Quantum convolutional error-correcting codes

H. F. Chau*
Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong
(Received 27 February 1998)

I report two general methods to construct quantum convolutional codes for N-state quantum systems. Using these general methods, I construct a quantum convolutional code of rate 1/4, which can correct one quantum error for every eight consecutive quantum registers. [S1050-2947(98)07608-2]

PACS number(s): 03.67.Lx, 89.70.+c, 89.80.+h

A quantum computer is more efficient than a classical computer in useful applications such as integer factorization [1] and database search [2]. However, decoherence remains one of the major obstacles to building a quantum computer [3]. Nevertheless, the effect of decoherence can be compensated for if one introduces redundancy in the quantum state. By first encoding a quantum state into a larger Hilbert space H. Then by projecting the wave function into a suitable subspace C of H. And finally by applying a unitary transformation to the orthogonal complement of C according to the measurement result; it is possible to correct quantum errors due to decoherence. This scheme is called the quantum error correction code (QECC) [4]. Many QECCs have been discovered (see, for example, Refs. [4–15]) and various theories on the QECC have also been developed (see, for example, Refs. [8–18]). In particular, the necessary and sufficient condition for a QECC is [16–19]

$$\langle i_{\text{encode}}|\mathcal{A}^{\dagger}\mathcal{B}|j_{\text{encode}}\rangle=\Lambda_{\mathcal{A},\mathcal{B}}\delta_{ij}, \tag{1}$$

where $|i_{\text{encode}}\rangle$ denotes the encoded quantum state $|i\rangle$ using the QECC; $\mathcal{A},\mathcal{B}$ are the possible errors the QECC can handle; and $\Lambda_{\mathcal{A},\mathcal{B}}$ is a complex constant independent of $|i_{\text{encode}}\rangle$ and $|j_{\text{encode}}\rangle$. Note that the above condition for a QECC is completely general, working for finite or infinite number of N-state quantum registers.[1]

All QECCs discovered so far are block codes. That is, the original state ket is first divided into *finite* blocks of the same length. Each block is then encoded separately using a code that is *independent* of the state of the other blocks (cf. Refs. [20,21]).

In addition to block codes, convolutional codes are well known in classical error correction. Unlike a block code, the encoding operation depends on current as well as a number of past information bits [20,21]. For instance, given a (possibly infinite) sequence of classical binary numbers $(a_1,a_2,\ldots,a_m,\ldots)$, the encoding $(b_1,c_1,b_2,c_2,\ldots,b_m,c_m,\ldots)$ with

$$b_i=a_i+a_{i-2}\bmod 2,\quad c_i=a_i+a_{i-1}+a_{i-2}\bmod 2 \tag{2}$$

for all i, and $a_0=a_{-1}=0$ is able to correct up to one error for every two consecutive bits [22].

In classical error correction, good convolutional codes often can encode with higher efficiencies than their corresponding block codes in a noisy channel [20,21]. It is, therefore, instructive to find quantum convolutional codes (QCC) and to analyze their performance. In this paper, I first report a way to construct a QCC from a known quantum block code (QBC). Then I discuss a way to construct a QCC from a known classical convolutional code. Finally, I report the construction of a QCC of rate 1/4, which can correct one quantum error for every eight consecutive quantum registers.

Let me first introduce some notations before I construct QCCs. Suppose each quantum register has N orthogonal eigenstates for $N\geqslant 2$. Then, the basis of a general quantum state consisting of many quantum registers can be written as $\{|\mathbf{k}\rangle\}\equiv\{|k_1,k_2,\ldots,k_m,\ldots\rangle\}$ for all $k_m\in\mathbb{Z}_N$. And I abuse the notation by defining $k_m=0$ for all $m\leqslant 0$.

Suppose $|k\rangle\mapsto\Sigma_{i_1,i_2,\ldots,i_m}a^{(k)}_{i_1,i_2,\ldots,i_m}|i_1,i_2,\ldots,i_m\rangle$ be a QBC mapping one quantum register to a code of length m. Hence, the rate of the code equals $1/m$. The effect of decoherence can be regarded as an error operator acting on certain quantum registers. I denote the set of all possible errors that can be corrected by the above quantum block code by E. Based on this QBC, one can construct a family of QCCs as follows:

Theorem 1. Given the above QBC and a quantum state $|\mathbf{k}\rangle\equiv|k_1,k_2,\ldots,k_n,\ldots\rangle$ making up of possibly infinitely many quantum registers, then the encoding

$$|\mathbf{k}\rangle\equiv|k_1,k_2,\ldots,k_n,\ldots\rangle\mapsto|\mathbf{k}_{\text{encode}}\rangle\equiv\bigotimes_{i=1}^{+\infty}\left[\sum_{j_{i1},j_{i2},\ldots,j_{im}}a^{(\Sigma_p\mu_{ip}k_p)}_{j_{i1},j_{i2},\ldots,j_{im}}|j_{i1},j_{i2},\ldots,j_{im}\rangle\right] \tag{3}$$

forms a QCC of rate $1/m$ provided that the matrix μ_{ip} is invertible. This QCC can handle errors in the form $E\otimes E\otimes\cdots$.

*Electronic address: hfchau@hkusua.hku.hk

[1]Perhaps the simplest way to see that Eq. (1) holds for infinite number of N-state registers is to observe that Gottesman's proof in Ref. [19] does not depend on the finiteness of the Hilbert space for encoded state.

Proof. I consider the effects of errors $\mathcal{E}\equiv\mathcal{E}_1\otimes\mathcal{E}_2\otimes\cdots$ and $\mathcal{E}'\equiv\mathcal{E}'_1\otimes\mathcal{E}'_2\otimes\cdots\in E\otimes E\otimes\cdots$ on the encoded quantum registers by computing

$$\langle\mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle=\prod_{i=1}^{\infty}\left[\sum_{j_{i1},\ldots,j_{im},j'_{i1},\ldots,j'_{im}}\overline{a}^{(\Sigma_{p'}\mu_{ip'}k'_{p'})}_{j'_{i1},\ldots,j'_{im}}a^{(\Sigma_p\mu_{ip}k_p)}_{j_{i1},\ldots,j_{im}}\langle j'_{i1},\ldots,j'_{im}|\mathcal{E}'^{\dagger}_i\mathcal{E}_i|j_{i1},\ldots,j_{im}\rangle\right]. \tag{4}$$

Substituting Eq. (1) into Eq. (4), we have

$$\begin{aligned}\langle\mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle&=\prod_{i=1}^{+\infty}\left[\left\langle\left(\sum_p\mu_{ip}k'_p\right)_{\text{encode}}\middle|\mathcal{E}'^{\dagger}_i\mathcal{E}_i\middle|\left(\sum_p\mu_{ip}k_p\right)_{\text{encode}}\right\rangle\right]\\&=\prod_{i=1}^{+\infty}\left[\delta_{\Sigma_p\mu_{ip}k_p,\Sigma_p\mu_{ip}k'_p}\Lambda_{\mathcal{E}_i,\mathcal{E}'_i}\right]\end{aligned} \tag{5}$$

for some constants $\Lambda_{\mathcal{E}_i,\mathcal{E}'_i}$ independent of $\mathbf{k}$ and $\mathbf{k}'$. Since the matrix μ is invertible, $k_i=k'_i$ for all i is the unique solution of the systems of linear equations $\Sigma_p\mu_{ip}k_p=\Sigma_p\mu_{ip}k'_p$. Consequently,

$$\langle\mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle=\delta_{\mathbf{k},\mathbf{k}'}\Lambda_{\mathcal{E},\mathcal{E}'} \tag{6}$$

for some constant $\Lambda_{\mathcal{E},\mathcal{E}'}$ independent of $\mathbf{k}$ and $\mathbf{k}'$. Thus, the encoding in Eq. (3) is a QECC. □

At this point, readers should realize that the above scheme can be generalized to construct a QCC from a QBC that maps n quantum registers to $m(>n)$ registers. It is also clear that the following two useful corollaries follow directly from theorem 1:

Corollary 1. The encoding scheme given by Eq. (3) gives a QCC from a QBC provided that (1) the elements in the matrix μ are either zeros or ones; (2) μ_{ip} is a function of $i-p$ only; and (3) $\mu_{ip}=\mu(i-p)$ consists of finitely many ones.

Corollary 2. The encoding scheme given by Eq. (3) gives a QCC from a QBC if (1) N is a prime power; (2) μ is not a zero matrix; and (3) μ_{ip} is a function of $i-p$ only.

Let me illustrate the above analysis by an example.

Example 1. Starting from the spin five register code in Ref. [12], one knows that the following QCC can correct up to one error in every five consecutive quantum registers:

$$|k_1,k_2,\ldots,k_m,\ldots\rangle\mapsto\bigotimes_{i=1}^{+\infty}\left[\frac{1}{N^{3/2}}\sum_{p_i,q_i,r_i=0}^{N-1}\omega_N^{(k_i+k_{i-1})(p_i+q_i+r_i)+p_ir_i}|p_i,q_i,p_i+r_i,q_i+r_i,p_i+q_i+k_i+k_{i-1}\rangle\right], \tag{7}$$

where $k_m\in\mathbb{Z}_N$, ω_N is a primitive Nth root of unity, and all additions in the state ket are modulo N. The rate of this code equals 1/5.

Although the QCC in Eq. (3) looks rather complicated, the actual encoding process can be performed readily. Because μ is invertible, one can reversibly map $|k_1,k_2,\ldots,k_n,\ldots\rangle$ to

$$\left|\sum_p\mu_{1p}k_p,\sum_p\mu_{2p}k_p,\ldots,\sum_p\mu_{np}k_p,\ldots\right\rangle$$

[23–25]. Then, one obtains the above five register QCC by encoding each quantum register using the procedure in Ref. [12].

Now, I turn to the construction of QCCs from classical convolutional codes. Let me first introduce two technical lemmas (which work for both QBCs and QCCs).

Lemma 1. Suppose the QECC

$$|\mathbf{k}\rangle\mapsto\sum_{j_1,j_2,\ldots}a^{(\mathbf{k})}_{j_1,j_2,\ldots}|j_1,j_2,\ldots\rangle \tag{8}$$

corrects (independent) spin flip errors in certain quantum registers with $j_i\in\mathbb{Z}_N$. Then, the following QECC, which is obtained by discrete Fourier transforming every quantum register in Eq. (8),

$$\begin{aligned}|\mathbf{k}\rangle\mapsto&\sum_{j_1,j_2,\ldots,p_1,p_2,\ldots}a^{(\mathbf{k})}_{j_1,j_2,\ldots}\\&\times\prod_{i=1}^{+\infty}\left(\frac{1}{\sqrt{N}}\omega_N^{j_ip_i}\right)|p_1,p_2,\ldots\rangle\end{aligned} \tag{9}$$

corrects (independent) phase errors occurring in the same quantum registers. The converse is also true.

Proof. Observe that one can freely choose a computational basis for the encoded quantum state. In particular, if one chooses the discrete Fourier transformed basis $\{|\tilde{m}\rangle\}\equiv\{\Sigma_{j=0}^{N-1}\omega_N^{jm}|j\rangle\}$ for each of the encoded quantum register, then the encoding in Eq. (9) is reduced to the encoding in Eq. (8). Thus, the code in Eq. (9) handles spin flip errors with

respect to the discrete Fourier transformed basis $\{|\tilde{m}\rangle\}$. Consequently, the same code handles phase errors in the original $\{|m\rangle\}$ basis.

Conversely, suppose one chooses the original $\{|m\rangle\}$ basis to encode a phase error correcting code. Then with respect to the $\{|\tilde{m}\rangle\}$ basis, it is easy to check that the same code corrects spin flip errors. □

Lemma 2. Suppose a QECC handles errors E_1 and E_2 satisfying (a) for all $\mathcal{E}_i \in E_i$ $(i=1,2)$, there exists $\mathcal{E}_2' \in E_2$ such that $\mathcal{E}_2^\dagger \circ \mathcal{E}_1 = \mathcal{E}_1^\dagger \circ \mathcal{E}_2'$; and (b) for $\mathcal{E}_i, \mathcal{E}_i' \in E_i (i=1,2)$, $\mathcal{E}_i^\dagger \circ \mathcal{E}_i' \in E_i$ whenever errors $\mathcal{E}_i$ and $\mathcal{E}_i'$ occur at the same set of quantum registers; then the QECC actually handles errors in $E_1 \circ E_2 \equiv \{\mathcal{E}_1 \circ \mathcal{E}_2 : \mathcal{E}_1 \in E_1, \mathcal{E}_2 \in E_2$ and errors $\mathcal{E}_1, \mathcal{E}_2$ occur at the same set of quantum registers$\}$.

Proof. One knows from Eq. (1) that $\langle \mathbf{k}'_{\text{encode}} | \mathcal{E}_i^\dagger \mathcal{E}_i' | \mathbf{k}_{\text{encode}} \rangle = \delta_{\mathbf{k},\mathbf{k}'} \Lambda_{\mathcal{E}_i, \mathcal{E}_i'}$ for some $\Lambda_{\mathcal{E}_i, \mathcal{E}_i'}$ independent of k $(i=1,2)$. Also, Eq. (1) implies that the effect of an error $\mathcal{E}_i$ is simply to rigidly rotate and to contract (or expand) the encoded ket space independent of the state $|\mathbf{k}_{\text{encode}}\rangle$ itself. Thus, one concludes that

$$\langle \mathbf{k}'_{\text{encode}} | (\mathcal{E}_1 + \mathcal{E}_2)^\dagger (\mathcal{E}_1 + \mathcal{E}_2) | \mathbf{k}_{\text{encode}} \rangle = \delta_{\mathbf{k},\mathbf{k}'} \Gamma_{\mathcal{E}_1, \mathcal{E}_2} \tag{10a}$$

and

$$\langle \mathbf{k}'_{\text{encode}} | (\mathcal{E}_1 + i\mathcal{E}_2)^\dagger (\mathcal{E}_1 + i\mathcal{E}_2) | \mathbf{k}_{\text{encode}} \rangle = \delta_{\mathbf{k},\mathbf{k}'} \Gamma'_{\mathcal{E}_1, \mathcal{E}_2} \tag{10b}$$

for all $\mathcal{E}_i \in E_i$ $(i=1,2)$, where $\Gamma_{\mathcal{E}_1, \mathcal{E}_2}$ and $\Gamma'_{\mathcal{E}_1, \mathcal{E}_2}$ are independent of $\mathbf{k}$. By expanding Eqs. (10a) and (10b), one arrives at

$$\langle \mathbf{k}'_{\text{encode}} | \mathcal{E}_1^\dagger \mathcal{E}_2 | \mathbf{k}_{\text{encode}} \rangle = \delta_{\mathbf{k},\mathbf{k}'} \Xi_{\mathcal{E}_1, \mathcal{E}_2} \tag{11}$$

for some $\Xi_{\mathcal{E}_1, \mathcal{E}_2}$ independent of $\mathbf{k}$. Finally, I consider errors $\mathcal{E}_i, \mathcal{E}_i' \in E_i$ $(i=1,2)$ occurring at the same set of quantum registers, then

$$\begin{aligned} \langle \mathbf{k}'_{\text{encode}} | (\mathcal{E}_1' \mathcal{E}_2')^\dagger (\mathcal{E}_1 \mathcal{E}_2) | \mathbf{k}_{\text{encode}} \rangle &= \langle \mathbf{k}'_{\text{encode}} | \mathcal{E}_2'^\dagger \mathcal{E}_1'^\dagger \mathcal{E}_1 \mathcal{E}_2 | \mathbf{k}_{\text{encode}} \rangle \\ &= \langle \mathbf{k}'_{\text{encode}} | \mathcal{E}_1'' \mathcal{E}_2'' | \mathbf{k}_{\text{encode}} \rangle \end{aligned} \tag{12}$$

for some $\mathcal{E}_i'' \in E_i (i=1,2)$. Hence from Eqs. (1) and (11), I conclude that the QECC handles errors in the set $E_1 \circ E_2$. □

The next corollary follows directly from Lemma 2.

Corollary 3. A QECC handles general quantum error if and only if it handles both spin flip and phase errors in the corresponding quantum registers.

Now, I am ready to prove the following theorem regarding the construction of quantum codes from classical codes.

Theorem 2. Suppose QECCs $C1$ and $C2$ handle phase shift and spin flip errors, respectively, for the same set of quantum registers. Then, pasting the two codes together by first encoding the quantum state using $C1$ then further encoding the resultant quantum state using $C2$, one obtains a QECC C that corrects general errors in the same set of quantum registers.

Proof. From Corollary 3, it suffices to show that the new QECC C corrects both spin flip and phase errors. By the construction of C, it clearly can correct spin flip errors. And using the same trick in the proof of Lemma 2, it is easy to check that C can correct phase shift errors as well.

Readers should note that the order of pasting in Theorem 2 is important. Reversing the order of encoding does not give a good quantum code. Also, proofs of Corollary 3 and Theorem 2 for the case of $N=2$ can also be found, for example, in Ref. [9].

Theorem 3. Suppose C is a classical (block or convolutional) code of rate r that can correct p (classical) errors for every q consecutive registers. Then, C can be extended to a QECC of rate r^2 that can correct at least p quantum errors for every q^2 consecutive quantum registers.

Proof. Suppose C is a classical code. By mapping m to $|m\rangle$ for all $m \in \mathbb{Z}_N$, C can be converted to a quantum code for spin flip errors. Let C' be the QECC obtained by Fourier transforming each quantum register of C. Then Lemma 1 implies that C' is a code for phase shift errors. From Theorem 2, pasting codes C and C' together will create a QECC C'' of rate r^2. Finally, one can verify the error correcting capability of C'' readily [26]. □

Theorem 3 is useful to create high rate QCCs from high rate classical convolutional codes. Note that one of the simplest classical convolutional code with rate 1/2 is given by Eq. (2). Being a nonsystematic[2] and non-catastrophic[3] code [22], it serves as an ideal starting point to construct good QCCs. First, let me write down this code in quantum mechanical form:

Lemma 3: The QCC

$$|k_1, k_2, \ldots\rangle \bigotimes_{i=1}^{+\infty} |k_i + k_{i-2}, k_i + k_{i-1} + k_{i-2}\rangle \tag{13}$$

for all $k_i \in \mathbb{Z}_N$, where all additions in the state ket are modulo N, can correct up to one spin flip error for every four consecutive quantum registers.

Proof. Using notations as in the proof of Theorem 1, I consider $\langle \mathbf{k}'_{\text{encode}} | \mathcal{E}'^\dagger \mathcal{E} | \mathbf{k}_{\text{encode}} \rangle$. Clearly, the worst case happens when errors $\mathcal{E}$ and $\mathcal{E}'$ occur at different quantum registers. And in this case, Eq. (13) implies that exactly two of the following four equations hold:

$$\begin{aligned} k_{2i} + k_{2i-2} &= k'_{2i} + k'_{2i-2}, \\ k_{2i} + k_{2i-1} + k_{2i-2} &= k'_{2i} + k'_{2i-1} + k'_{2i-2}, \\ k_{2i+1} + k_{2i-1} &= k'_{2i+1} + k'_{2i-1}, \\ k_{2i+1} + k_{2i} + k_{2i-1} &= k'_{2i+1} + k'_{2i} + k'_{2i-1} \end{aligned} \tag{14}$$

[2]That is, both b_i and c_i are not equal to a_i.

[3]That is, a finite number of channel errors does not create an infinite number of decoding errors.

for all i. One may regard k_i's as unknowns and k_i''s as arbitrary but fixed constants. Then, by straightforward computation, one can show that picking *any* two equations out of Eq. (14) for each i will form an invertible system with the unique solution $k_i=k_i'$ for all i. Thus, $\langle \mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle = \delta_{\mathbf{k},\mathbf{k}'}\delta_{\mathcal{E},\mathcal{E}'}$ and hence this lemma is proved. □

Example 2. Theorem 3 and Lemma 3 imply that the following QCC of rate 1/4:

$$|k_1,k_2,\ldots\rangle \mapsto |\mathbf{k}_{\text{encode}}\rangle \equiv \bigotimes_{i=1}^{+\infty}\left[\sum_{p_1,q_1,\ldots}\frac{1}{N}\omega_N^{(k_i+k_{i-2})p_i+(k_i+k_{i-1}+k_{i-2})q_i}|p_i+p_{i-1},p_i+p_{i-1}+q_{i-1},q_i+q_{i-1},q_i+q_{i-1}+p_i\rangle\right] \tag{15}$$

for all $k_i\in\mathbb{Z}_N$, where all additions in the state ket are modulo N can correct at least one error for every 16 consecutive quantum registers. But, in fact, this code is powerful enough to correct one error for every eight consecutive quantum registers (see also Ref. [26]).

Proof. Let $\mathcal{E}$ and $\mathcal{E}'$ be two quantum errors affecting at most one quantum register per every eight consecutive ones. By considering $\langle \mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle$, I know that at least six of the following eight equations hold:

$$\begin{gathered}
p_{2i-1}+p_{2i-2}=p'_{2i-1}+p'_{2i-2},\\
p_{2i-1}+p_{2i-2}+q_{2i-2}=p'_{2i-1}+p'_{2i-2}+q'_{2i-2},\\
q_{2i-1}+q_{2i-2}=q'_{2i-1}+q'_{2i-2},\\
q_{2i-1}+q_{2i-2}+p_{2i-1}=q'_{2i-1}+q'_{2i-2}+p'_{2i-1},\\
p_{2i}+p_{2i-1}=p'_{2i}+p'_{2i-1},\\
p_{2i}+p_{2i-1}+q_{2i-1}=p'_{2i}+p'_{2i-1}+q'_{2i-1},\\
q_{2i}+q_{2i-1}=q'_{2i}+q'_{2i-1},\\
q_{2i}+q_{2i-1}+p_{2i}=q'_{2i}+q'_{2i-1}+p'_{2i}
\end{gathered} \tag{16}$$

for all $i\in\mathbb{Z}^+$. Let me regard p_i and q_i as unknowns; and p_i' and q_i' as arbitrary but fixed constants. Then, it is straightforward to show that choosing *any* six equations in Eq. (16) for each $i\in\mathbb{Z}^+$ would result in a consistent system having a unique solution of $p_i=p_i'$ and $q_i=q_i'$ for all $i\in\mathbb{Z}^+$. Consequently,

$$\langle \mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle = \sum_{p_1,q_1,p_2,q_2,\ldots}\left\{\prod_{i=1}^{+\infty}\left[\omega_N^{\sum_{j=2i-1}^{2i}p_j(k_j+k_{j-2}-k'_j-k'_{j-2})+q_j(k_j+k_{j-1}+k_{j-2}-k'_j-k'_{j-1}-k'_{j-2})}\times\langle f_i|\mathcal{E}'^{\dagger}_i|f_i\rangle\langle g_i|\mathcal{E}|g_i\rangle\right]\right\} \tag{17}$$

for some linearly independent functions $f_i(p_1,q_1,p_2,q_2,\ldots)$ and $g_i(p_1,q_1,p_2,q_2,\ldots)$.

Now, I consider a basis $\{h_i(p_1,q_1,p_2,q_2,\ldots)\}$ for the orthogonal complement of the span of $\{f_i,g_i\}_{i\in\mathbb{Z}^+}$. By summing over all h_i's while keeping f_i's and g_i's constant in Eq. (17), one ends up with the constraints that $k_i=k_i'$ for all $i\in\mathbb{Z}^+$. Thus,

$$\langle \mathbf{k}'_{\text{encode}}|\mathcal{E}'^{\dagger}\mathcal{E}|\mathbf{k}_{\text{encode}}\rangle = \delta_{\mathbf{k},\mathbf{k}'}\sum_{p_1,q_1,p_2,q_2,\ldots}\left[\prod_{i=1}^{+\infty}\left[\langle f_i(p_1,q_1,\ldots)|\mathcal{E}'^{\dagger}|f_i(p_1,q_1,\ldots)\rangle\langle g_i(p_1,q_1,\ldots)|\mathcal{E}|g_i(p_1,q_1,\ldots)\rangle\right]\right]. \tag{18}$$

Hence, Eq. (15) corrects up to one quantum error per every eight consecutive quantum registers. □

The above rate 1/4 QCC is constructed from a classical convolutional code of rate 1/2. One may further boost up the code performance by converting other efficient classical convolutional codes [such as various $k/(k+1)$-rate codes in Ref. [27]] into QCCs. On the other hand, it is impossible to construct a four quantum register QBC that can correct one quantum error [12,16]. With modification, the same argument can be used to show that no QCC can correct one error

for every four consecutive quantum registers [26]. It is instructive to compare the performances of QBCs and QCCs in other situations.

In addition, in order use QCCs in quantum computation, one must investigate the possibility of fault tolerant computation on them. Moreover, it would be ideal if the fault tolerant implementation of single- and two-quantum register operations must involve only a finite number of quantum registers in the QCC. While a general QCC may not admit a finite fault tolerant implementation, many QCCs with finite memories[4] can be manipulated fault tolerantly.

Example 3. By subtracting those quantum registers containing p_i, p_{i+2}, q_i, q_{i+1}, and q_{i+2} by one in Eq. (15), one ends up with changing $|k_1,k_2,\ldots,k_i,\ldots,_{\text{encode}}\rangle$ to $|k_1,k_2,\ldots,k_{i-1},k_i+1,k_{i+1},\ldots,_{\text{encode}}\rangle$. Clearly, the above operation is fault tolerant and involves only a finite number of quantum registers. Fault tolerant implementation of single register phase shift can be obtained in a similar way. Further results on fault tolerant implementation on QCCs will be reported elsewhere [29].

Finally, decoding a classical convolutional code can be quite involved [28]. So, it is worthwhile to investigate the efficiency of decoding a QCC. I plan to report them in future works [29].

I would like to thank T. M. Ko for introducing me to the subject of convolutional codes. I would also like to thank Debbie Leung, H.-K. Lo, and Eric Rains for their useful discussions. This work is supported by Hong Kong Government RGC Grant No. HKU 7095/97P.

[4]That is, codes with encoding schemes that depend on a finite number of quantum registers in $|\mathbf{k}\rangle$.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundation of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.
[2] L. K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1996), p. 212.
[3] R. Landauer, in *Proceedings of PHYSCOMP94*, edited by D. Matzke (IEEE Computer Society, Los Alamitos, CA, 1994), p. 54.
[4] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).
[5] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[6] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[7] A. M. Steane, Phys. Rev. A **54**, 4741 (1996).
[8] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
[9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
[10] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
[11] H. F. Chau, Phys. Rev. A **55**, 839 (1997).
[12] H. F. Chau, Phys. Rev. A **56**, 1 (1997).
[13] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, Phys. Rev. Lett. **79**, 953 (1997).
[14] S. Llyod and J.-J. E. Slotine, Los Alamos e-print quant-ph/9711021 (1997).
[15] S. L. Braunstein, Los Alamos e-print quant-ph/9711049 (1997).
[16] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[17] E. Knill, Los Alamos e-print quant-ph/9608048 (1996).
[18] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[19] D. Gottesman, Ph.D. thesis, California Institute of Technology, 1997, Chap. 2.
[20] Ph. Piret, *Convolutional Codes: An Algebraic Approach* (MIT Press, Cambridge, MA, 1988).
[21] A. Dholakia, *Introduction to Convolutional Codes with Applications* (Kluwer, Dordrecht, 1994).
[22] See, for example, *Introduction to Convolutional Codes with Applications* (Ref. [21]), Chap. 4.
[23] C. H. Bennett, IBM J. Res. Dev. **17**, 525 (1973).
[24] C. H. Bennett, SIAM J. Comput. **18**, 766 (1989).
[25] H. F. Chau and H.-K. Lo, Cryptologia **21**, 139 (1997).
[26] H. F. Chau (unpublished).
[27] A list of good classical convolutional codes can be found, for example, in Appendix A of Ref. [21].
[28] See, for example, *Introduction to Convolutional Codes with Applications* (Ref. [21]), Chaps. 5–8.
[29] H. F. Chau, Los Alamos e-print quant-ph/9806032.