, X_3\}$. The stabilizer set is not unique. An example of the commutative set is given by $\{S_j\} = \{Z_1Z_2, Z_1Z_3\}$, which have the simultaneous eigenstates $\{|000\rangle,\ |111\rangle\}$ with eigenvalue $+1$. Note that the commutativity $+(-)$ in Table.1 is used for 'commutative' ('anti-commutative') to keep consistency with the sign of the eigenvalues.

(Commutativity)

error	Z_1Z_2	Z_1Z_3
$I^{\otimes 3}$	$+$	$+$
X_3	$+$	$-$
X_2	$-$	$+$
X_1	$-$	$-$

(Eigenvalues)

error states	Z_1Z_2	Z_1Z_3
$\|000\rangle, \|111\rangle$	$+1$	$+1$
$\|001\rangle, \|110\rangle$	$+1$	-1
$\|010\rangle, \|101\rangle$	-1	$+1$
$\|100\rangle, \|011\rangle$	-1	-1

Table. 1. The characteristics of the stabilizer set for 3-qubit bit-flip QEC.

An example of commutative set for the five qubit QEC of the general (X, Y, Z)-error is given by[10]

$$\begin{aligned} S_1 &= iY \otimes Z \otimes I \otimes Z \otimes iY, \\ S_2 &= \ X \otimes Z \otimes Z \otimes X \otimes I, \\ S_3 &= iY \otimes iY \otimes Z \otimes I \otimes Z, \\ S_4 &= \ X \otimes I \otimes X \otimes Z \otimes Z. \end{aligned} \tag{16}$$

Apparently these are commutative and each of fifteen error operators $\{W_k\}$ $= \{X_{1\sim5}, Y_{1\sim5}, Z_{1\sim5}\}$ has a different pattern of commutativity with $\{S_j\}$.

By using relations $S_j(I + S_j) = I + S_j$ $(I = I^{\otimes 5}$, hereafter) it can be easily shown that

$$|0\rangle_{\mathrm{L}} = \frac{1}{\sqrt{8}}(I + S_1)(I + S_2)(I + S_3)(I + S_4)|00000\rangle, \tag{17}$$

and

$$|1\rangle_{\mathrm{L}} = \frac{1}{\sqrt{8}}(I + S_1)(I + S_2)(I + S_3)(I + S_4)|11111\rangle, \tag{18}$$

are the simultaneous eigenstates of $\{S_j\}$ with eigenvalue $+1$, and are orthogonal to each other, because the number of 1's in each binary basis of $|0\rangle_{\mathrm{L}}$ is even while that in $|1\rangle_{\mathrm{L}}$ is odd. (Indeed it can be shown that $|1\rangle_{\mathrm{L}} = X_1X_2X_3X_4X_5|0\rangle_{\mathrm{L}}$.) Note that

$$S_1S_2S_3S_4 = I_2 \otimes Y \otimes X \otimes X \otimes Y,$$

and

$$S_1S_2S_3S_4|10000\rangle = |11111\rangle.$$

Then the encoded state is given by

$$\frac{1}{\sqrt{8}}(I + S_1)(I + S_2)(I + S_3)(I + S_4)|\psi\rangle \otimes |0000\rangle = \alpha|0\rangle_{\mathrm{L}} + \beta|1\rangle_{\mathrm{L}}, \tag{19}$$

where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The operator in the left side of this equation is non-unitary, because $I + S_j$ has an eigenvalue 0 (and 2).

The encoding operation is constructed by using Eq.(19) and the following tricky identities. Let U be an arbitrary unitary operator in $\mathrm{U}(2^4)$ and $|\phi\rangle$ an arbitrary state of 4-qubits. Then one finds a *unitary* expression,

$$\begin{aligned} \frac{1}{\sqrt{2}}(I + X \otimes U)(|0\rangle \otimes |\phi\rangle) &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |\phi\rangle + |1\rangle \otimes U|\phi\rangle), \\ &= C\text{-}U\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\phi\rangle\right) \\ &= C\text{-}U(H \otimes I)(|0\rangle \otimes |\phi\rangle), \end{aligned} \tag{20}$$

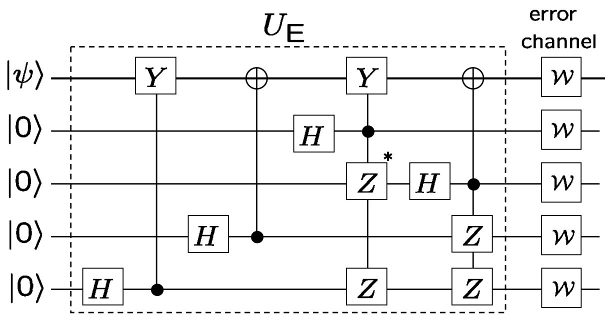

Fig. 8. The encoding operator U_{E} for the five qubit QEC using the stabilizer set defined by Eq.(16). The Z-gate marked * can be neglected in encoding, but is to be included in U_{E}^{-1} in decoding. The order of the stabilizer gates is changed from the original one reprinted in Ref.8 to make the encoding/correcting circuits as simple as possible.

and just the same expression for Y, where C-U denotes the controlled-U operator and the relations,

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{21}$$

are used.

The detection of the eigenvalues of $\{S_j\}$ with respect to the error state, i.e. an eigenstate, $|\Psi'\rangle = W_k(\alpha|0\rangle_{\mathrm{L}} + \beta|1\rangle_{\mathrm{L}})$ can be implemented as shown in Fig.9 with a subsidiary ancilla for each S_j by using the relation,

$$\begin{aligned} C\text{-}S_j\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\Psi'\rangle\right) &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |\Psi'\rangle + |1\rangle \otimes S_j|\Psi'\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + \lambda_j|1\rangle) \otimes |\Psi'\rangle, \end{aligned} \tag{22}$$

where $\lambda_j(=\pm 1)$ is the eigenvalue of S_j, i.e. $S_j|\Psi'\rangle = \lambda_j|\Psi'\rangle$.

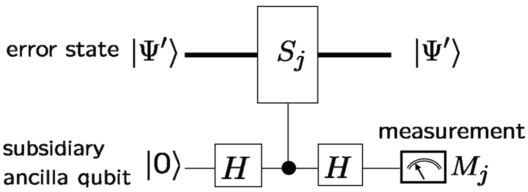

Fig. 9. Detection of the eigenvalue of S_j. The eigenvalue ± 1 is given by the measurement M_j (= 0 or 1) by applying the inverse relations of Eq.(21) with $H^{-1} = H$ to Eq.(22).

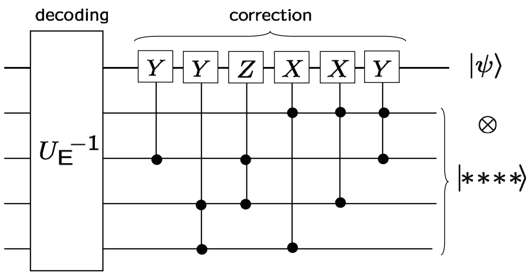

Fig. 10. The unitary error correction corresponding to Fig.8.

We can also construct a unitary error correction without detecting the error syndrome in this example. First, decode the error state with U_{E}^{-1}. Then we find a direct product form released from entanglement,[4]

$$U_{\mathrm{E}}^{-1}|\Psi'\rangle = |\psi'\rangle \otimes |****\rangle, \tag{23}$$

where $|****\rangle$ denotes the syndrome of the four ancilla qubits. The data qubit state $|\psi'\rangle$ has one of the four patterns,

$$\alpha|0\rangle + \beta|1\rangle,\ \alpha|0\rangle - \beta|1\rangle,\ \alpha|1\rangle + \beta|0\rangle,\ \alpha|1\rangle - \beta|0\rangle.$$

This mismatch (except for the first one) can be corrected to a desired form $|\psi\rangle \otimes |****\rangle$ by a Toffoli gate having four controlled qubits, e.g.

'Operate Z on the first qubit, if the syndrome is $****$'

for the second pattern, and so on. The fifteen Toffoli gates corresponding to the probable error states caused by each of the fifteen operators $\{W_k\} = \{X_{1\sim5}, Y_{1\sim5}, Z_{1\sim5}\}$ can be reduced to a more compact form as is shown in Fig.10 with use of some Boolean algebra. (See Fig.11.)

(*Conjecture*) We find an entanglement-free, direct product form Eq.(23) in general after decoding with U_{E}^{-1}, at least if

$$\text{all} \ \ \theta = \frac{n\pi}{2}, \quad (n = 0, \pm1, \pm2, ...),$$

when U_{E} is decomposed into a standard form of a matrix product of CNOTs and one-qubit-gates (=local rotations) such as $\exp[(i\theta/2)V]$, where V is one of the unitary operators $\{X_j, iY_j, Z_j\}$. Note that the Hadamard gate H in Fig.8 is decomposed as $H = i\exp[(-i\pi/2)\sigma_z]\exp[(i\pi/4)\sigma_y]$, and has an acceptable form of this conjecture.

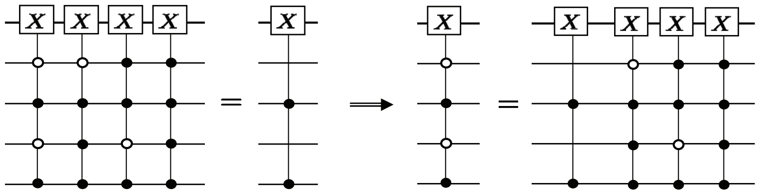

Fig. 11. An example of Boolean relations used to contract the Toffoli gates into a compact circuit shown in Fig.10. The open circle denotes 'If 0' (=If false).

2.4. *Collective error*

So far we have considered quantum errors which act on each qubit independently and have assumed that an error occurs on at most one qubit only. However, the error caused by noises of an external electro-magnetic wave has very long range compared to the quantum devices, e.g. molecules or nano-devices. In this case an error operator acts on several qubits in a given microscopic system *simultaneously*. Let us call this type of error caused by a longwave noise a collective error or a correlated error.[11]

A simple example is a fully correlated (X, Y, Z)-error. In this case we have three kinds of error $\{X^{\otimes n}, Y^{\otimes n}, Z^{\otimes n}\}$ for a n-qubit system. By analogy with the bit-flip error $n = 3$ qubit encoding is sufficient to discriminate the error states and to recover one data qubit. [b] Empirically we found several candidates of encoding/correcting operations. One of the simplest is shown in Fig.12. Note that the encoded state has no entanglement[11] in this case. By encoding with H and decoding the error state with $U_{\rm R}$ we find

$$|\psi\rangle \otimes |00\rangle \;\longrightarrow\; |\psi\rangle \otimes |**\rangle. \tag{24}$$

Note that the error caused by an arbitrarily repeated errors of $X^{\otimes 3}$, $Y^{\otimes 3}$ and $Z^{\otimes 3}$ with arbitrary probabilities can be *exactly* corrected in this model because we have the relations $XZ = Y$, etc. This fact means that the initial state of two ancilla qubits is arbitrary, though the encoding operator should be modified to the inverse of the recovery operator $U_{\rm R}$ defined in Fig.12. [c] The ancilla qubits can be reused without resetting the syndrome, i.e. any longwave noise of this type does not practically cause any error in

[b] Just after the Symposium we have found that by using $2m + 1$ qubit encoding we can recover $2m$ data qubits for this type error.[12]

[c] In general one may define the encoding operator by $U_{\rm E} = U_{\rm R}^{-1}$. However, two controlled gates in $U_{\rm R}$ can be omitted in encoding, when the ancilla state is $|00\rangle$. This is applicable to all examples introduced in this talk.

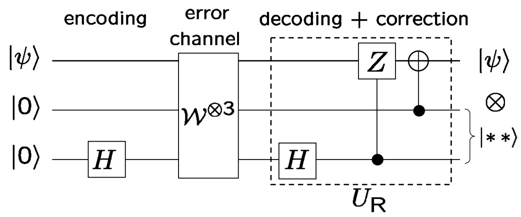

Fig. 12. The QEC for the fully correlated error. The notation $\mathcal{W}$ denotes X, Y or Z.

the system.

This situation becomes clearer if we describe the encoding/correcting processes in the density operator form as

$$|\psi\rangle\langle\psi| \otimes \rho_{\mathrm{a}} \longrightarrow |\psi\rangle\langle\psi| \otimes \rho'_{\mathrm{a}}, \tag{25}$$

where ρ_{a} and ρ'_{a} are the initial and the final density matrices of the ancilla qubits. If we prepare a completely mixed state as the initial ancilla state, i.e. $\rho_{\mathrm{a}} = \mathrm{Diag}[\,1/4, 1/4, 1/4, 1/4\,]$, we find $\rho'_{\mathrm{a}} = \rho_{\mathrm{a}}$. Thus the present unitary QEC system for this specialized error gives us a closed, error-free system.

The model is extended to a more general collective noise $V^{\otimes n}, \forall V \in \mathrm{U}(2)$.[13] Note that generator of such an error is written as

$$(\mathrm{e}^{ia\sigma_\xi})^{\otimes n} = \exp\left(ia\sum_{k=1}^{n}\sigma_\xi^{(k)}\right), \quad (a \in \mathbb{R})$$

where $\xi = x, z$ and $\sigma_\xi^{(k)}$ denotes the Pauli operator acting on the k-th qubit. Let us introduce a total angular momentum defined by

$$\boldsymbol{L} = \frac{1}{2}\sum_{k=1}^{n}\boldsymbol{\sigma}^{(k)}.$$

There are $K_n = {}_nC_m - {}_nC_{m-1}$ eigenstates of $L = 1/2$ for odd $n = 2m+1$. The set of the eigenvector pairs $\{(e_{i0}, e_{i1}), i = 1, 2, ..., K_n\}$ of $L_z = \pm 1/2$ serves as a set of logical qubits for this QEC, because we have the relations

$$(\varSigma_z e_{i0} = e_{i0},\ \varSigma_z e_{i1} = -e_{i1}) \ \text{ and } \ (\varSigma_x e_{i0} = e_{i1},\ \varSigma_x e_{i1} = e_{i0}), \tag{26}$$

for the $L = 1/2$ eigenstates, where $\boldsymbol{\varSigma} = 2\boldsymbol{L}$ is used to compare to $n = 1$.

For simplicity we restrict the following discussions to $n = 3$. Let (e_{a0}, e_{a1}), (e_{b0}, e_{b1}) be the two eigenvector pairs and construct a unitary matrix as

$$U_{\mathrm{E}} = (e_{a0}, e_{a1}, *, *, e_{b0}, e_{b1}, *, *). \tag{27}$$

where the irrelevant vectors shown by $*$ are chosen so as to make $U_{\rm E}$ unitary, e.g. may be chosen to be the four eigenvectors for $L = 3/2$. By encoding with $U_{\rm E}$ and decoding the error state with $U_{\rm R} = U_{\rm E}^{-1}$, one finds that

$$|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| \otimes |v\rangle\langle v| \;\longrightarrow |\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| \otimes |v'\rangle\langle v'|,$$

where $|v'\rangle = V|v\rangle$ with the error operator $V^{\otimes 3}$. In this case the initial state of only one of two ancilla qubits is arbitrary as shown by $|v\rangle$. Thus the error caused by the general longwave noise is limited within the ancilla qubits again.

3. Summary

Conventional theories on QEC are surveyed, emphasizing the usefulness of the unitary correction especially in the operator QEC. The unitary method needs no subsidiary ancilla qubits to detect the error syndrome in the recovery process. This is the most advantageous point, especially, for experimental realization of QEC.[14]

References

1. H. Tomita and M. Nakahara, arXiv:quant-ph/1101.0413.
2. C.-K. Li, M. Nakahara, Y.-T. Poon, N.-S. Sze and H. Tomita, arXiv:quant-ph/1102.1618; Quant. Inf. Comp., **12**, 0148 (2012).
3. S.L. Braunstein, arXiv:quant-ph/9603.024.
4. R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek, Phys. Rev. Lett., **77**, 198 (1996).
5. M. Nakahara and T. Ohmi, *Quantum Computing*, (CRC Press, 2008). Chap.10.
6. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, 2000), Chap.10.
7. N. D. Mermin, *Quantum Computer Science: An introduction*, (Cambridge University Press, 2007), Chap.5.
8. F. Gaitan, *Quantum Error Correction and Fault Tolerant Quantum Computing*, (CRC Press, 2008).
9. P. W. Shor, Phys. Rev. A **52**, 2493 (1995).
10. D. Gottesman, Ph. D. thesis, California Institute of Technology, 1996. (Cited in Ref.8, Chap.4.)
11. G. C. Chiribella, M. Dall'Arno, G. M. D'Ariano, C. Macchiavello and P. Perinotti, Phys. Rev. A **83**, 052305 (2011).
12. C.-K. Li, M. Nakahara, Y.-T. Poon, N.-S. Sze and H. Tomita, arXiv:quant-ph/1104.4750; Phys. Lett. A **375**, 3255 (2011).
13. C.-K. Li, M. Nakahara, Y.-T. Poon, N.-S. Sze and H. Tomita, arXiv:quant-ph/1106.5210; Phys. Rev. A **84**, 044301 (2011).
14. E. Nill, R. Laflamme, R. Martinez and C. Negrevergne, Phys. Rev. Lett., **86**, 5811 (2001).