# Jointly-check iterative decoding algorithm for quantum sparse graph codes*

Shao Jun-Hu(邵军虎), Bai Bao-Ming(白宝明)†,
Lin Wei(林 伟), and Zhou Lin(周 林)

*State Key Lab of Integrated Service Networks, Xidian University, Xi'an* 710071, *China*

(Received 12 October 2009; revised manuscript received 22 March 2010)

For quantum sparse graph codes with stabilizer formalism, the unavoidable girth-four cycles in their Tanner graphs greatly degrade the iterative decoding performance with a standard belief-propagation (BP) algorithm. In this paper, we present a jointly-check iterative algorithm suitable for decoding quantum sparse graph codes efficiently. Numerical simulations show that this modified method outperforms the standard BP algorithm with an obvious performance improvement.

**Keywords:** quantum error correction, sparse graph code, iterative decoding, belief-propagation algorithm

**PACC:** 0367, 2841C, 0210

## 1. Introduction

Quantum error correction (QEC) coding is a vital technique in protecting quantum information against decoherence noise, which can be widely used in quantum information systems such as quantum fault-tolerant computation, quantum communication and entanglement distillation.[1−3] Devising good error correction codes has been an important problem of information and coding theory either in classical field or in quantum field.[4−8] Fortunately, the existence of good quantum codes has been proved.[9]

In classical coding theory, low-density parity-check (LDPC) codes and Turbo codes are two classes of sparse graph codes with capacity-approaching performance, both of which can be decoded efficiently with iterative decoding algorithm.[10] While in quantum coding theory, feasibility of QEC mechanism and quantum belief-propagation (QBP) algorithm make quantum sparse graph codes possible to be practical good quantum codes.[11] Stabilizer code (also known as additive code) is an important class of QEC codes with simple formalism, which can be constructed from classical codes.[12,13]

The existing quantum sparse graph codes can be classified into three categories: namely CSS stabilizer structure, general stabilizer structure (Non-CSS), and non-additive codes.[14] In this paper, we mainly concentrate on stabilizer sparse graph codes. Based on CSS structure, many construction methods have been proposed such as dual-containing CSS codes with random sparse cyclic matrices,[6] quantum LDPC code constructed with algebraic method,[15] finite geometry method,[16] and so on.[17−19] Due to the special structure of CSS codes, a separate decoding strategy can be implemented on their component classical codes. However, the flexibilities in coderates and performances of these codes are limited by their construction methods. Therefore non-CSS quantum LDPC codes with more flexible rates and better performance have been proposed recently.[20−22]

In either classical or quantum coding theory, efficient decoding algorithm (with good decoding performance and low complexity) is an important criterion for code applications. And some heuristic methods introduced to break the symmetric problem in decoder improve the decoding performance of quantum sparse graph codes.[23] It is well known that the iterative decoding process of the BP algorithm can be described visually by using the Tanner graph. Unluckily there exist unavoidable grith-four cycles in the Tanner graph of quantum stabilizer codes, which greatly degrade their BP decoding performance. For codes with CSS structure, well-devised component codes can avoid this problem; but for general structure quantum codes, efficient decoding method is still required.

*Project supported by the National Natural Science Foundation of China (Grant No. 60972046) and Grant from the National Defense Pre-Research Foundation of China.
†Corresponding author. E-mail: bmbai@mail.xidian.edu.cn
© 2010 Chinese Physical Society and IOP Publishing Ltd

Inspired by the issues above and the classical coding techniques in Ref. [24], we give a modified QBP decoding method for quantum sparse graph codes. By choosing some stabilizer generators involved in girth-four cycles into jointly-check pairs, the convergence of the iterative decoding process can be improved. On the other hand, this modified method can also compromise the symmetric degeneracy problem in the decoder. To illustrate the effect of this jointly-check strategy, we simulate some available quantum LDPC codes with different algorithms. Numerical simulation results show that an improved decoding performance can be obtained with the method presented in this paper.

The rest of the paper is organized as follows. In Section 2, we review the basic stabilizer theory and principle of sparse graph QEC codes. And Section 3 describes the jointly-check iterative decoding algorithm for quantum sparse graph codes. In Section 4 some illustrating simulation results are given. Finally in Section 5, we make a conclusion from the present study in this paper.

# 2. Stabilizer formalism and quantum sparse graph codes

In this section, we first present some notations used in this paper and a brief review of the basic stabilizer theory. Then quantum stabilizer sparse graph codes are defined together with their Tanner graph characteristics. For more details about stabilizer code theory, we refer the readers to Ref. [25]–[27].

## 2.1. Notation

In this paper, we denote single qubit state by $|\varphi\rangle$ and $n$-qubits state by $|\psi\rangle$. Error on single qubit can be described by Pauli group $\mathbb{G}_1 = \{I, X, Z, Y\}$. And error on $n$-qubits is denoted by group $\mathbb{G}_n$, which is $n$-fold tensor product of single qubit errors.

**Lemma 1** Two elements of $\mathbb{G}_1$ commute if and only if one of them is $I$ or they are equal. Any two elements from group $\mathbb{G}_n$ commute if and only if there is an even number of anti-commuting components between them.

In the subsequent parts of this paper, we use symbol "$\circ$" for the commutativity operator between elements $P_1, P_2 \in \mathbb{G}_n$, i.e., $P_1 \circ P_2 = 0$ when they commute and $P_1 \circ P_2 = 1$ if they anti-commute.

## 2.2. Stabilizer code theory

Stabilizer code $[[n, k]]$ is defined as vector space $V_s$ stabilized by a subgroup $\mathcal{S}$ of $\mathbb{G}_n$ such that $-I \notin \mathcal{S}$ and $\mathcal{S}$ has $n-k$ linearly independent and commuting operators $\boldsymbol{z}_1, \boldsymbol{z}_2 \ldots \boldsymbol{z}_{n-k}$.[26] It is convenient to describe stabilizer generators by binary symplectic matrix $\boldsymbol{A}_{GF(2)}$ over $GF(2)$ or self-orthogonal quaternary matrix $\boldsymbol{A}_{GF(4)}$ over $GF(4)$. And these matrices are called quantum check matrices, which can be used to do encoding and decoding operations of QEC codes.

Conventionally we take finite field $GF(4) = \{0, 1, \omega, \omega^2\}$ with $\omega^2+\omega+1 = 0$ and $\bar{\omega} = \omega^2$. The mapping relationship between Pauli matrices and $GF(4)$ elements can be shown in Table 1.

**Table 1.** Mapping relationship between Pauli matrix and GF(4) element.

| Pauli matrix | $I$ | $X$ | $Z$ | $Y$ |
|---|---|---|---|---|
| $GF(4)$ element | 0 | 1 | $\omega$ | $\omega^2$ |

Then quantum check matrix in $GF(4)$ form can be written as

$$\boldsymbol{A}_{GF(4)} = (\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_{n-k})^{\mathrm{T}}, \tag{1}$$

which is self-orthogonal with respect to trace inner product over $GF(4)$. Decoding of quantum sparse graph code is performed on $GF(4)$.

The CSS code is a special class of stabilizer code with the following check matrix structure:

$$\boldsymbol{A}_{GF(2)} = \left(\begin{array}{c|c} \boldsymbol{H}_1 & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{H}_2 \end{array}\right)_{(n-k)\times 2n}, \tag{2}$$

where $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ satisfy $\boldsymbol{H}_1\boldsymbol{H}_2^{\mathrm{T}} = 0$. When $\boldsymbol{H}_1 = \boldsymbol{H}_2$, there comes a dual-containing (also as weakly self-dual) CSS code. More theories about stabilizer code can been found in Refs. [6], [26] and [27].

## 2.3. Quantum sparse graph codes

Just as their classical counterpart, the sparseness characteristics of quantum sparse graph codes make them more feasible to be practical good quantum codes. Each row in quantum check matrix $\boldsymbol{A}$ represents a quantum check equation, i.e. a check node in its Tanner graph. Tanner graph plays an important role in decoding sparse graph codes. Different from classical cases, the messages propagating in Tanner graph of quantum codes are probability messages of qubit errors.

As an example, we depict the Tanner graph of the famous [[5, 1]] QEC code in Fig. 1. Check node $\boldsymbol{z}_i$ corresponds to the $i$-th stabilizer generator, and variable node $x_j$ corresponds to the $j$-th qubit. An edge connecting a check node $\boldsymbol{z}_i$ and a variable node $x_j$ indicates that the $i$-th row of quantum check matrix $\boldsymbol{A}_{GF(4)}$ has a nonzero value over $GF(4)$ (i.e. a non-identity matrix in $\mathbb{G}_1$). A cycle is defined as a closed path with edges starting and ending at the same node position. The length of the shortest cycle is called the girth. We can see from Fig. 1 that there are many girth-four cycles as illustrated in the following Lemma 2.

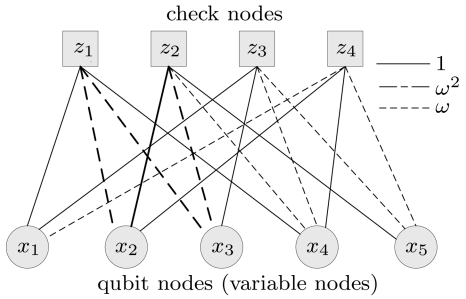



**Fig. 1.** Tanner graph of the [[5,1]] QEC code. Messages passing along edges are probabilities of corresponding qubit errors. The bold lines indicate a girth-four cycle in this Tanner graph.

**Lemma 2** Quantum stabilizer codes must contain girth-four cycles in their Tanner graphs.

From the definition of stabilizer code in the last section, we can see that stabilizer generators of QEC codes commute with each other. From Lemma 1, two commuting operators must have an even number of anti-commuting component positions. It means that any two rows of quantum check matrix should have an even number of non-trivial entries in common, which form a girth-four cycle. So there must exist girth-4 cycles in Tanner graphs of sparse QEC codes.

# 3. Iterative decoding of quantum sparse graph codes

## 3.1. Quantum channel model

The channel model we used in this paper is depolarizing channel (memoryless Pauli channel), which is widely used in quantum information field. Depolarizing channel plays a role similar to AWGN (Additive White Gauss Noise) channel in classical coding theory. For each qubit transmitted through this quantum channel, error $I$ (no error) occurs with probability $1-\varepsilon$, and error $X$, $Z$, $Y$ with probability $\varepsilon/3$, expressed as

$$p(E_j = a) = \begin{cases} 1-\varepsilon, & \text{when } a = 0, \\ \varepsilon/3, & \text{when } a = 1, \omega, \omega^2, \end{cases} \tag{3}$$

where $1 \leq j \leq n$ and $a \in \mathrm{GF}(4)$. Depolarizing channel is a quaternary memoryless symmetric channel with $\varepsilon$ being the transition probability (also being the depolarizing strength).

## 3.2. Syndrome measurement and error estimation

After receiving the quantum codeword state $|\psi'\rangle = \boldsymbol{E}|\psi\rangle$ from the channel output, we make eigenvalue measurement of each stabilizer generator $z_i$ without disturbing the quantum state. This process is shown in Eq. (4)

$$\boldsymbol{z}_i|\psi'\rangle = \boldsymbol{z}_i\boldsymbol{E}|\psi\rangle = s_i\boldsymbol{E}\boldsymbol{z}_i|\psi\rangle = s_i\boldsymbol{E}|\psi\rangle = s_i|\psi'\rangle, \tag{4}$$

where $|\psi\rangle$ is the channel input quantum codeword state, $\boldsymbol{E} \in \mathbb{G}_n$ is the occurring channel error on quantum codeword. The measurement result $s_i = \{0, 1\}$ depends on the commutation between error operator $\boldsymbol{E}$ and stabilizer generators $\boldsymbol{z}_i$. Suppose an $n$-qubit QEC stabilizer code $[[n, k]]$ and $\boldsymbol{E}$ is the occurring channel error, then we will obtain an error syndrome given as

$$\boldsymbol{s} = (s_0, s_1, \ldots s_{n-k}), \tag{5}$$

where $\boldsymbol{s}$ is an $(n-k)$-tuple binary vector.

Given error syndrome $\boldsymbol{s}$, the decoding problem is to find the most likely channel error $\hat{\boldsymbol{E}}$ that can satisfy all check equations in the following Eq. (6), which are different from classical parity check equations.

$$\hat{\boldsymbol{E}} \circ \boldsymbol{z}_i = s_i, \forall\ 1 \leq i \leq n-k, \tag{6}$$

$$\hat{\boldsymbol{E}}(\boldsymbol{s}) = \operatorname{argmax}\left\{p(\boldsymbol{E}/s)\right\}, \forall\ \boldsymbol{E} \in \mathbb{G}_n. \tag{7}$$

And the decoding problem is to find this vector with the highest probability as shown in Eq. (7).

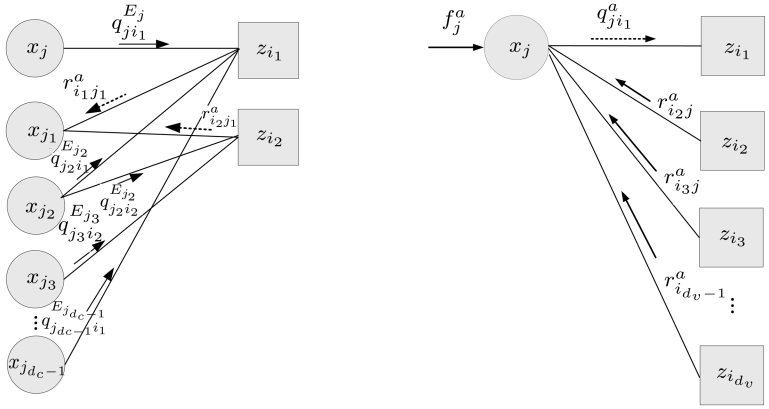
While the task of computing Eq. (7) is a non-deterministic polynomial (NP) problem. Memoryless assumption of the channel model makes bit-wise maximum-likely decoding possible, i.e., $\hat{\boldsymbol{E}} = \bigotimes_{j=1}^{n} \hat{E}_j$. But it is also a difficult task due to its exponential computation complexity. The BP algorithm used in classical sparse sparse codes can settle this problem efficiently. Different from classical codes, the

QEC codes have degeneracy problem, i.e., some different errors can produce the same syndromes. The basic QBP decoding of QEC sparse graph codes and some methods dealing with symmetric problem can be seen in Ref. [23].

### 3.3. Jointly-check iterative decoding algorithm

In classical coding theory, sparse graph codes have good iterative decoding performances by using the BP algorithm. But girth-four cycles in Tanner graph of quantum code make this algorithm unworkable efficiently as shown in Lemma 2. In order to improve the decoding performance based on Tanner graph over $GF(4)$, we choose the check nodes involved in girth-four cycles into jointly check pairs. By disturbing the updated message distribution of qubit nodes involved in cycle-four, the iterative decoding process can converge better.

As the Tanner graph in Fig. 2, we denote by $M(j)=\{i : A_{ij} \neq 0\}$ the set of check nodes connected with qubit $x_j$. And the set of qubits that check node $\boldsymbol{z}_i$ connected is denoted by $N(i)=\{j : A_{ij} \neq 0\}$. We denote a set $M(j)$ with qubit $x_j$ excluded by $M(j)\backslash i$ and a set $N(i)$ with check node $\boldsymbol{z}_i$ excluded by $N(i)\backslash j$. Now we give the jointly-check decoding method as the following steps for all nonzero variable nodes $x_j$ with $1 \leq j \leq n$ and all check nodes $\boldsymbol{z}_i$ with $1 \leq i \leq n-k$.




(a) Message computation on check nodes (b) Message computation on variable nodes

**Fig. 2.** Message updating process in Tanner graph of quantum sparse graph codes. Here $\boldsymbol{z}_{i_1}$ and $\boldsymbol{z}_{i_2}$ are two check nodes with common qubits $x_{j_1}, x_{j_2}$ involved in a cycle-four. And $x_j$ is the variable node not in girth-four cycle. $d_c$ is the degree of check nodes (i.e. row-weight of check matrix $\boldsymbol{A}_{GF(4)}$), and $d_v$ is the degree of variable nodes (i.e. column-weight of check matrix $\boldsymbol{A}_{GF(4)}$). And $f_j^a$ is the initial probability information from the channel output.

**Step 1** Initialize: From the quantum channel model in Subsection 3.1, channel error on each qubit has the probability message as shown in Eq. (3). Then every variable node $x_j$ broadcasts this initial probability message $f_j^a = p(E_j = a)$ to all its connected check nodes $M(j)$.

**Step 2** Check nodes updating: After receiving messages from connected variable nodes, each check node $\boldsymbol{z}_i$ computes the new message $r_{ij}$ transferring to its connected variable nodes $x_j$. In the $(l+1)$-th iterative process, the information transmitted from check node $\boldsymbol{z}_i$ to variable node $x_j$ uninvolved in a girth-4 cycles can be computed as

$$r_{ij}^a(l+1) = \sum_{x_{j'}:j' \in N(i)\backslash j} P\big(\boldsymbol{z}_i \,|\, E_j = a, \{x_{j'} : j' \in N(i)\backslash j\}\big) \times \prod_{j' \in N(i)\backslash j} q_{j'i}^{x_{j'}}(l), \tag{8}$$

where $a$, $x_{j'} \in GF(4)$ and $q_{ji}^a(0) = f_j^a$. The conditional probabilities above are either zero or one, depending on whether the check equation in Eq. (6) can be satisfied. This can be done efficiently, owing to the fact that the probability of an $n$-tuple binary sequence with an even number of 1s is $\big(1+\prod_{j=1}^{n}(1-2p_j^1)\big)/2$ if its $j$-th bit is equal to 1 with probability $p_j^1$.

As shown in Fig. 2(a), if two check nodes $(z_{i_1}, z_{i_2})$ involved in a girth-4 cycle ($x_{j_1}$ and $x_{j_2}$ are their common variable nodes), we use these two check equations together to avoid the impasse due to girth-4 cycles. For

variable nodes $x_{j_1}$ and $x_{j_2}$, only $r^a_{i_1j_1}$ and $r^a_{i_1j_2}$ are computed as follows:

$$r^a_{i_1j_1}(l+1) = \sum_{x_{j'}:j'\in N(i_1)\cup N(i_2)\backslash j_1} P\big(z_{i_1}, z_{i_2} \mid E_{j_1}=a, \{x_{j'}: j'\in N(i_1)\cup N(i_2)\backslash j_1\}\big) \times \prod_{j'\in N(i_1)\cup N(i_2)\backslash j_1} q^{x_{j'}}_{j'i_1}(l) q^{x_{j'}}_{j'i_2}(l) \tag{9}$$

with a similar process that $r^a_{i_1j_2}$ can be computed. On the other hand, $r^a_{i_2j_1}$, $r^a_{i_2j_2}$ are set to be 1 for all $a \in GF(4)$.

**Step 3** Variable nodes updating: From Fig. 2(b), we can compute the new message $q_{ji}$ that variable node $x_j$ transfers to its connected check node $z_i$ in the following equation:

$$q^a_{ji}(l+1) = \alpha_{ji} f^a_j \prod_{i'\in M(j)\backslash i} r^a_{i'j}(l), \tag{10}$$

where $\alpha_{ji}$ is chosen such that $\sum_{a\in GF(4)} \alpha_{ji} q^a_{ji}(l+1)$=1.

**Step 4** Decision: For each qubit node, marginal qubit-wise probability can be computed as

$$q^a_j(l+1) = \alpha_j f^a_j \prod_{i'\in M(j)} r^a_{i'j}(l), \tag{11}$$

where $\alpha_j$ is chosen such that $\sum_{a\in GF(4)} \alpha_j q^a_j(l+1)$=1. Then we choose a most likely error value $\hat{E}_j$ with the highest probability on qubit-$j$ as the following equation:

$$\hat{E}_j = \mathrm{argmax}\left\{q^a_j(l+1)\right\}, \forall a \in GF(4). \tag{12}$$

**Step 5** Output: From the memoryless assumption of the channel model, we have $\hat{\boldsymbol{E}} = \bigotimes_{j=1}^{n} \hat{E}_j$. If $\hat{\boldsymbol{E}}$ can satisfy Eq. (6), then output the correct decoding. Otherwise, go to Step 2 with the next iterative process with $l = l+1$ until $l$ reaches the predetermined maximum iterative number $T$. When the iterative process halts with the maximum iterative number or outputs a trivial result, we can use the method from Ref. [23] and begin a new iterative process. When the final decoded value $\hat{\boldsymbol{E}} = \boldsymbol{E}$, the decoder gives a correct result. Otherwise, the deocoder fails with a frame error (also called codeword error) output.

After error estimation, the transmitted quantum codeword can be recovered by acting operator $\hat{\boldsymbol{E}}$ on the corrupted codeword states as $\hat{\boldsymbol{E}}|\psi'\rangle = \boldsymbol{E}\boldsymbol{E}|\psi\rangle = \boldsymbol{I}|\psi\rangle = |\psi\rangle$. If errors $\boldsymbol{E}$ and $\boldsymbol{E}'$ differ by an stabilizer element $\boldsymbol{S}$ with $\boldsymbol{E}' = \boldsymbol{E}\boldsymbol{S}$, $\exists\ \boldsymbol{S} \in \mathcal{S}$, then they have the same syndromes. And both of them can be used to correct the received quantum state $\boldsymbol{E}'|\psi'\rangle = \boldsymbol{E}\boldsymbol{S}|\psi'\rangle = \boldsymbol{E}|\psi'\rangle = |\psi\rangle$. Degeneracy can improve QEC performance, but it also induces some impasse problem by using qubit-wise decoding algorithms. Jointly-check strategy can converge the iterative decoding process of quantum sparse graph codes.

## 4. Simulation results

In this paper we choose some codes from Refs. [22] and [23] to test our decoding method. Now we briefly give these codes with quantum rate $R = 1/2$ and then simulate their performance by using our modified decoding method.

To compare with quantum LDPC codes with CSS structure, we first simulate the code from Ref. [23] with codelength $n = 800$, rate $R = 1/2$, row-weight 30 and average column-weight 18. With separately decoding strategy in Ref. [6], the decoding performance is worse than that of standard BP algorithm over $GF(4)$ as shown in Fig. 3. The reason is that there are still girth-four cycles in this self-dual classical component code. Furthermore, we can see that our method outperforms standard BP significantly.

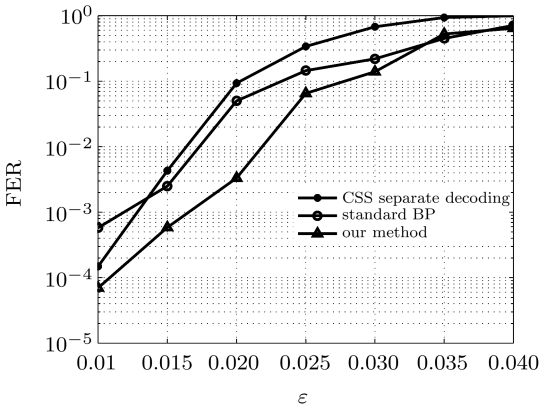



**Fig. 3.** Comparison among decoding performances of different methods for the codes from Ref. [23], where we set $T$=100 and FER stands for frame error rate.

The second code we simulated has codelength $n = 2068$ and 1/2 coderate.[22] Its check matrix $\boldsymbol{A} = [\boldsymbol{A}_1|\boldsymbol{A}_2]$ can be constructed by the following ma-

trices:

$$\boldsymbol{A}_1 = \begin{pmatrix} \boldsymbol{X}_1 & \boldsymbol{X}_1^{\mathrm{T}}\boldsymbol{P}^{\mathrm{T}} & \boldsymbol{Y}_1 & \boldsymbol{Y}_1^{\mathrm{T}}\boldsymbol{Q}^{\mathrm{T}} \\ \boldsymbol{P}\boldsymbol{X}_1^{\mathrm{T}} & \boldsymbol{P}\boldsymbol{X}_1\boldsymbol{P}^{\mathrm{T}} & \boldsymbol{Q}\boldsymbol{Y}_1^{\mathrm{T}} & \boldsymbol{Q}\boldsymbol{Y}_1\boldsymbol{Q}^{\mathrm{T}} \end{pmatrix}, \quad (13)$$

$$\boldsymbol{A}_2 = \begin{pmatrix} \boldsymbol{X}_2 & \boldsymbol{X}_2^{\mathrm{T}}\boldsymbol{P}^{\mathrm{T}} & \boldsymbol{Y}_2 & \boldsymbol{Y}_2^{\mathrm{T}}\boldsymbol{Q}^{\mathrm{T}} \\ \boldsymbol{P}\boldsymbol{X}_2^{\mathrm{T}} & \boldsymbol{P}\boldsymbol{X}_2\boldsymbol{P}^{\mathrm{T}} & \boldsymbol{Q}\boldsymbol{Y}_2^{\mathrm{T}} & \boldsymbol{Q}\boldsymbol{Y}_2\boldsymbol{Q}^{\mathrm{T}} \end{pmatrix}, \quad (14)$$

where $\boldsymbol{X}_1$=[$\boldsymbol{I}_0$ + $\boldsymbol{I}_{121}$], $\boldsymbol{X}_2$=[$\boldsymbol{I}_1$ + $\boldsymbol{I}_{100}$], $\boldsymbol{Y}_1$=[$\boldsymbol{I}_8$ + $\boldsymbol{I}_{79}$], $\boldsymbol{Y}_2$=[$\boldsymbol{I}_{29}$ + $\boldsymbol{I}_{165}$] , and $\boldsymbol{P}$, $\boldsymbol{Q}$ are randomly interleaving matrices with size 517×517.

The quantum code [[2068, 1034]] constructed above has row-weight 16 and column-weight 4 in their check matrix. We simulate its error correcting performance by using the method given in Section 3 with numerical results shown in Fig. 4. By combining jointly-check and random-perturbation methods together, the threshold of $10^{-4}$ FER can be around 0.02, which is significantly higher than the result 0.013 in Refs. [6] and [22].

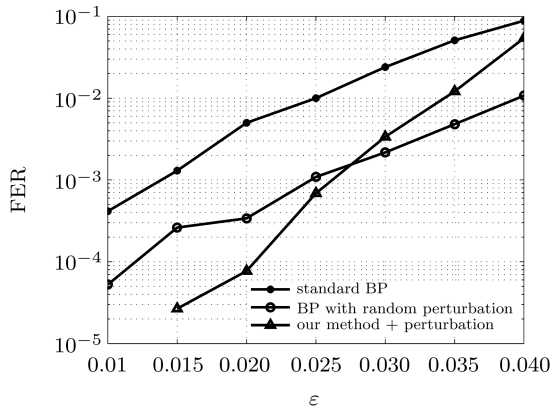



**Fig. 4.** Curves of frame error rate (FER) versus depolarizing strength $\varepsilon$ for different iterative decoding algorithms for quantum LDPC codes from Ref. [22], where maximum iterative number $T = 80$.

Jointly-check strategy has a similar effect to random perturbation method. The former is forward adjustment and the latter is feedback, together with these two methods we can improve the decoding performance much more as the results shown in Fig. 4. Furthermore, the example codes above are not designed optimally for jointly-check method, we think it can have a much better performance for well designed quantum sparse graph codes.

## 5. Conclusion

In either classical field or quantum field, the existence of the efficient decoding algorithm is an important criterion for the utilization of those error correcting codes. In this paper, by taking into account the unavoidable girth-four cycles in quantum Tanner graph, we present a more suitable method of decoding quantum sparse graph codes.

With numerical simulations, we find that by grouping some check nodes involved in girth-four cycles into jointly-check pairs, the BP decoding process of quantum codes can converge efficiently. Compared with the standard BP decoding algorithm, our method significantly improves the performance in decoding QEC sparse graph codes. Furthermore, a much better decoding performance is obtained by combining the jointly-check method with random perturbation method together.

The degeneracy problem of quantum codes makes their decodings different from classical ones. It is an challenging problem to devise good quantum codes and efficient decoding algorithms based on this feature. In the future work, we will extend this technique into nonbinary quantum codes and find more good quantum codes with efficient decoding algorithm.

## References


[1] Divincenzo D P and Shor P W 1996 *Phys. Rev. Lett.* **77** 3260

[2] Brito D B, Nascimento J C and Ramos R V 2007 *IEEE J. Quantum Electron.* **44** 113

[3] Ambainis A and Gottesman D 2006 *IEEE Trans. Information Theory* **52** 748

[4] Li Z and Xing L J 2007 *Acta Phys. Sin.* **56** 5602 (in Chinese)

[5] Wu S, Liang L M and Li C Z 2007 *Chin. Phys.* **16** 1229

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

[7] David J C MacKay 1999 *IEEE Trans. Information Theory* **45** 399

[8] Li Z and Xing L J 2008 *Acta Phys. Sin.* **57** 28 (in Chinese)

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

[10] Forney G D and Costello D J 2007 *Proceedings of the IEEE* **95** 1150

[11] Poulin D and Bilgin E 2008 *Phys. Rev.* A **77** 052318

[12] Zhang Q, Tang C J and Gao F 2002 *Acta Phys. Sin.* **51** 15 (in Chinese)

[13] Xing L J, Li Z, Bai B M and Wang X M 2008 *Acta Phys. Sin.* **57** 4695 (in Chinese)

[14] John A S, Smith G and Wehner S 2007 *Phys. Rev. Lett.* **99** 130505
[15] Hagiwara M and Imai H 2007 *IEEE International Symposium on Information Theory* France June 24–29 p. 806
[16] Aly S A 2008 *IEEE Global Telecommunications Conference* New Orleans 30 November–4 December p. 1097
[17] Brun T, Devetak I and Hsieh M H 2006 *Science* **314** 1464
[18] Poulin D 2005 *Phys. Rev. Lett.* **95** 230504
[19] Vontobel P O 2008 *The 5th International Symposium on Turbo Codes and Related Topics* Lausanne, September 1–5 p. 215
[20] Camara T, Ollivier H and Tillich J P 2005 arXiv quant-ph/0502086 [hep-ph]
[21] Tan P Y and Li J 2007 *IEEE International Symposium on Information Theory* Nice June 24–29 p. 2106
[22] Tan P Y and Li J 2008 *IEEE International Conference on Communications* Ontario July 6–11 p. 1166
[23] Poulin D and Chung Y 2008 *International Journal of Quantum Information and Computation* **8** 987
[24] Chung K and Heo J 2006 *IEEE 63rd on Vehicular Technology Conference* Melbourne May 7–10 p. 1464
[25] Gottesman D 1997 *Stabilizer Codes and Quantum Error Correction* (Ph.D. Thesis) (California: California Institute of Technology)
[26] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) pp. 454–468
[27] Calderbank A R, Rains E M and Shor P W 1998 *IEEE Trans. Information Theory* **44** 1369