

# Recursive encoding and decoding of the noiseless subsystem and decoherence-free subspace

Chi-Kwong Li,<sup>1,\*</sup> Mikio Nakahara,<sup>2,†</sup> Yiu-Tung Poon,<sup>3,‡</sup> Nung-Sing Sze,<sup>4,§</sup> and Hiroyuki Tomita<sup>5,||</sup>

<sup>1</sup>*Department of Mathematics, College of William & Mary, Williamsburg, Virginia 23187-8795, USA*

<sup>2</sup>*Research Center for Quantum Computing and Department of Physics, Kinki University, 3-4-1 Kowakae, Higashi-Osaka 577-8502, Japan*

<sup>3</sup>*Department of Mathematics, Iowa State University, Ames, Iowa 50011, USA*

<sup>4</sup>*Department of Applied Mathematics, The Hong Kong Polytechnic University, Hung Hom, Hong Kong*

<sup>5</sup>*Research Center for Quantum Computing, Kinki University, 3-4-1 Kowakae, Higashi-Osaka 577-8502, Japan*

(Received 4 July 2011; revised manuscript received 14 July 2011; published 5 October 2011)

When an 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. The noiseless subsystem and decoherence-free subspace are immune to such collective noise. We construct simple quantum circuits that implement these error-avoiding codes for a small number  $n$  of physical qubits. A single logical qubit is encoded with  $n = 3$  and 4, while two and three logical qubits are encoded with  $n = 5$  and 7, respectively. Recursive relations among subspaces employed in these codes play essential roles in our implementation.

DOI: 10.1103/PhysRevA.84.044301

PACS number(s): 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 are microscopic in size, typically on the order of a few micrometers. In contrast, environmental noise, such as electromagnetic waves, has a wavelength on the order of a few centimeters or more. Therefore, it is natural to assume that all the qubits in the register suffer from the same error operator. We call such an error the collective error. The  $n$ -qubit quantum states  $\rho$  are represented as  $2^n \times 2^n$  density matrices and a quantum channel is realized as a completely positive linear map  $\Phi$  with an operator sum representation

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

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

The decoherence-free subspace (DFS) [3–6] and noiseless subsystem (NS) [7–10] are two standard methods of coding used to correct collective errors [10,11]. The scheme is explained using the operator sum representation of the quantum channel Eq. (1). Suppose the finite-dimensional  $C^*$ -algebra  $\mathcal{A}_n$  generated by the error operators admits the unique decomposition into IRs up to a unitary equivalence (similarity) as  $\bigoplus_j (I_{r_j} \otimes M_{n_j})$  with  $\sum_j r_j n_j = N$ , where  $N = 2^n$ ,  $n_j$  is the dimension of the IR, and  $r_j$  is its multiplicity. Then every error operator  $E_i$  has the form  $\bigoplus_j (I_{r_j} \otimes B_j)$  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  $\sigma_E$  is the ancilla state after  $\Phi$  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 a NS. The situation is particularly pleasant if  $n_j = 1$ , i.e., we use the one-dimensional IRs 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 a common error on each qubit in the register. From the discussion in the preceding paragraph we have that the DFS employs one-dimensional IRs of algebra  $\mathcal{A}_n$  generated by  $\mathbf{2}^{\otimes n}$  for encoding while the NS encodes logical qubits by making use of the multiplicity of an IR.

The purpose of this paper is to investigate the implementation of these ideas in terms of quantum circuits. We consider the DFS with  $n = 4$ , which implements a single logical qubit, and the 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 the  $n = 3$  NS and demonstrated its validity by using an ion-trap quantum computer. We are unaware of further work having been conducted to date for  $n \geq 4$ . Our implementation, starting with  $n = 3$  NS, is recursive so that the  $n = 4$  DFS and the  $n = 5$  NS are implemented with the quantum circuit for  $n = 3$ . Moreover, our circuit for  $n = 3$  is simpler than that obtained in Refs. [9,12].

We construct a quantum circuit for the  $n = 3$  NS in Sec. II. We analyze the  $n = 4$  DFS and the  $n = 5$  NS in Secs. III and IV, respectively, by making use of the result of Sec. II. Our analysis is concrete and the encoding basis vectors and quantum circuits are explicitly constructed. We conclude in Sec. V with a summary and discussion.

We use the fact [10] that the algebra  $\mathcal{A}_n$  generated by  $\mathbf{2}^{\otimes n}$  has the unique decomposition  $\bigoplus_{0 \leq j \leq n/2} (I_{r_j} \otimes M_{n_j})$  with  $(r_0, n_0) = (1, n+1)$  and  $(r_j, n_j) = \binom{n}{j} - \binom{n}{j-1}, n+1-2j$  for  $0 < j \leq n/2$ . We also employ the Lie theoretic notation and regard a qubit belonging to the representation space of

\*ckli@math.wm.edu

†nakahara@math.kindai.ac.jp

‡ytpoon@iastate.edu

§raymond.sze@inet.polyu.edu.hk

||tomita@alice.math.kindai.ac.jp

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. THE 3-QUBIT NOISELESS SUBSYSTEM

Let us consider a 3-qubit system and see how it can be used to encode a logical qubit that 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  $\mathbf{2}^{\otimes 3}$  in which  $\mathcal{A}_3$  is decomposed into the sum of IRs 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  $V = V_4 \oplus (I_2 \otimes V_2)$  for a proper choice of basis vectors. Here  $V_4$  belongs to  $\mathbf{4}$  and  $V_2$  belongs 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

$$\begin{aligned} |e_{4,1}\rangle &= |000\rangle, \\ |e_{4,2}\rangle &= \frac{1}{\sqrt{3}}[|0\rangle(|01\rangle + |10\rangle) + |1\rangle|00\rangle], \\ |e_{4,3}\rangle &= (\sigma_x)^{\otimes 3}|e_{4,2}\rangle, \end{aligned} \quad (2)$$

$$\begin{aligned} |e_{4,4}\rangle &= |111\rangle = (\sigma_x)^{\otimes 3}|e_{4,1}\rangle; \\ |e_{a1}\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|10\rangle - |01\rangle), \end{aligned} \quad (3)$$

$$\begin{aligned} |e_{a2}\rangle &= -(\sigma_x)^{\otimes 3}|e_{a1}\rangle; \\ |e_{b1}\rangle &= \frac{1}{\sqrt{6}}[|0\rangle(|01\rangle + |10\rangle) - 2|1\rangle|00\rangle], \\ |e_{b2}\rangle &= -(\sigma_x)^{\otimes 3}|e_{b1}\rangle, \end{aligned} \quad (4)$$

where  $\sigma_k$  is the  $k$ th Pauli matrix. We implement a NS from two  $\mathbf{2}$  IRs.

Suppose  $U_E^{(3)}$  is an encoding matrix that generates the above basis vectors from the binary basis vectors  $|i_1 i_2 i_3\rangle$  ( $i_k \in \{0, 1\}$ ). 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  $\{|e_{4,k}\rangle\}$  are irrelevant for our purposes 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 Refs. [9,12] regarding the number of gates.

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

*Theorem.* Let  $\alpha$ ,  $\beta$ , and  $\gamma$  be any real numbers and let

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

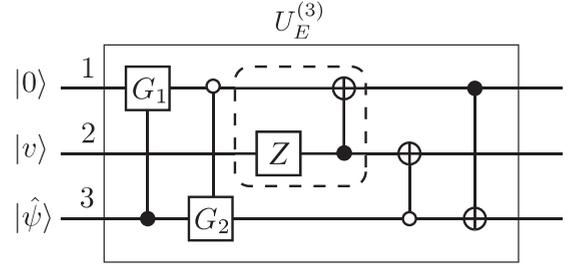


FIG. 1. Encoding circuit  $U_E^{(3)}$  of the NS with  $n = 3$ . It encodes a single-qubit state  $|\hat{\psi}\rangle$ . The part surrounded by the dashed line can be omitted if the initial state  $|v\rangle$  of the central qubit is  $|0\rangle$ . The recovery operation is given by  $U_E^{(3)\dagger}$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

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

$$\Phi(\rho) = p_0\rho + p_1 X_\alpha \rho X_\alpha^\dagger + p_2 Y_\beta \rho Y_\beta^\dagger + p_3 Z_\gamma \rho Z_\gamma^\dagger$$

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

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

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

*Proof.* We show that the  $\mathbf{2} \oplus \mathbf{2}$  IRs form a NS by explicit evaluation. Let the logical  $|0\rangle_L$  lie in the span of  $\{|e_{a1}\rangle, |e_{a2}\rangle\}$  and the logical  $|1\rangle_L$  lie in the span of  $\{|e_{b1}\rangle, |e_{b2}\rangle\}$ . We show that noise operators  $X_\alpha$ ,  $Y_\beta$ , and  $Z_\gamma$  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  $X_\alpha P_k X_\alpha^\dagger = Y_\beta P_k Y_\beta^\dagger = Z_\gamma P_k Z_\gamma^\dagger = P_k$  ( $k = a, b$ ).

Now we prove the identity. We use a pure-state notation to simplify the expressions. The general case with mixed initial states  $\rho_a$  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

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

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

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

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

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

which shows that data qubit state is immune to  $X_\alpha$ . It is shown similarly that the data qubit is immune to other error operators as well. Since each error is in action with the probability  $p_i$ , we have proved the identity in Eq. (5). ■

In contrast with an ordinary quantum error-correcting code, the scheme corrects multiple actions 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 or mixed state under an action of a single error operator in  $X_\alpha, Y_\beta$ , and  $Z_\gamma$ . Note that the error channel leaves the encoded word unchanged, namely, given any initial ancilla state  $\rho_a$ , there exists an ancilla state  $\rho'_a$  such that  $\Phi(U_E^{(3)}(|0\rangle\langle 0| \otimes \rho_a \otimes \hat{\rho})U_E^{(3)\dagger}) = U_E^{(3)}(|0\rangle\langle 0| \otimes \rho'_a \otimes \hat{\rho})U_E^{(3)\dagger}$ . 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. THE 4-QUBIT DECOHERENCE 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 preceding 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  $V = V_5 \oplus (I_3 \otimes V_3) \oplus (I_2 \otimes V_1)$  for a proper choice of basis vectors. Here  $V_k$  is an element of a  $k$ -dimensional IR of  $SU(2)^{\otimes 4}$ . The singlet IR is immune to any operator  $V = W^{\otimes 4}$ , where  $W \in \mathbf{2}$ , and two of them form a single logical qubit that is immune to any noise of the form  $V$ . This (reducible) vector space is the DFS that is robust against the collective noise.

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

$$\begin{aligned} |0\rangle_L &= \frac{1}{\sqrt{2}}(|1\rangle|e_{a1}\rangle - |0\rangle|e_{a2}\rangle) \\ &= \frac{1}{\sqrt{2}}[|1\rangle|e_{a1}\rangle + |0\rangle(\sigma_x)^{\otimes 3}|e_{a1}\rangle], \\ |1\rangle_L &= \frac{1}{\sqrt{2}}(|1\rangle|e_{b1}\rangle - |0\rangle|e_{b2}\rangle) \\ &= \frac{1}{\sqrt{2}}[|1\rangle|e_{b1}\rangle + |0\rangle(\sigma_x)^{\otimes 3}|e_{b1}\rangle]. \end{aligned} \quad (6)$$

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

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

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. THE 5-QUBIT NOISELESS SUBSYSTEM

The 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.

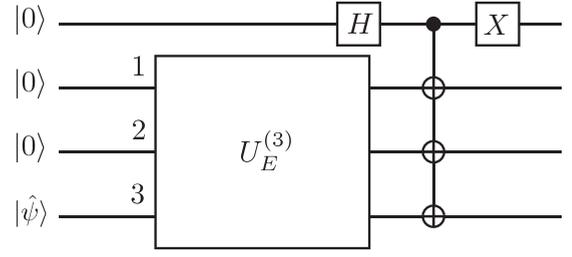


FIG. 2. Encoding circuit  $U_E^{(4)}$  of the DFS with  $n = 4$ . It encodes a single-qubit state  $|\hat{\psi}\rangle$ .

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 a NS by employing four of five two-dimensional IRs.

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

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

and their bit-flipped basis vectors, which are obtained by applying  $\sigma_x^{\otimes 5}$  to them in the same manner that Eqs. (3) and (4) are obtained from the basis vectors  $|0\rangle$  and  $|1\rangle$  of  $n = 1$ .

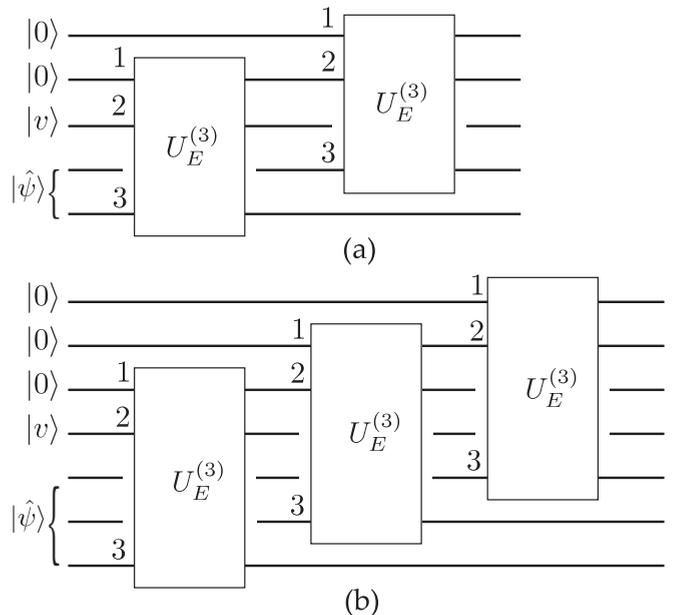


FIG. 3. (a) Encoding circuit  $U_E^{(5)}$  of the 5-qubit NS, which encodes a two-data-qubit state  $|\hat{\psi}\rangle$ . The third and fourth qubits in Eq. (7) are exchanged to make the recursive symmetry manifest in this diagram. (b) Encoding circuit  $U_E^{(7)}$  for the 7-qubit NS, which encodes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

We emphasize the similar structure between Eqs. (7) and Eqs. (3) and (4). This observation makes implementation of the encoding-decoding circuit almost a trivial matter. Note that we do not need to worry about the rest of the basis vectors as long as they are orthogonal to the above basis vectors spanning the NS. This orthogonalization is automatically taken into account by the 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 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).

## V. CONCLUSION

The DFS and NS make use of vector subspaces that 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 for the NS for  $n = 3$  and 5 and the 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 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). We 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 these 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 from 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 two-dimensional IRs for  $n = 2m + 1$ , which encode  $k = \lfloor \log_2[\binom{n}{m} - \binom{n}{m-1}] \rfloor$  qubits. This number  $k$  is greater than  $m$  for  $n \geq 9$  and actually  $k/n \rightarrow 1$  as  $n \rightarrow \infty$ . This asymptotic behavior is also observed in Ref. [10] for the DFS.

Full details of the recursion scheme are beyond the scope of the present paper. Moreover, we plan to present an 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 elsewhere [13].

It was shown that the central qubit in Figs. 1 and 3 can be any state. Although the entropy of the qubit system generally increases, 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 that of the DFS with  $\rho_a = |0\rangle\langle 0|$ , in which the entropy does not change at all.

## ACKNOWLEDGMENTS

C.-K.L. was supported by a US NSF grant, a HK RGC grant, and the 2011 Shanxi 100 Talent Program. M.N. and H.T. were supported by the ‘‘Open Research Center’’ Project for Private Universities with a matching fund subsidy from MEXT. M.N. would like to thank the JSPS (Grant No. 23540470) for partial support of Grants-in-Aid for Scientific Research. Y.-T.P. was supported by a US NSF grant. N.-S.S. was supported by a HK RGC grant.

- 
- [1] M. A. Nielsen 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, 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, and M. Lesosky, *Quantum Inf. Comput.* **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 (unpublished).