Vol 18 No 10, October 2009
1674-1056/2009/18(10)/4154–07

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Quantum quasi-cyclic low-density parity-check error-correcting codes*

Li Yuan(李 渊)[a)†], Zeng Gui-Hua(曾贵华)[a)], and Moon Ho Lee[b)]

[a)] *Laboratory of Coding and Communication Security, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, China*

[b)] *Institute of Information & Communication, Department of Information & Communication Engineering, Chonbuk National University, Chonju 561-756, Korea*

(Received 3 September 2007; revised manuscript received 14 October 2008)

In this paper, we propose the approach of employing circulant permutation matrices to construct quantum quasi-cyclic (QC) low-density parity-check (LDPC) codes. Using the proposed approach one may construct some new quantum codes with various lengths and rates of no cycles-length 4 in their Tanner graphs. In addition, these constructed codes have the advantages of simple implementation and low-complexity encoding. Finally, the decoding approach for the proposed quantum QC LDPC is investigated.

Keywords: quantum LDPC code, quasi-cyclic, circulant permutation matrix, CSS code
PACC: 0367, 0365

CPB WITHDRAWN

1. Introduction

Since the initial discovery and the general descriptions of quantum error-correction codes (QECC) were presented,[1−3] QECC have drawn much interest during recent years. The first quantum code which was introduced by Shor in 1995,[4] encoded one qubit into nine qubits and could correct both bit-flip errors and phase-flip errors. Shortly after, it was shown that QECC can be constructed based on the classical block codes. This led to the development of an important class of QECC by Calderbank, Shor and Steane,[5,6] known as CSS codes. Afterwards, a more general quantum code, i.e., stabilizer quantum code, was brought forward by Gottesman.[7] Currently, almost all the advanced code constructions may be categorized as these two classes according to the different construction methods and principles. It has been shown that QECC play an important role in quantum computation,[8] quantum signal processing[9,10] and quantum communication.[11−14]

A class of classical codes called LDPC codes were first proposed by Gallager[15] and more research was renewed many years later.[16] The advantage of LDPC codes is its lower decoding complexity although there is a disadvantage of higher encoding complexity. According to the weight of rows and columns in parity-check matrix, LDPC codes are classified into regular one and irregular one. With the development of quantum information, generalizing this notion to quantum codes is significant. Actually, the quantum LDPC codes have been proposed recently,[17] and Thomas Camarain *et al* proposed a general construction of quantum LDPC codes within the stabilizer formalism in 2005. In these proposed quantum LDPC codes, the decoding evolves pure quantum nature so that the constructed code has some novel properties.

It is well known that the CSS codes may be constructed by two classical linear codes. This motivates us to consider the quantum LDPC codes based on the CSS approach in this paper. In addition, the constructed quantum LDPC codes have lower encoding complexity, subsequently, the corresponding quantum circuit of the constructed quantum LDPC codes is more simple than other kinds of quantum codes. Especially, since the QC LDPC codes are a class of optimal LDPC codes, the quantum LDPC code constructed using classic QC LDPC codes will benefit reducing decoding complexity and encoding complexity of the constructed quantum LDPC codes.

This paper is arranged as follows. In Section 2, we present some preliminaries which are necessary for

*Project supported by the National Natural Science Foundation of China (Grant Nos 60773085 and 60801051), and the NSFC-KOSEF International Collaborative Research Funds (Grant Nos 60811140346 and F01-2008-000-10021-0).
†Corresponding author. E-mail: yuanli@sjtu.edu.cn

the quantum LDPC codes. In Section 3, we investigate the construction and encoding of quantum QC LDPC codes. Then the decoding approaches are presented in Section 4. Finally, the conclusions are drawn in Section 5.

2. Preliminaries

Firstly, we introduce some basic notations on the QECC, especially the stabilizer codes and CSS codes. Let C^2 be a 2-dimensional complex vector space, its tensors product space $H_N = (C^2)^{\otimes N}$ over field $\mathbb{Z}_2$ can be reviewed as code words of binary codes. A quantum code $\mathcal{C}[[N,k]]$ is a subspace of dimension 2^k of the Hilbert space H_N. It is a linear code which encodes vectors from k-dimensional space to N-dimensional space, and its rate is k/N. In a depolarizing channel, there are four basic operators maybe performing on a single qubit, i.e., $I = \sigma_0$, $X = \sigma_x$, $Z = \sigma_z$ and $Y = ZX = \sigma_y$, where $\sigma_0, \sigma_x, \sigma_z, \sigma_y$ are Pauli matrices. Over N qubits, the four operators generate a Pauli group by tensor products,

$$P_N = \{i^\lambda(\omega_1 \otimes \cdots \otimes \omega_N) | \omega_i \in E, 0 \le \lambda \le 3\}. \quad (1)$$

Any pair of elements in P_N are either commutes or anti-commutes.

One important quantum codes is the so-called stabilizer code. This kind of QECC is useful for building quantum fault tolerant circuits. That an operator $M \in P_N$ stabilizes a state can be formally expressed as

$$M|\varphi\rangle = |\varphi\rangle. \quad (2)$$

Let S be an Abelian (i.e. commutative) subgroup of the Pauli group P_N without including $-I$ and $\pm \mathrm{i}\, I$. If quantum code $\mathcal{C} = \{|\varphi\rangle : M|\varphi\rangle = |\varphi\rangle \forall M \in S\}$, then it is a stabilizer code and S is its stabilizer. Furthermore, the quantum Hamming bound[18] of stabilizer code $Q[[N,k,d]]$ which can correct up to $[(d-1)/2]$ errors, satisfies

$$\sum_{l=0}^{[(d-1)/2]} 3^l \binom{N}{l} \le 2^{N-k}. \quad (3)$$

Other kinds of important quantum codes are the CSS codes which are special stabilizer codes. Their construction is based on the properties of two classical linear codes, so the CSS code construction provides a link to classical coding theory. In this paper, we present a CSS code construction employing a pair of QC LDPC codes. Suppose C_1 and C_2 are classical linear codes with parameters $[[N,k_1,d_1]]$ and $[[N,k_2,d_2]]$, respectively. If the two classical codes satisfy some conditions, i.e., $k_2 < k_1$, $C_2 \subset C_1$, both C_1 and $C_2^\perp$ can correct up to t errors, then the resulting CSS codes will be an $C[[N, k_1 - k_2, \min\{d_1, d_2\}]]$ code and also correct t quantum errors. The form of generator matrix of the resulting CSS codes can be expressed as follows:

$$A = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix}, \quad (4)$$

where H_1 and H_2 are parity check matrices of the classical codes C_1 and $C_2^\perp$ respectively. If $C_1 = C_2^\perp$, the obtained CSS code is called self-dual containing.[17,19]

3. Constructions of classical codes for QECC

To construct CSS codes, a pair of classical codes are necessary. Codes are called QC codes if a cyclic shift of any codeword by some positions is still a codeword. In addition, if the parity check matrix of QC codes is a low density matrix, the codes are QC LDPC codes. The characteristic of QC LDPC codes is that, the parity-check matrix consists of small square blocks which are the zero matrix or circulant permutation matrices. Furthermore, QC LDPC codes have good performance for short code length. From Eq.(4), we may know that if the parity check matrices H_1 and H_2 of two classical codes are low density, the parity check matrix A of quantum codes Q is still a low density parity check matrix. Therefore, the corresponding quantum QC LDPC codes should also have more advantage on the encoding process than other kinds of quantum codes.[20,31] In this Section, we construct quantum LDPC codes employing two classical quasi-cyclic codes.

To construct the parity check matrices H_1 and H_2, we need to obtain the circulant permutation matrices. First, we introduce some notions. An $L \times L$ square matrix $P = (p_{ij})$ is called basic-matrix given by

$$p_{ij} = \begin{cases} 1 \text{ if } i = (j+1) \bmod L \\ 0 \text{ otherwise} \end{cases},$$

where L is an odd prime. Obviously, a family of matrices $P^i, 0 \le i \le L-1$ can form a finite cyclic group.

CPB WITHDRAWN

The $mL \times nL$ matrix G is called circulant permutation matrix if it may be denoted by $G = (P^{a_{ij}})_{Lm \times Ln}$, i.e.,

$$G = \begin{pmatrix} P^{a_{11}} & P^{a_{12}} & \dots & P^{a_{1n}} \\ P^{a_{21}} & P^{a_{22}} & \dots & P^{a_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ P^{a_{m1}} & P^{a_{m2}} & \dots & P^{a_{mn}} \end{pmatrix},$$

where $a_{ij}, 1 \le i \le m, 1 \le j \le n$, is the exponent of basic-matrix P. Denote $P^{\infty} = 0_{L \times L}$, $a_{ij} \in \{0, 1, \dots, L-1, \infty\}$, $E(G) = (a_{ij})$ is called exponent matrix of G, i.e.,

$$E(G) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Now, we first consider how to design two circulant permutation matrices G_1 and G_2. According to the theory of group, if L is odd prime, $Z_L = \{0, 1, \dots, L-1\}$ is a field. A set Z_L^* constructed by non-zero elements in Z_L is a cyclic group, and its order should be even. Therefore, Z_L^* may be divided into two subsets averagely, i.e., Z_{L1}^* and Z_{L2}^*. The two subsets satisfy the following conditions:

(i) $|Z_{L1}^*| = |Z_{L2}^*| = l, l = (L-1)/2$.

(ii) $\forall\ a \in Z_{L1}^*, b \in Z_{L2}^*, a \ne b$.

(iii) The elements are $a_i = \sigma^i \mod L$ and $b_i = \tau\sigma^i \mod L$, where $a_i \in Z_{L1}^*, b_i \in Z_{L2}^*$, $\sigma \in Z_L^*, \tau \in Z_L^*/\{\sigma, \sigma^2, \dots\}$ for $1 \le i \le l$.

Now, we will use these elements in the two subsets to obtain exponent matrices $E(G_1) = (a_{ij})$ and $E(G_2) = (b_{ij})$. Assume vectors

$$u_1 = (a_{11}, a_{12}, \dots, a_{1l}), a_{1i} \in Z_{L1}^*,$$

$$v_1 = (b_{11}, b_{12}, \dots, b_{1l}), b_{1j} \in Z_{L2}^*, 1 \le i, j \le l.$$

We get the exponent matrices of circulant permutation matrices $E(G_1)$ and $E(G_2)$ by the following algorithm.

Step 1 Divides $E(G_1)$ into two parties which denoted as square matrices $E(G_{A1})$ and $E(G_{A2})$, i.e., $E(G_1) = (E(G_{A1}), E(G_{A2}))$.

Step 2 Let vector $u_1 = (\sigma, \sigma^2, \dots, \sigma^l)$ be first row of matrix $E(G_{A1})$. With the clockwise (or anticlockwise) permutation of positions in vector u_1, one may create the second row vector u_2 of $E(G_{A1})$. After l times, the $E(G_{A1})$ is obtained.

Step 3 Assume that row vector u_1' obtained from some permutation of u_1 is the first row of $E(G_{A2})$. The second row u_2' of $E(G_{A2})$ may be created by anticlockwise (or clockwise) permutation of positions from the u_1'. In the same way, one may get another matrix divided matrix $E(G_{A2})$.

Step 4 Combining $E(G_{A1})$ and $E(G_{A2})$, an exponent matrix $E(G_1)$ is achieved.

Step 5 Let $b_{is} = \tau_1 a_{is}, 1 \le s \le l$ and $b_{it} = \tau_2 a_{it}, l+1 \le t \le 2l$ with $\tau_\delta \in Z_L^*/\{\sigma, \sigma^2, \dots\}$ $(\delta = 1, 2)$ and $\tau_1 \ne \tau_2$. According to mapping $a_{ij} \to b_{ij}$, another exponent matrix $E(G_2)$ is obtained in a similar way as that for $E(G_1)$.

Step 6 Combining exponent matrices described above with basic-matrix, the circulant permutation matrices G_1, G_2 can be generated.

Example 1 Let $L = 7, (Z_1^* = \{1, 2, \dots, 6\})$, one may get $l = (L-1)/2 = 3$, $Z_{A1}^* = \{1, 2, 4\}$ and $Z_{A2}^* = \{3, 5, 6\}$. Therefore, $u_1 = (2, 4, 1)$, $u_1' = (1, 2, 4)$, and the exponent matrix $E(G_1)$ is

$$E(G_1) = \begin{pmatrix} G_{A1} & G_{A2} \end{pmatrix} = \begin{pmatrix} 2 & 4 & 1 & 1 & 2 & 4 \\ 1 & 2 & 4 & 2 & 4 & 1 \\ 4 & 1 & 2 & 4 & 1 & 2 \end{pmatrix}.$$

Let $\tau_1 = 3$ and $\tau_2 = 5$, then the mapping is $3a_{is} = b_{is}, 1 \le s \le 3$, $5a_{it} = b_{it}, 4 \le t \le 6$. Therefore, the exponent matrix G_2 is obtained by

$$E(G_2) = \begin{pmatrix} 6 & 5 & 3 & 5 & 3 & 6 \\ 3 & 6 & 5 & 3 & 6 & 5 \\ 5 & 3 & 6 & 6 & 5 & 3 \end{pmatrix}.$$

Combining the two exponent matrices and the 7 by 7 basic-matrix P, circulant permutation matrices G_1 and G_2 are obtained.

In the following, we investigate how to generate two $(N - k_i) \times N$ $(i = 1, 2)$ parity check matrices using two circulant permutation matrices. And then, we will show how to construct the quantum QC LDPC codes.

Lemma 1 If circulant permutation matrices G_1 and G_2 are created by using the algorithm presented above, then any rows of G_1 is orthogonal to all rows of G_2, i.e., $G_1 \cdot G_2^{\mathrm{T}} = \mathbf{0}$, where G_2^{T} is the transpose matrix of G_2 and $\mathbf{0}$ is a zero matrix.

Proof Let $E(G_1)$ and $E(G_2)$ denote two exponent matrices of circulant permutation matrices G_1 and G_2, and L be a prime number. In terms of the QC quantum codes construction algorithm described previously, one may know that the mapping between Z_{L1}^* and Z_{L2}^* for $Z_{L1}^* \cup Z_{L2}^* = Z_L^*$ is a one-to-one mapping.

Take any two row vectors $x = (x_{a1}, x_{a2})$ and $y = (y_{b1}, y_{b2})$ of $E(G_1)$ and $E(G_2)$ respectively, where

CPB WITHDRAWN

$|x_{aj}| = |y_{bj}| = l = (L-1)/2,\ j = 1, 2$. Denote $\sigma \in Z_L^*, \tau \in Z_L^*/\{\sigma, \sigma^2, \dots\}$. Assume that a cyclic group $\mathbb{H} = \{\tau, \tau\sigma, \tau\sigma^2, \dots, \tau\sigma^{L-1}\}$ is a subspace of Z_L^*. According to the chosen parameters σ and τ, suppose that the elements of $E(G_1)$ and $E(G_2)$ are σ^i and $\tau\sigma^i$ for $0 \le i \le L-1$, respectively. One may know that the inner product of any x_{ai} and y_{bi} in the two vectors x and y is 0 or 1. However, one may know that $\tau\sigma^i/\sigma^{i'} = \tau\sigma^{i''}$ for $1 \le i', i'' \le L-1$ is the element of $\mathbb{H}$. Therefore, in terms of the one-to-one mapping, the result 0 and 1 of inner product appear contemporarily in the two divided matrices $E(G_{A1})$ and $E(G_{A2})$ (or $E(G_{B1})$ and $E(G_{B2})$). Subsequently, the inner product of rows x and y should always be 0 for mode 2. Therefore, one may get that any row of G_1 is orthogonal to all rows of G_2, i.e., $G_1 \cdot G_2^{\mathrm{T}} = \mathbf{0}$. □

Lemma 2 Let H_1 and H_2 be the parity check matrices of two classical codes C_1 and $C_2^{\perp}$ respectively. If any rows in H_1 are orthogonal to any rows in H_2, the linear codes C_1 and C_2 can construct a quantum code.

Proof If any rows of H_1 and H_2 are orthogonal mutually, i.e., $\langle a, b\rangle = 0, \forall a \in H_1, \forall b \in H_2$, one gets that $H_1 \cdot b^{\mathrm{T}} = 0, \forall b \in C_2$. Therefore, the cause $C_2 \subset C_1$ is satisfied and a quantum code can be obtained by the two classical codes. □

With the Hamming bound (3) and $k_2 < k_1$, one may obtain the following theorem.

Theorem 1 Using the constructed circulant permutation matrices, quantum codes $\mathcal{C}$ with parameter $[[N, k, d]]$ may be constructed.

Proof Let parameters be $k_2 < k_1$. According to the Hamming bound (3), one chooses properly $N - k_i$ $(i = 1, 2)$ rows of G_i as parity check matrix H_i. From Lemma 1, it is orthogonal between any rows in H_1 and H_2. With $k_2 < k_1$ and Lemma 2 we can gain quantum codes $\mathcal{C}$ with parameter $[[N, k, d]]$. □

As designed previously, if there is "∞" in exponent matrix, and let $\tau_1 = \tau_2$, then QC LDPC can also be obtained by the non-zero matrix.

Example 2 In example 1, if replace element $\tau = 3$ in exponent matrices with ∞, then we can get the following exponent matrices $E(G_1)$ and $E(G_2)$

$$E(G_{A1}) = \begin{pmatrix} 2 & 4 & \infty & \infty & 2 & 4 \\ \infty & 2 & 4 & 2 & 4 & \infty \\ 4 & \infty & 2 & 4 & \infty & 2 \end{pmatrix}. \tag{5}$$

According to function $b_{ij} = 3a_{ij}$, then $E(G_2)$ is,

$$E(G_{A2}) = \begin{pmatrix} 6 & 5 & \infty & \infty & 6 & 5 \\ \infty & 6 & 5 & 6 & 5 & \infty \\ 5 & \infty & 6 & 5 & \infty & 6 \end{pmatrix}. \tag{6}$$

The parity check matrices H_1 and H_2 can also be taken from G_1 and G_2 which is based on the basic matrix and exponent matrices designed above. We show this fact with the following cause.

Theorem 2 Now, suppose the non-zero exponent matrices based on the described previous principles, consider the following mapping,

$$x \to \infty, \infty \to y \tag{7}$$

with $x \in Z_{L_1}^*, y \in Z_{L_2}^*$. If take the proper parameters k_1 and k_2, the quantum codes $\mathcal{C}[[N, k, d]]$ may be obtained.

Proof Denote $x = (x_{a1}, x_{a2})$ and $y = (y_{b1}, y_{b2})$, where $|x_{a1}| = |y_{b1}| = l$. In terms of the features of basic-matrix P and mapping (7), same value of inner product between x_{ai} $(i = 1, 2)$ and y_{bi} appears always contemporarily. Therefore, it induces that $\langle x, y\rangle = 0$. According to Lemma 1, condition $C_2 \subset C_1$ may be satisfied. Furthermore, if take proper parameters k_1, k_2, the condition $k_2 < k_1$ also can be ensured. Let two classical codes C_1 and C_2 be with parameters $[[N, k_1, d_1]]$ and $[[N, k_2, d_2]]$. According to Lemma 2, quantum QC LDPC codes $\mathcal{C}[[N, k, d]]$ based on codes C_1, C_2 can be obtained, where $k = k_1 - k_2$ and $d = \min\{d_1, d_2\}$. □

Because G_1 and G_2 are l by $2l$ matrices, the classical codes rate will not be more than 1/2 if based on the above design, regardless that there is ∞ or not in exponent matrices. In the following, we provide codes with various code lengths so that various rates with no cycles of length 4 in their Tanner graph. To adjust the code rate and code length, we can use the following method.

Let corresponding exponent chain of two of cycles be represented as follows:

$$a_1 \to a_2 \to \dots\ a_{2l} \to a_1 \text{ or } (a_1, a_2, \dots, a_{2l}, a_1).$$

Corollary 1 Suppose $(a_1, a_2, \dots, a_{2l}, a_1)$ be the exponent chain corresponding to a block-cycle. Let r be the least positive integer, if repeating r cycle times, such that

$$r\sum_{i=1}^{2l}(-1)^{i-1}a_i \equiv 0 \bmod L, \tag{8}$$

CPB WITHDRAWN

then the block-cycle leads to a cycle of length $2lr$.

Proof Let length $2l$ of matrix as a cycle of exponent matrix, denoted as $E_\lambda(G_i), \lambda = 1, \ldots, r$. First we consider columns from 1 to l. According to the relation of P^{a_i} and P^{a_i+1} corresponding to some $E_\delta(G_i), 1 \le \delta \le r$, the "1" of the j-th row in P^{a_i} is located at the $j + \sum_{i=2}^{l}(-1)^k a_k$-th row in a row block $(i = 2, 3, \ldots, l)$ and the last is $(j + a_2 - a_3 \ldots a_{2l} - a_1)$. Similarly, we can also analyze the remaining columns from $l+1$ to $2l$. Repeating this procedure r times, the "1" of the j-th row in row block is connected to the "1" at the $j + r\sum_{i=1}^{2l}(-1)^i a_i$-th row of P^{a_1} in row block. This procedure may be represented by the following chain

$$\underbrace{P^{a_1} \to P^{a_2} \to \ldots P^{a_{2l}}}_{r \text{ times}} \to P^{a_1}. \tag{9}$$

By the assumption of (9), we also have

$$j \equiv j + r\sum_{i=1}^{2l}(-1)^i a_i \bmod L. \tag{10}$$

Let every $2l$ length of matrix be designed as before, and choose a suitable parameter τ_i and τ_{i+1} building the relation between two circulant permutation matrices. Therefore, the block-cycle leads to a cycle of length $2lr$. According to different r, we can get various code lengths so that various rates. □

Furthermore, we consider quantum self-dual containing codes of construction based on QC LDPC codes and have the following result.

Corollary 2 There is no self-dual containing quantum QC-LDPC code based on the construction described above.

Proof Suppose C_1, C_2 are linear classical codes which are used to construct a self-dual containing quantum code. It means $C_1 = C_2^{\perp}$. According to the condition about CSS code, it implies that the parameters k_1, k_2 should be $0 \le k_1 < k_2 \le m$. Therefore, the condition $C_1 = C_2^{\perp}$ cannot be obtained. □

Finally, the distance and girth of the Tanner graph should be considered. Combining all column vectors in a block matrix, it will be a column vector of which every element is 1. It must be linear for two vectors are combining $2l$ column vectors of two block matrices. Therefore, the distance d will not be greater than $2l$. On the other hand, according to the design of classical QC-LDPC codes, we know that every exponent matrix is divided into two parties. Therefore, there must be $\binom{l}{2} \ge 2$, i.e., $L \ge 7$ and the girth of the Tanner graph of provided parity check matrix is greater than or equal to six.

From the previous analysis, the circulant permutation matrices G_1 and G_2 can be used to construct quantum QC-LDPC codes. In terms of the characters of circulant permutation matrices, the constructed quantum codes have advantage of simple implementation and low-complexity encoding. In the following, we will show the detail of how to encode the quantum codes with the constructed G_1 and G_2.

Firstly, one chooses $N - k_1$ and $N - k_2$ rows in the two circulant permutation matrices according to the Hamming bound in Section 1. Furthermore, the distance d can be calculated by the number of the independent lines of the check matrix H_{N-k_1} and H_{N-k_2}. Subsequently two classical codes $C_1[[N, k_1, d_1]]$ and $C_2[[N, k_2, d_2]]$ may be obtained.

Any quantum codeword $x \in C_1$, quantum state $|x + C_2\rangle$ can be expressed as,

$$|x + C_2\rangle \equiv \frac{1}{2^{k_2/2}} \sum_{y \in C_2} |x + y\rangle. \tag{11}$$

The right of the above equation satisfies the computation of mold 2 in F_2. If take all of the quantum codewords in C_1, the number of orthogonal state $|x + C_2\rangle$ is $n = 2^{k_1 - k_2}$. Therefore, we can get a set which includes different states,

$$\Omega = \{|x_0 + C_2\rangle, |x_1 + C_2\rangle, \ldots, |x_{n-1} + C_2\rangle\}. \tag{12}$$

Therefore, $k_1 - k_2$ qubits overlap state is obtained as

$$|\psi\rangle = \alpha_0|0 \ldots 00\rangle + \alpha_1|0 \ldots 01\rangle + \cdots + \alpha_{n-1}|1 \ldots 11\rangle. \tag{13}$$

Then, one transforms $|\psi\rangle$ as a codes system of qubits overlap state

$$|\varphi\rangle = \alpha_0|x_0 + C_2\rangle + \cdots + \alpha_{n-1}|x_{n-1} + C_2\rangle. \tag{14}$$

Therefore, from two classical liner codes C_1 and C_2, we may get quantum codes $\mathcal{C}[[N, k, d]]$, where $k = k_1 - k_2$ and $d = \min\{d_1, d_2\}$. For instant, the check matrices H_1, H_2 which are obtained from Example 1 and the corresponding codes, can correct one error. If one chooses k_1 and k_2 which satisfy the Hamming bound such as $k_1 = 17$, $k_2 = 15$, and the distance $d = 12$, one can get the quantum codes $[[42, 2, 12]]$. There will be 2^{17} code vectors in C_2, and 2^{15} in C_1. One may hence get $2^{k_1 - k_2} = 2^2$ states $|s_0\rangle \ldots |s_{2^2-1}\rangle$ which can be denoted as $|s_i\rangle = |x + C_2\rangle, (0 \le i \le 2^2 - 1)$, regardless of $x \notin C_2$, or $x \in C_2$. Finally, the quantum

CPB WITHDRAWN

error-corrected coding set can be transformed as the following encoded coding,

$$|\varphi\rangle = \alpha_0|s_0\rangle + \alpha_1|s_1\rangle + \alpha_2|s_2\rangle + \alpha_3|s_3\rangle. \quad (15)$$

And then the encoded coding is sent into the depolarizing channel. The receiver will decode his received quantum codes. In the following Section, we show how to decode the presented quantum codes.

4. Decoding of the presented codes

Suppose the liner coding sets C_1 and C_2 can correct t qubits error, we will show how the CSS codes constructed by C_1 and C_2 correct most t bit-flip and phase-flip errors.

4.1. Error detection

As to the decoding of quantum CSS codes, we first consider the state (11). Because $x \in C_1$, and $C_2 \subset C_1$, we have

$$xH_1^{\mathrm{T}} = 0, \quad yH_1^{\mathrm{T}} = 0, \quad \forall y \in C_2. \quad (16)$$

On the other hand, if vector e_i denotes i-th flipped qubits and the encoded code is state in Eq.(11), then that we accepted is

$$|\varphi_1\rangle = \frac{1}{2^{k_2/2}} \sum_{y \in C_2} |x + y + e_i\rangle. \quad (17)$$

According to the syndrome of vector $x + y + e_i$ corresponding to the state in Eq.(11), even $y \notin C_2$, the following result can also be obtained

$$(x + y + e_i)H_1^{\mathrm{T}} = xH_1^{\mathrm{T}} + yH_1^{\mathrm{T}} + e_iH_1^{\mathrm{T}} = e_iH_1^{\mathrm{T}}. \quad (18)$$

Because the linear codes set C_1 can correct t errors, the syndromes $e_1H_1^{\mathrm{T}}, e_2H_1^{\mathrm{T}}, \ldots, e_NH_1^{\mathrm{T}}$ corresponding to the only one error are all different. Clearly, according to classical method of error correcting coding, we will know that the error happens on the i-th qubit by computing the syndrome $e_iH_1^{\mathrm{T}}$ in the accepted information state $|\varphi_1\rangle$.

4.2. Error correction

From the process of error detection, we can know which position qubit has flipped. The errors of flipped qubit include: bit-flip error (X error), phase-flip error (Z error), and the case of two kinds of errors happened contemporarily. Now, we discuss how to correct the error.

To bit-flip error, we only impose X-Gate on the qubit on which the error happened, the error will be corrected. For instance, if two classical codes $C_1[[42, 17, 12]]$ and $C_2[[42, 15, 12]]$ can correct one error, the constructed quantum code based on C_1 and C_2 is $\mathcal{C}[[42, 2, 12]]$ can also correct one error. The circuit of measuring on the X error syndrome can be expressed as shown in Fig.1.

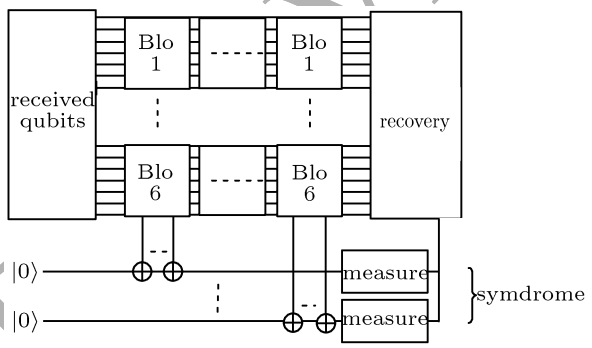


Fig.1. Circuit correcting X errors of qubit encoded in [[42,2,12]] code, where Blo denotes block matrix, and there are 17 Blos i ($i = 1, \ldots, 6$) in circuit every qubits.

Operating a Hadamard transition on a single state $|x\rangle$ yields

$$|x\rangle \xrightarrow{\text{Hadamard}} \frac{1}{2^N} \sum_{y \in \{0,1\}^N} (-1)^{x \cdot y} |y\rangle. \quad (19)$$

Now, we impose Hadamard transition on every qubits in the state $|\varphi_1\rangle$ by applying coding. With Eq.(11), one obtains

$$|\varphi_2\rangle = \frac{1}{2^{k_2/2} 2^{N/2}} \sum_{x \in \{0,1\}^N} \sum_{y \in C_2} (-1)^{(x+y)z} |z\rangle. \quad (20)$$

According to the linearity of liner coding sets C_2, and

$$\sum_{y \in C_2} (-1)^{y \cdot z} = \begin{cases} 2^{k_2} & \text{if } z \in C_2^{\perp}, \\ 0 & \text{if } z \notin C_2^{\perp}, \end{cases} \quad (21)$$

$|\varphi_2\rangle$ may become

$$|\varphi_3\rangle = \frac{2^{k_2/2}}{2^{N/2}} \sum_{z \in C_2^{\perp}} (-1)^{x \cdot z} |z\rangle. \quad (22)$$

Therefore, if the phase-flip happened in the i-th qubit in the state $|x + C_2\rangle$, the following state may be obtained

$$|\varphi^{(i)}\rangle = \frac{1}{2^{k_2/2}} \sum_{y \in C_2} (-1)^{(x+y)e_i} |x + y\rangle. \quad (23)$$

CPB WITH VN

To impose Hadamard transition on every qubits in the above equation, one may get

$$\frac{1}{2^{k_2/2}2^{N/2}}\sum_{z\in\{0,1\}^N}\sum_{y\in C_2}(-1)^{(x+y)(e_i+z)}|z\rangle$$
$$=\frac{1}{2^{k_2/2}2^{N/2}}\sum_{z'\in\{0,1\}^N}\sum_{y\in C_2}(-1)^{(x+y)z'}|e_i+z'\rangle, \quad (24)$$

where $z'=e_i+z$. Applying expression (19) again, we also obtain

$$|\varphi_h\rangle=\frac{2^{k_2/2}}{2^{N/2}}\sum_{z'\in C_2^{\perp}}(-1)^{(x\cdot z')}|z'+e_i\rangle. \quad (25)$$

From the above cause, the phase-flip error can be turned as bit-flip error through the Hadamard transition. Therefore, to the state $|\varphi_h\rangle$, we only correct the bit-flip error, then the phase-flip error can be corrected. In fact, we apply the parity check matrix H_2 of coding set $C_2^{\perp}$ to solve the syndrome of the vector $z'+e_i$ corresponding to the state $|z'+e_i\rangle$. Because $C_2^{\perp}$ can correct t errors, from the syndrome, we can detect the error e_i and correct it. At last, the state is achieved

$$|\varphi_0\rangle=\frac{2^{k_2/2}}{2^{N/2}}\sum_{z'\in C_2^{\perp}}(-1)^{(x+y)z'}|z'\rangle, \quad (26)$$

and then imposes Hadamard transition on every qubits in Eq.(26) again, one will get the original information.

Finally, if the two kinds of flipped errors happen contemporarily, we only correct the bit-flip error because this process includes the correction to the phase-flip error. To the two classical codes C_1 and C_2 with parameters $[[42,17,12]]$ and $[[42,15,12]]$, the CSS code error correction circuit system is described as shown in Fig.2. From the description, regardless of the bit-flip or phase-flip error, one can correct t errors with the quantum circuit.

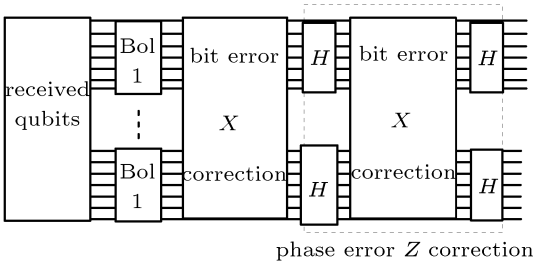


Fig.2. CSS code [[42,2,12]] error correction circuit, where Blo denotes block matrix.

5. Conclusion

In this paper, we proposed a method of employing the classical codes to construct the quantum QC LDPC codes. From the design of the presented codes, it can be efficiently constructed with the short codeword length. We showed that the constructions provide codes with various lengths and rates with no cycles of length 4 in their Tanner graph. This approach can be directly extended to other quantum LDPC codes. According to the features of LDPC codes, the presented codes have the advantage of simple implementation and low complexity encoding.

CPB WITHDRA

References

[1] Ashikhmin A E, Barg A M, Knill E and Litsyn S N 2000 *IEEE Trans. Inf. Theory* **46** 778

[2] Calderbank A R, Rains E M and Shor Phys P W 1997 *Phys. Rev. Lett.* **76** 405

[3] Calderbank A R and Shor P 1996 *Phys. Rev.* A **54** 1098

[4] Shor P W 1995 *Phys. Rev.* A **52** 2493

[5] Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098

[6] Steane A M 1996 *Phys. Rev. Lett.* **77** 793

[7] Gottesman D 1997 *Stabilizer Codes and Quantum Error Correction* PhD thesis, California Institute of Technology, Pasadena

[8] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[9] Ahlswede R and LÄober P 2001 *IEEE. Trans. Inform. Theory* **47** 474

[10] Bowen G. 2004 *IEEE. Trans. Inform. Theory* **50** 2429

[11] Lo H K and Chau H F 1999 *Science* **283** 2050

[12] Li Y, Zeng G H, Yao W and Lee M 2009 *Opt. Rev.* **16** 229

[13] Guo Y and Zeng G H 2007 *Chin. Phys* **16** 2549

[14] Li Y and Zeng G H 2007 *Chin. Phys* **16** 2875

[15] Gallager R G 1962 *IRE Trans. Inform. Theory* **8** 21

[16] MacKay D J C and Neal R M 1996 *Electron. Lett.* **32** 1645

[17] MacKay D J C, Mitchison G and McFadden P L 2004 *IEEE Trans. Inform. Theory* **50** 2315

[18] Feng K and Ma Z 2004 *IEEE Trans. Inform. Theory* **50** 3323

[19] Hamada M 2005 *IEEE Trans. Inform. Theory* **51** 4263

[20] Li Z W, Chen L, Zeng L Q, Lin S and Fong W H 2006 *IEEE Trans. Commun.* **54** 71

[21] Richardson T J, Shokrollahi A and Urbanke R 2001 *IEEE Trans. Inform. Theory* **47** 619