Recursive Encoding and Decoding of Noiseless Subsystem and Decoherence Free Subspace

Chi-Kwong Li,[1] Mikio Nakahara,[2] Yiu-Tung Poon,[3] Nung-Sing Sze,[4] and Hiroyuki Tomita[5]

*[1]Department of Mathematics, College of William & Mary, Williamsburg, VA 23187-8795, USA.**
[2]Research Center for Quantum Computing and Department of Physics, Kinki University, 3-4-1 Kowakae, Higashi-Osaka, 577-8502, Japan.†
[3]Department of Mathematics, Iowa State University, Ames, IA 50051, USA.‡
[4]Department of Applied Mathematics, The Hong Kong Polytechnic University, Hung Hom, Hong Kong.§
[5]Research Center for Quantum Computing, Kinki University, 3-4-1 Kowakae, Higashi-Osaka, 577-8502, Japan.¶

When environmental disturbance to a quantum system has a wavelength much larger than the system size, all qubits in the system are under the action of the same error operator. Noiseless subsystem and decoherence free subspace are immune to such collective noise. We construct simple quantum circuits which implement these error avoiding codes for a small number n of physical qubits. A single logical qubit is encoded with $n = 3$ and $n = 4$, while two and three logical qubits are encoded with $n = 5$ and $n = 7$, respetively. Recursive relations among subspaces employed in these codes play essential roles in our implementation.

PACS numbers: 03.67.Pp

I. INTRODUCTION

A quantum system is vulnerable to external noise and the system must be protected from it in quantum information processing and quantum computation. The majority of quantum systems employed for these purposes is microscopic in size, typically on the order of a few microns. In contrast, the environmental noise, such as electromagnetic wave, has the wavelength on the order of a few centimeters or more. Therefore, it is natural to assume all the qubits in the register suffer from the same error operator. We call such error the collective error. n-qubit quantum states ρ are represented as $2^n \times 2^n$ density matrices and a quantum channel is realized as a completely positive linear map Φ with an operator sum representation

$$\Phi(\rho) = \sum_{j=1}^{r} E_j \rho E_j^\dagger \tag{1}$$

with error operators $\{E_j\}$; see [1, 2]. The error operators in Φ can be expressed as multiples of operator of the form $W^{\otimes n} \in \mathbf{2}^{\otimes n}$, where $\mathbf{2}$ is the two-dimensional (fundamental) irreducible representation (irrep) of SU(2).

Decoherence free subspace (DFS) [3–6] and noiseless subsystem (NS) [7–10] are two standard methods to correct collective errors [10, 11]. The scheme is explained using the operator sum representation of the quantum channel (1). Suppose the finite dimensional C^*-algebra $\mathcal{A}_n$ generated by the error operators admits the unique decomposition into irreps up to unitary equivalence (similarity) as $\oplus_j (I_{r_j} \otimes M_{n_j})$ with $\sum_j r_j n_j = N$, where $N = 2^n$ and n_j is the dimension of the irrep while r_j its multiplicity. Then every error operator E_i has the form $\oplus_j (I_{r_j} \otimes B_j)$ with $B_j \in M_{n_j}$. For every index j, if we regard $M_N = (I_{r_j} \otimes M_{n_j}) \oplus M_q$ with $q = N - r_j n_j$, and if we apply the channel to a quantum state $\rho = (\hat{\rho} \otimes \sigma) \oplus O_q$ with $\hat{\rho} \in M_{r_j}$ and $\sigma \in M_{n_j}$, according to this decomposition, then $\Phi(\rho) = (\hat{\rho} \otimes \sigma_E) \oplus O_q$ because of the special form of the error operators in this decomposition. Here σ_E is the ancilla state after Φ is applied and O_q is a null matrix of order q. Thus, the state $\hat{\rho}$ encoded as above will not be affected by the errors (noise) and can be easily recovered. This gives rise to an NS. The situation is particularly pleasant if $n_j = 1$, i.e., we use the one-dimensional irreps of $\mathcal{A}_n$, so that $\Phi(\hat{\rho} \oplus O_q) = \hat{\rho} \oplus O_q$. In such a case, we get a DFS.

We are interested in simple implementation of DFSs and NSs for the channels with common error on each qubit in the register. By the discussion in the preceding paragraph, DFS employs one-dimensional irreps of the algebra $\mathcal{A}_n$ generated by $\mathbf{2}^{\otimes n}$ for encoding while the latter encodes logical qubits by making use of the multiplicity of some irreps.

It is the purpose of this paper to investigate the implementation of these ideas in terms of quantum circuits. We consider DFS with $n = 4$, which implements a single logical qubit, and NS with $n = 3$ and 5, which encodes a single logical qubit and two logical qubits, respectively. Viola *et al* [12] worked out the circuit implementation of $n = 3$ NS and demonstrated its validity by using ion trap quantum computer. No further works have been conducted for $n \geq 4$ to date to our knowledge. Our implementation, starting with $n = 3$ NS, is recursive so that $n = 4$ DFS and $n = 5$ NS are implemented with the quantum circuit for $n = 3$. Moreover, our circuit for $n = 3$ is simpler than that obtained in [9] and [12].

We construct a quantum circuit for $n = 3$ NS in the next section. We analyze $n = 4$ DFS and $n = 5$ NS in Sections III and IV by making use of the result of Section II. Our analysis is concrete and encoding basis vectors and quantum circuits are explicitly constructed. The last section is devoted to summary and discussion.

We will use the fact (see [10]) that the algebra $\mathcal{A}_n$ gener-

*Electronic address: ckli@math.wm.edu
†Electronic address: nakahara@math.kindai.ac.jp
‡Electronic address: ytpoon@iastate.edu
§Electronic address: raymond.sze@inet.polyu.edu.hk
¶Electronic address: tomita@alice.math.kindai.ac.jp

ated by $\mathbf{2}^{\otimes n}$ has the unique decomposition $\bigoplus_{0\le j\le n/2}(I_{r_j}\otimes M_{n_j})$ with $(r_0,n_0) = (1,n+1)$ and $(r_j,n_j) = \left(\binom{n}{j}-\binom{n}{j-1}, n+1-2j\right)$ for $0<j\le n/2$. Also, we will employ the Lie theoretic notation and regard a qubit belonging to the representation space of the fundamental representation $\mathbf{2}$ of SU(2) while the product operator $W^{\otimes n}$ acts as a reducible representation $\mathbf{2}^{\otimes n}$.

II. 3-QUBIT NOISELESS SUBSYSTEM

Let us consider a 3-qubit system and see how it can be used to encode a logical qubit which is robust against any noise of the form $W^{\otimes 3}$, where W is an arbitrary element of $\mathbf{2}$. We first consider the algebra $\mathcal{A}_3$ of $\mathbf{2}^{\otimes 3}$. $\mathcal{A}_3$ is decomposed into the sum of irreps as $\mathbf{2}^{\otimes 3} = \mathbf{4}\oplus(I_2\otimes\mathbf{2})$, where I_n is the unit matrix of dimension n. Corresponding to this decomposition, any unitary matrix $V\in\mathbf{2}^{\otimes 3}$ can be decomposed as $V = V_4\oplus(I_2\otimes V_2)$ under a proper choice of basis vectors. Here V_4 belongs to $\mathbf{4}$ and V_2 to $\mathbf{2}$ of SU(2). It should be noted that I_2 is immune to any collective noise of the form $W^{\otimes 3}, W\in\mathbf{2}$ and the corresponding vector space forms the NS.

The success of our schemes depends on a judicious choice of orthonormal basis for the decomposition of the algebra $\mathcal{A}_3$ generated by $\mathbf{2}^{\otimes 3}$. Let $\{|e_{4,1}\rangle,|e_{4,2}\rangle,|e_{4,3}\rangle,|e_{4,4}\rangle|\}$ be a basis of $\mathbf{4}$, and $\{|e_{a1}\rangle,|e_{a2}\rangle\}$ and $\{|e_{b1}\rangle,|e_{b2}\rangle\}$ be bases of the two $\mathbf{2}$'s defined as follows

$$\begin{cases} |e_{4,1}\rangle = |000\rangle, \\ |e_{4,2}\rangle = \dfrac{1}{\sqrt{3}}[|0\rangle(|01\rangle+|10\rangle)+|1\rangle|00\rangle], \\ |e_{4,3}\rangle = (\sigma_x)^{\otimes 3}|e_{4,2}\rangle, \\ |e_{4,4}\rangle = |111\rangle = (\sigma_x)^{\otimes 3}|e_{4,1}\rangle, \end{cases} \tag{2}$$

$$\begin{cases} |e_{a1}\rangle = \dfrac{1}{\sqrt{2}}|0\rangle(|10\rangle-|01\rangle), \\ |e_{a2}\rangle = -(\sigma_x)^{\otimes 3}|e_{a1}\rangle, \end{cases} \tag{3}$$

$$\begin{cases} |e_{b1}\rangle = \dfrac{1}{\sqrt{6}}[|0\rangle(|01\rangle+|10\rangle)-2|1\rangle|00\rangle], \\ |e_{b2}\rangle = -(\sigma_x)^{\otimes 3}|e_{b1}\rangle, \end{cases} \tag{4}$$

where σ_k is the kth Pauli matrix. We implement an NS from two $\mathbf{2}$ irreps.

Suppose $U_E^{(3)}$ is an encoding matrix which generates the above basis vectors from the binary basis vectors $|i_1i_2i_3\rangle,\ (i_k\in\{0,1\})$. We choose $U_E^{(3)}$ to have columns

$$(|e_{a1}\rangle,|e_{b1}\rangle,|e_{a2}\rangle,|e_{b2}\rangle,|e_{4,4}\rangle,|e_{4,2}\rangle,-|e_{4,1}\rangle,-|e_{4,3}\rangle)$$

in this order. The basis vectors $\{|e_{4,k}\rangle\}$ is irrelevant for our purpose and their order and signs have been chosen so as to make the circuit implementation as simple as possible.

Figure 1 shows an example of the encoding circuit, in which

$$G_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & \sqrt{2} \\ -\sqrt{2} & 1\end{pmatrix},\quad G_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1\end{pmatrix}.$$

Note that our circuit is simpler than that found in [9] and [12] regarding the number of gates.

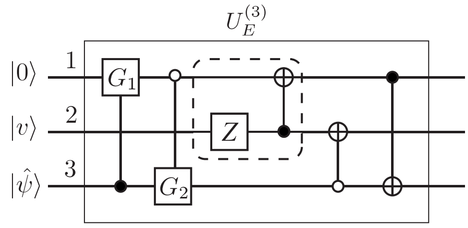

FIG. 1: Encoding circuit $U_E^{(3)}$ of NS with $n=3$. It encodes a single qubit state $|\hat\psi\rangle$. The part surrounded by a broken line can be omitted if the initial state $|v\rangle$ of the central qubit is $|0\rangle$. The recovery operation is given by $U_E^{(3)\dagger}$.

Now we prove that collective errors are corrected by employing basis vectors (3) and (4) as a logical qubit basis.

Theorem II.1 *Let α,β,γ be any real numbers and let*

$$X_\alpha = (e^{i\alpha\sigma_x})^{\otimes 3}, Y_\beta = (e^{i\beta\sigma_y})^{\otimes 3}, Z_\gamma = (e^{i\gamma\sigma_z})^{\otimes 3}.$$

Consider a quantum channel $\Phi: M_8\to M_8$ given by

$$\Phi(\rho) = p_0\rho + p_1X_\alpha\rho X_\alpha^\dagger + p_2Y_\beta\rho Y_\beta^\dagger + p_3Z_\gamma\rho Z_\gamma^\dagger$$

for some $p_i\in\mathbb{R}$ such that $\sum_{i=0}^3 p_i\le 1$. Then for any data state $\hat\rho\in M_2$, $U_E^{(3)}$ and Φ satisfy the identity

$$\begin{aligned} &U_E^{(3)\dagger}\Phi\left(U_E^{(3)}(|0\rangle\langle 0|\otimes\rho_a\otimes\hat\rho)U_E^{(3)\dagger}\right)U_E^{(3)} \\ &= |0\rangle\langle 0|\otimes\left(\sum_{j=0}^3 p_jU_j\rho_aU_j^\dagger\right)\otimes\hat\rho, \end{aligned} \tag{5}$$

that is, the initial data state is recovered in the output state with no entanglement with the ancilla qubits. Here ρ_a is an initial single qubit ancilla state and $U_0 = I_2$, $U_1 = e^{i\alpha\sigma_x}$, $U_2 = e^{i\beta\sigma_y}$, $U_3 = e^{i\gamma\sigma_z}$.

Proof: We show that the $\mathbf{2}\oplus\mathbf{2}$ irreps form an NS by explicit evaluation. Let $\{|e_{a1}\rangle,|e_{a2}\rangle\}$ span the logical $|0\rangle_L$, while $\{|e_{b1}\rangle,|e_{b2}\rangle\}$ spans the logical $|1\rangle_L$. We show that noise operators X_α, Y_β and Z_γ leave each subspace invariant. Let $P_a = \sum_{i=1}^2|e_{ai}\rangle\langle e_{ai}|$ and $P_b = \sum_{i=1}^2|e_{bi}\rangle\langle e_{bi}|$. Then it is easy to show that $X_\alpha P_kX_\alpha^\dagger = Y_\beta P_kY_\beta^\dagger = Z_\gamma P_kZ_\gamma^\dagger = P_k\ (k=a,b)$.

Now we prove the identity. We use a pure state notation to simplify the expressions. The general case with mixed initial states ρ_a and $\hat\rho$ is obtained by simply mixing the pure state results using linearity. Let $|\hat\psi\rangle = a|0\rangle+b|1\rangle$ be a data qubit state to be encoded and $|v\rangle = v_0|0\rangle+v_1|1\rangle$ be the initial state of the first ancilla qubit, while that of the first qubit is set to $|0\rangle$. The encoding under the action of $U_E^{(3)}$ yields

$$|\Psi\rangle = U_E^{(3)}|0\rangle|v\rangle|\hat\psi\rangle = v_0(a|e_{a1}\rangle+b|e_{b1}\rangle)+v_1(a|e_{a2}\rangle+b|e_{b2}\rangle).$$

Let us consider a noise operator X_α. Its action on $|\Psi\rangle$ yields

$$\begin{aligned} X_\alpha|\Psi\rangle &= (v_0\cos\alpha+iv_1\sin\alpha)(a|e_{a1}\rangle+b|e_{b1}\rangle) \\ &\quad +(v_1\cos\alpha+iv_0\sin\alpha)(a|e_{a2}\rangle+b|e_{b2}\rangle). \end{aligned}$$

The action of the recovery operator $U_E^{(3)\dagger}$ recovers the initial state, except for the second qubit, as

$$U_E^{(3)\dagger} X_\alpha |\Psi\rangle = |0\rangle \left(e^{i\alpha\sigma_x}|v\rangle\right) |\hat{\psi}\rangle,$$

which shows that data qubit state is immune to X_α. It is shown similarly that the data qubit is immune to other error operators either. Since each error is in action with the probability p_i, we have proved the identity (5). ∎

In contrast with an ordinary QECC, the scheme corrects multiple action of the error operators. It was shown in the theorem that the central qubit can be any superposition state or mixed state initially and its output state is another superposition/mixed state under an action of a single error operator in X_α, Y_β and Z_γ. Note that the error channel leaves the encoded word unchanged. Namely, given any initial ancilla state ρ_a, there exists an ancilla state ρ_a' such that $\Phi\left(U_E^{(3)}(|0\rangle\langle 0| \otimes \rho_a \otimes \hat{\rho}) U_E^{(3)\dagger}\right) = U_E^{(3)}(|0\rangle\langle 0| \otimes \rho_a' \otimes \hat{\rho}) U_E^{(3)\dagger}$. Then the error correction may be repeated as many times as required. This implies that it corrects any error operator of the form $W^{\otimes 3}$, where $W \in \mathbf{2}$. This is because any element $W \in \mathbf{2}$ is decomposed as $W = e^{i\theta_1\sigma_x} e^{i\theta_2\sigma_y} e^{i\theta_3\sigma_x}$. This is clear since $W^{\otimes 3}$ is expressed as a product $X_{\theta_1} Y_{\theta_2} X_{\theta_3}$, each factor of which leaves the NS invariant.

III. 4-QUBIT DECOHRENCE FREE SUBSPACE

We design the 4-qubit DFS, which is robust against collective noise of the form $W^{\otimes 4}$ ($W \in \mathbf{2}$), by taking advantage of the NS analyzed in the previous section.

The algebra $\mathcal{A}_4$ obtained from $\mathbf{2}^{\otimes 4}$ is decomposed as $\mathbf{2}^{\otimes 4} = \mathbf{5} \oplus (I_3 \otimes \mathbf{3}) \oplus (I_2 \otimes \mathbf{1})$. Correspondingly any $V \in \mathbf{2}^{\otimes 4}$ is decomposed as $V = V_5 \oplus (I_3 \otimes V_3) \oplus (I_2 \otimes V_1)$ under a proper choice of basis vectors. Here V_k an element of a k-dimensional irrep of SU(2)$^{\otimes 4}$. The singlet irrep is immune to any operator $V = W^{\otimes 4}, W \in \mathbf{2}$ and two of them form a single logical qubit immune to any noise of the form V. This (reducible) vector space is the DFS which is robust against the collective noise.

We generate basis vectors of two one-dimensional irreps of SU(2) from $\{|e_{ai}\rangle, |e_{bi}\rangle\}$ as

$$\begin{cases} |0\rangle_L &= \dfrac{1}{\sqrt{2}}(|1\rangle|e_{a1}\rangle - |0\rangle|e_{a2}\rangle) \\ &= \dfrac{1}{\sqrt{2}}(|1\rangle|e_{a1}\rangle + |0\rangle(\sigma_x)^{\otimes 3}|e_{a1}\rangle), \\ |1\rangle_L &= \dfrac{1}{\sqrt{2}}(|1\rangle|e_{b1}\rangle - |0\rangle|e_{b2}\rangle) \\ &= \dfrac{1}{\sqrt{2}}(|1\rangle|e_{b1}\rangle + |0\rangle(\sigma_x)^{\otimes 3}|e_{b1}\rangle). \end{cases} \tag{6}$$

It is important in the implementation of the encoding circuit to realize that

$$\begin{aligned} |0\rangle_L &= (X \otimes I_8)(\mathrm{CNNN})(H \otimes I_8)|0\rangle \otimes |e_{a1}\rangle \\ &= (X \otimes I_8)(\mathrm{CNNN})(H \otimes U_E^{(3)})|0\rangle \otimes |000\rangle, \\ |1\rangle_L &= (X \otimes I_8)(\mathrm{CNNN})(H \otimes I_8)|0\rangle \otimes |e_{b1}\rangle \\ &= (X \otimes I_8)(\mathrm{CNNN})(H \otimes U_E^{(3)})|0\rangle \otimes |001\rangle, \end{aligned}$$

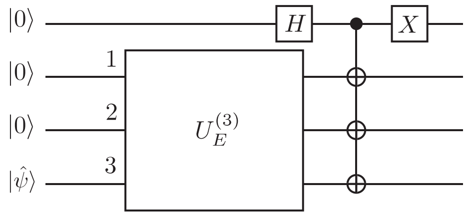

FIG. 2: Encoding circuit $U_E^{(4)}$ of DFS with $n = 4$. It encodes a single qubit state $|\hat{\psi}\rangle$.

where CNNN is a controlled NOT gate with three target bits.

Figure 2 shows an example of the encoding circuit for the DFS. In contrast with the three-qubit NS, all the ancilla qubits must be initially set to $|0\rangle$.

IV. 5-QUBIT NOISELESS SUBSYSTEM

NS using five qubits encodes two data qubits. It is recursively implemented by employing the encoding circuit $U_E^{(3)}$ for the three-qubit NS.

The algebra $\mathcal{A}_5$ obtained from $\mathbf{2}^{\otimes 5}$ is decomposed as $\mathbf{2}^{\otimes 5} = \mathbf{6} \oplus (I_4 \otimes \mathbf{4}) \oplus (I_5 \otimes \mathbf{2})$. Correspondingly, any unitary matrix $V \in \mathbf{2}^{\otimes 5}$ is decomposed as $V = V_6 \oplus (I_4 \otimes V_4) \oplus (I_5 \otimes V_2)$ under a proper choice of basis vectors. We implement an NS by employing four of five two-dimensional irreps.

Let $\{|e_{ai}\rangle, |e_{bi}\rangle\}$ be basis vectors introduced for $n = 3$ in Section II. We generate eight basis vectors from them as

$$\begin{cases} |00\rangle_L = \dfrac{1}{\sqrt{2}}|e_{a1}\rangle(|01\rangle - |10\rangle), \\ |01\rangle_L = \dfrac{1}{\sqrt{6}}[|e_{a1}\rangle(|01\rangle + |10\rangle) - 2|e_{a2}\rangle|00\rangle], \\ |10\rangle_L = \dfrac{1}{\sqrt{2}}|e_{b1}\rangle(|01\rangle - |10\rangle), \\ |11\rangle_L = \dfrac{1}{\sqrt{6}}[|e_{b1}\rangle(|01\rangle + |10\rangle) - 2|e_{b2}\rangle|00\rangle], \end{cases} \tag{7}$$

and their bit-flipped ones obtained by applying $\sigma_x^{\otimes 5}$ on them, just in the same manner as Eqs. (3) and (4) are obtained from the basis vectors $|0\rangle$ and $|1\rangle$ of $n = 1$. We emphasize the similar structure between Eq. (7) and Eqs. (3) and (4). This observation makes implementation of the encoding/decoding circuit almost a trivial work. Note that we do not need to worry about the rest of the basis vectors so far as they are orthogonal to the above basis vectors spanning the NS. This orthogonalization is automatically taken into account by unitarity of the encoding circuit.

Figure 3 (a) shows an example of the encoding circuit $U_E^{(5)}$ of the NS. The central qubit can be any state while all the other ancilla qubits must be in $|0\rangle$. Each $U_E^{(3)}$ acts on the three qubits numbered 1, 2 and 3, which are fed into the input ports 1,2 and 3, respectively, in Fig. 1. The $n = 7$ NS encoding circuit can be also constructed recursively as shown in Fig. 3 (b).

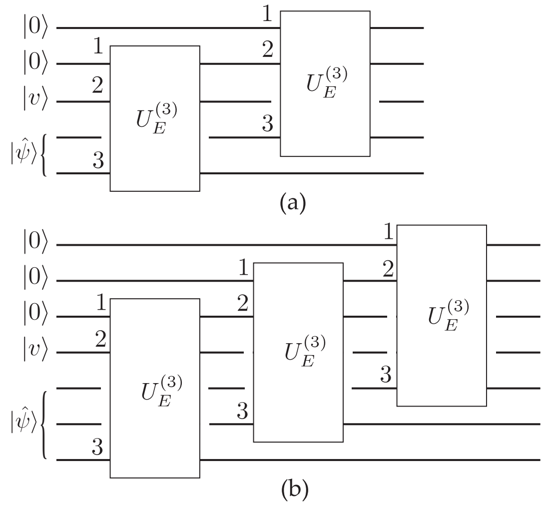

FIG. 3: (a) Encoding circuit $U_E^{(5)}$ of the 5-qubit NS, which encodes a two-data-qubit state $|\hat{\psi}\rangle$. The third and the fourth qubits in Eq. (7) are exchanged to make the recursive symmetry manifest in this diagram. (b) Encoding circuit $U_E^{(7)}$ for the 7-qubit NS, which encodes a three-data-qubit state $|\hat{\psi}\rangle$.

V. SUMMARY AND DISCUSSIONS

DFS and NS make use of vector subspaces which are immune to noise of the form $W^{\otimes n}$, where W belongs to $\mathbf{2}$ of SU(2). We have constructed simple encoding and decoding quantum circuits of NS for $n = 3$ and 5 and DFS for $n = 4$. Our strategy is to use the encoding/decoding circuit $U_E^{(3)}$ for $n = 3$ recursively in the implementation for $n = 4$ and $n = 5$. We have constructed the bases of $\mathbf{1}$'s for $n = 4$ and the bases of $\mathbf{2}$'s for $n = 5$ from the bases of two $\mathbf{2}$'s for $n = 3$ as given in Eqs. (6) and (7). One can then generalize this construction to find the bases of $\mathbf{1}$'s for $n = 2m + 2$ and the basis of $\mathbf{2}$'s for $n = 2m+3$ from the 2^m bases of $\mathbf{2}$'s for $n = 2m+1$. We have implemented DFS and NS encoding/decoding circuits by taking advantage of this recursive relations among basis vectors of different n. The number of logical qubits in the limit of large n is asymptotically $n/2$ for both even n and odd n. It should be clear form our construction that m logical qubits are implemented by use of $m\, U_E^{(3)}$-modules, which shows that the circuit complexity for our encoding and decoding circuits increases merely linearly in m.

Note, however, that our construction does not give the maximum number of correctable qubits for the channel. There are $\binom{n}{m} - \binom{n}{m-1}$ basis vectors in 2-dimensional irreps for $n = 2m + 1$, which encode $k = \lfloor \log_2 \left(\binom{n}{m} - \binom{n}{m-1} \right) \rfloor$ qubits. This number k is greater than m for $n \geq 9$, and actually $k/n \to 1$ as $n \to \infty$. This asymptotic behavior is also observed in [10] for DFS.

In a forth coming paper, we will give the full details of the recursion scheme. Moreover, in depth discussion of the decomposition of the algebra $\mathbf{2}^n$ and the construction of other noiseless subsystems of channels with error operators in the algebra will be presented [13].

It was shown that the central qubit in Figs. 1 and 3 can be any state. Although the entropy of the qubit system increases in general, it remains constant if the central qubit is maximally mixed initially as $\rho_a = \frac{1}{2} I_2$. This behavior is somewhat analogous to DFS with $\rho_a = |0\rangle\langle 0|$, in which the entropy does not change at all.

Acknowledgement

CKL is a visiting professor of the Hong Kong University of Science and Technology under a Fulbright Fellowship in 2011. His research was supported by a USA NSF grant, a HK RGC grant and the 2011 Shanxi 100 Talent Program. He is an honorary professor of University of Hong Kong, Taiyuan University of Technology, and Shanghai University. MN and HT were supported by "Open Research Center" Project for Private Universities: matching fund subsidy from MEXT. MN would like to thank partial supports of Grants-in-Aid for Scientific Research from the JSPS (Grant No. 23540470). YTP was supported by a USA NSF grant. NSS was supported by a HK RGC grant.

[1] M.A. Neilsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[2] M. Nakahara and T. Ohmi, *Quantum Computing, From Linear Algebra to Physical Realization*, CRC Press, New York, 2008.

[3] P. Zanardi and M. Rasetti, Phys. Rev. Lett., **79**, 3306 (1997).

[4] P. Zanardi and M. Rasetti, Mod. Phys. Lett. B **11**, 1085 (1997).

[5] P. Zanardi, Phys. Rev. A **57**, 3276 (1998).

[6] D. A. Lidar, I. L. Chuang and K. B. Whaley, Phys. Rev. Lett., **81**, 2594 (1998).

[7] E. Knill, R. Laflamme and L. Viola, Phys. Rev. Lett., **84**, 2525 (2000).

[8] S. De Filippo, Phys. Rev. A **62**, 052307 (2000).

[9] C.-P. Yang and J. Gea-Banacloche, Phys. Rev. A **63**, 022311 (2001).

[10] J. Kempe, D. Bacon, D. A. Lidar and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).

[11] D.W. Kribs, R. Laflamme, D. Poulin, M. Lesosky, Quant. Inf. Comp., **6**, 382 (2006).

[12] L. Viola, E. M. Fortunato, M. A. Pravia, E. Knill, R. Laflamme and D. G. Cory, Science, **293**, 2059 (2001).

[13] C.-K, Li, M. Nakahara, Y.-T. Poon, N.-S. Sze, and H. Tomita, in preparation.