

Low-loss belief propagation decoder with Tanner graph in quantum error-correction codes

Dan-Dan Yan(颜丹丹), Xing-Kui Fan(范兴奎), Zhen-Yu Chen(陈祯羽), and Hong-Yang Ma(马鸿洋)†

Citation: Chin. Phys. B, 2022, 31 (**1**): 010304. DOI: 10.1088/1674-1056/ac11cf
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Realization of arbitrary two-qubit quantum gates based on chiral Majorana fermions

Qing Yan(闫青) and Qing-Feng Sun(孙庆丰)
Chin. Phys. B, 2021, 30 (**4**): 040303. DOI: 10.1088/1674-1056/abe296

Realization of *t*-bit semiclassical quantum Fourier transform on IBM's quantum cloud computer

Xiang-Qun Fu(付向群), Wan-Su Bao(鲍皖苏), He-Liang Huang(黄合良), Tan Li(李坦), Jian-Hong Shi(史建红), Xiang Wang(汪翔), Shuo Zhang(张硕), Feng-Guang Li(李风光)
Chin. Phys. B, 2019, 28 (**2**): 020302. DOI: 10.1088/1674-1056/28/2/020302

Realization of quantum permutation algorithm in high dimensional Hilbert space

Dong-Xu Chen(陈东旭), Rui-Feng Liu(刘瑞丰), Pei Zhang(张沛), Yun-Long Wang(王云龙), Hong-Rong Li(李宏荣), Hong Gao(高宏), Fu-Li Li(李福利)
Chin. Phys. B, 2017, 26 (**6**): 060305. DOI: 10.1088/1674-1056/26/6/060305

One-dimensional lazy quantum walks and occupancy rate

Li Dan, Michael Mc Gettrick, Zhang Wei-Wei, Zhang Ke-Jia
Chin. Phys. B, 2015, 24 (**5**): 050305. DOI: 10.1088/1674-1056/24/5/050305

From fractional Fourier transformation to quantum mechanical fractional squeezing transformation

Lv Cui-Hong, Fan Hong-Yi, Li Dong-Wei
Chin. Phys. B, 2015, 24 (**2**): 020301. DOI: 10.1088/1674-1056/24/2/020301

Low-loss belief propagation decoder with Tanner graph in quantum error-correction codes

Dan-Dan Yan(颜丹丹), Xing-Kui Fan(范兴奎), Zhen-Yu Chen(陈祯羽), and Hong-Yang Ma(马鸿洋)†

School of Sciences, Qingdao University of Technology, Qingdao 266033, *China*

(Received 17 May 2021; revised manuscript received 28 June 2021; accepted manuscript online 7 July 2021)

Quantum error-correction codes are immeasurable resources for quantum computing and quantum communication. However, the existing decoders are generally incapable of checking node duplication of belief propagation (BP) on quantum low-density parity check (QLDPC) codes. Based on the probability theory in the machine learning, mathematical statistics and topological structure, a GF(4) (the Galois field is abbreviated as GF) augmented model BP decoder with Tanner graph is designed. The problem of repeated check nodes can be solved by this decoder. In simulation, when the random perturbation strength $p = 0.0115$–0.0116 and number of attempts $N = 60$–70, the highest decoding efficiency of the augmented model BP decoder is obtained, and the low-loss frame error rate (FER) decreases to 7.1975×10^{-5}. Hence, we design a novel augmented model decoder to compare the relationship between GF(2) and GF(4) for quantum code [[450,200]] on the depolarization channel. It can be verified that the proposed decoder provides the widely application range, and the decoding performance is better in QLDPC codes.

Keywords: tanner graph, belief propagation decoder, augmented model, fourier transform

PACS: 03.67.Ac, 03.67.Hk, 03.67.Dd **DOI:** 10.1088/1674-1056/ac11cf

1. Introduction

With the rapid development of information network, the quantum computing and quantum communication have made great progress.[1] The quantum communication and quantum computing have been applied for capturing imaginations for almost 60 years. Currently, there are two important parts of quantum information science, which offer deeply paths to solve problems that could never be overcame by classical computing and communication.[2] In recent years, many scholars are studying in the quantum walking fields.[3] The quantum communication and quantum computing have closely related.[4] On the one hand, the former is the theoretical and environmental basis of the latter. On the other hand, the latter provides operational guarantee for the former.

The quantum computing and quantum communication have made a qualitative leap. For instance, quantum communication includes quantum key distribution and quantum secure direct communication.[4,5] Propagation in quantum network has been studied in Ref. [6]. In 2019, Qi *et al*. have been studied quantum many-body states in Ref. [7] with neural network used, and routing in quantum network has been studied in Ref. [8]. Then, parity checks have been used in concentration and measurement.[9,10] In addition, low-density parity check (LDPC) codes have been extensively used in quantum secure direct communication,[11,12] and quantum error-correction has become one focus in quantum computing as shown in Ref. [13]. There is a huge challenge to reconstruct the existing decoders,[14,15] and the most difficult problem is how to resolve the node duplication of the existing decoders.[16,17] This paper mainly focused on resolving this problem and constructing a GF(4) augmented model belief propagation (BP) decoder with Tanner graph.[18–20] We not only use sparse matrix, bipartite graph and the properties of approaching Shannon limit for quantum low-density parity check (QLDPC) codes,[21–27] but also use the directivity of Tanner graph. From these properties we know that the length of the ring is at most one.[28–31] In 2019, Alex Rigby *et al*. have been proposed an improved belief propagation decoder on QLDPC code.[26] The decoder was designed to correct the error of the quantum error-correction code and obtained the accurate sequence, and then the information can be transmitted.[32,33]

In this paper, combined with the properties of stabilizers, a novel QLDPC code based on the BP algorithm decoding is studied.[34,35] The BP algorithm can achieve hardware parallelization. Besides, the algorithm is calculated by a simply linear function related to the code length, thus, it has no error layer effect. Since the stabilizers are theoretically GF(4) linear codes,[36] a new GF(4) augmented model BP decoder with the Tanner graph is constructed by using the augmented model. We use the received information to carry out iterative operation between the variable node and check node, and to obtain the maximum decoding gain.[28,35,37] As mentioned above, the BP algorithm is based on a linear function related to the code length. Therefore, the parallel implementation in hardware can greatly improve the decoder speed.[38] The decoding frame error rate (FER) of BP algorithm decreases aptly with the increase of the signal-noise ratio (SNR) and it does

†Corresponding author. E-mail: hongyang_ma@aliyun.com

© 2022 Chinese Physical Society and IOP Publishing Ltd

not have the phenomenon of error floor (carpet effect).[39–41] Combining the BP decoder, a novel GF(4) augmented model BP decoder with the Tanner graph is constructed, and the decoder adds an augmented model with the Tanner graph that can check the repeated nodes.[42] The conditional probability distribution and marginal probability distribution are used to calculate the decoding FER. Since there is no node duplication on the decoder, the FER has been greatly reduced. The algorithm rules and commutative principle in GF(4) field, the inverse Fourier transform and Hadamard transform are used for decoding.[43–45] Finally, the result of simulation shows that compared with the existing decoders, the proposed decoder has stronger anti-interference ability and it can achieve better FER performance in terms of the random perturbation strength and the number of attempts.

The structure of the present paper is organized as follows. In Section 2, the quantum error-correcting codes and the Tanner graphs are introduced. In Section 3, the limitations of the original belief propagation decoder are analyzed. In Section 4, we propose a scheme of the GF(4) augmented model BP decoder with Tanner graph. In Section 5, the GF(4) augmented model BP decoder with Tanner graph has better FER performance than the existing decoders through the simulation. Finally, the conclusion is given in the last section.

2. Quantum error-correction codes and Tanner graph

2.1. Quantum error-correction codes

The QLDPC code in this paper is a quantum code based on stabilizer codes. It not only meets the sparse matrix of classical LDPC codes, which is close to Shannon's limit performance,[26] but also meets the characteristics of cyclic difference sets of stabilizer codes. According to the above structural properties, the ring length is guaranteed to be no more than 1. In the Tanner graph, the problem of node duplication can be prevented and the efficiency of decoding can be improved. Therefore, the characteristics of QLDPC codes with Tanner graph provide a basic theory for the decoding process.

2.2. Tanner graph

Tanner graph (factor graph) of a linear code is a bipartite graph $G=(V,C,E)$. The variable nodes $V=\{v_1,\ldots,v_n\}$ correspond to the n error components, and the check nodes $C=\{c_1,\ldots,c_m\}$ correspond to the m constraints imposed by the rows of a parity-check matrix H. An edge $c_i,v_j\in E$ connects check node c_i to the variable node v_j if $H_{ij}\neq 0$, $i=1,2,\ldots,m$ and $j=1,2,\ldots,n$. For example, the $[[5,1,3]]$ Hamming code can be expressed by the parity-check matrix[46]

$$H_X=\begin{pmatrix}1&0&0&1&0\\0&1&0&0&1\\1&0&1&0&0\\0&1&0&1&0\end{pmatrix},$$
$$H_Z=\begin{pmatrix}0&1&1&0&0\\0&0&1&1&0\\0&0&0&1&1\\1&0&0&0&1\end{pmatrix}, \tag{1}$$

which gives Tanner graph shown in Fig. 1.[36]

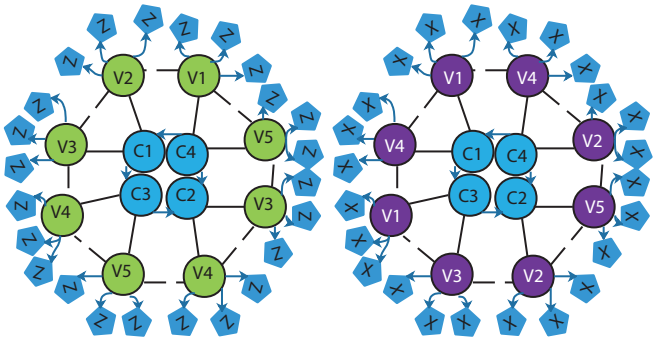


Fig. 1. [[5,1,3]] Z-error or X-error Tanner graph. The blue arrow between the variable node and the error node represents the exchange and correction of the information.

In Fig. 1, $\{v_1,v_2,v_3,v_4,v_5\}$ represents the variable node of [[5,1,3]], and $\{c_1,c_2,c_3,c_4\}$ represents its check node. The blue arrow in the check node indicates that the check node sequence has the property of cyclic difference set and solid lines at each node represent the transmission of information.

3. Limitations of belief propagation decoder

Belief propagation algorithm, also known as sum-product algorithm or message passing algorithm, is to treat the sum-product operation in variable elimination method as a message and save it, which can save a lot of computing resources. For the general quantum low-density parity code, the length of its ring is 2 or more, there will be a defect of node duplication. When the decoder operation is carried out, many nodes may recalculate the number of times more than twice, resulting in a relatively high FER.

The following is the construction of belief propagation algorithm. All error states $E\in P_n$ can affect the n-bit quantum code, and only those that conform to the exchange law of the stabilizers and error operator can be used to measure S_c . In other words, the conditional probability distribution under the error operator s is

$$P(E|s)\propto P(E)S_c^m\prod_{c=1}^{m}\varepsilon_{S_c}\cdot E\cdot S_c,$$

where ε_{S_c} is coefficient.

However, belief propagation has its inherent the limitations that it cannot check for node duplication in a Tanner

graph. Therefore, this paper improves the BP decoder via adding a GF(4) augmented model with Tanner graph. Such advantage is to solve the problem that node duplication cannot be checked in the BP decoder, which further reduces the decoding frame error rate (FER). The information shifted from the check node to the variable node can be expressed as

$$m_{c\to v}(E_v) \propto \sum_{E_{v'};v'\in n(c)\setminus v}\left(\varepsilon_{S_c}\cdot S_c\cdot E_c\prod_{v'\in n(c)\setminus v}(\varepsilon_{S_c}m_{v'\to c}(E_{v'}))\right), \quad (2)$$

where E_v and $E_{v'}$ represent error states on variable nodes v and v', respectively. The coefficient can be obtained from the normalized formula $\sum_{E_c} m_{c\to v}=1$. When the algorithm is initialized, its prior probability can be considered as 0.

Based on the information received above, each variable node sends a message to its neighbor check node,

$$m_{v\to c}(E_v)\propto p(E_v)\prod_{c'\in n(v)\setminus c} m_{c'\to v}(E_v), \quad (3)$$

where $n(v)\setminus c$ represents all of the adjacent nodes of v except node c.

On the basis of the above belief propagation algorithm, for GF(2) and GF(4) belief propagation decoders, the variation trend of FER of [[5,1,3]] is plotted under the random perturbation strength $p=0.008$–0.02. However, it can be seen from Fig. 2 that, for the belief propagation decoder, the value of FER reaches only an order of magnitude of 10^{-2}. Therefore, the efficiency and stability of the augmented model belief propagation decoder with Tanner graph is much higher than that of the belief propagation decoder, and the order of magnitude of FER is as low as 10^{-5}.

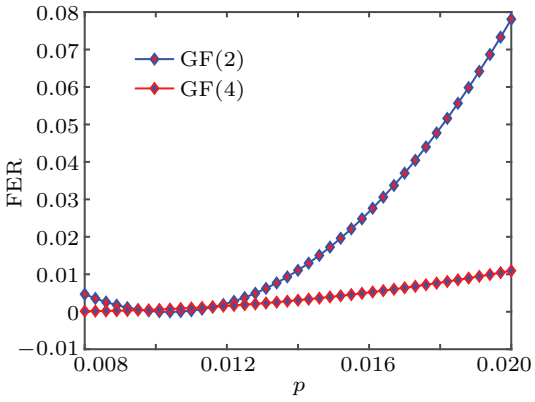


Fig. 2. Comparing the relationship of p and FER in the GF(2) and GF(4) of [[5,1,3]]. Note that the FER of GF(2) and GF(4) overlaps when $p=0.009$–0.012, due to node duplication in GF(4), which leads to higher FER.

For Fig. 3, the relationship between iterative attempts and FER of [[5,1,3]] is studied. As can be seen from the left figure, when the attempts between 5 and 15, there are two sharp points. The sharp points indicate that the gradient disappears, and this part of the simulation is invalid. In this case, the numerical simulation may not get the correct result. Comparatively, as can be seen from the right figure, the numerical results of GF(4) are more greatly impressive. The right figure of Fig. 3 shows the simulation of [[5,1,3]] code on the GF(4) belief propagation decoder. With the increasing of attempts, FER shows an approximately linear decline, and the accuracy of FER reaches 10^{-7} when the attempts are 100. In contrast, GF(2) is very unstable in the decoding process, and GF(4) has better FER performance and effects. As the code length is too short, it shows a downward trend with the increase of attempts. However, with the increase of code length, the FER also will gradually increase.

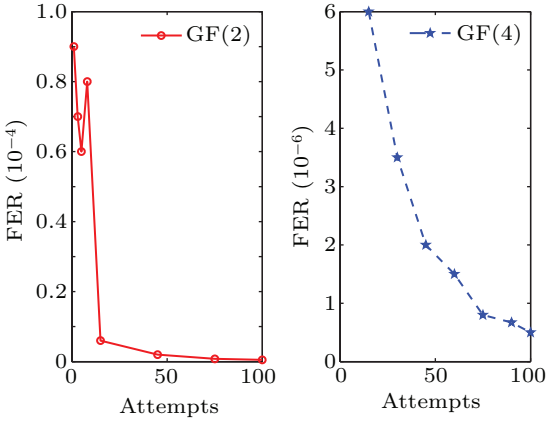


Fig. 3. Comparing the relationship of attempts and FER in the GF(2) and GF(4) of [[5,1,3]]. Specially, at about 5–15 in the left figure, there are two sharp point where the GF(2) decoder fails because the gradient disappears.

4. Schemes for implementing the augmented model BP decoder in quantum error-correction codes

4.1. The variable elimination method

Take the Bayesian network structure in Fig. 4(a) as an example. Suppose the objective of the inference is to calculate the marginal probability $p(x_5)$. Obviously, in order to do this, we simply eliminate the variable $\{x_1,x_2,x_3,x_4\}$ by addition, namely,

$$\begin{aligned} p(x_5) &= \sum_{x_4}\sum_{x_3}\sum_{x_2}\sum_{x_1} p(x_1,x_2,x_3,x_4,x_5) \\ &= \sum_{x_4}\sum_{x_3}\sum_{x_2}\sum_{x_1} p(x_1)p(x_2|x_1)p(x_3|x_2)p(x_4|x_3)p(x_5|x_4). \end{aligned} \quad (4)$$

The belief propagation algorithm takes the summation operation in the variable elimination method as a message passing process, and it solves the problem of repeated calculation when solving multiple marginal distributions. Specifically, the elimination of variables is done by summation

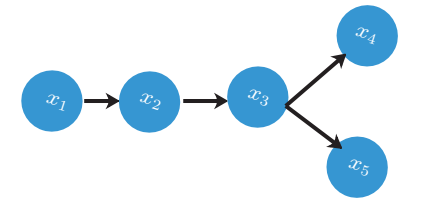
$$m_{i\to j}(x_j)=\sum_{x_i}\psi(x_i,x_j)\Pi_{k\in n(i)\setminus j}m_{k\to i}(x_i). \quad (5)$$

The variable x_i is eliminated, where $n(i)$ represents the adjacency node of node x_i. In the belief propagation algorithm, this operation is treated as passing a message $m_{ij}(x_j)$ from x_i to x_j. Thus, the variable elimination process described by Eq. (5) can be described as the message passing process shown in Fig. 4(b). It is not difficult to find that each message passing operation is only directly related to the variable x_i and its adjacent nodes. In other words, the calculation related to message passing is limited to the local part of the graph.

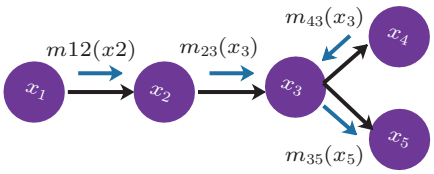
In the belief propagation algorithm, a node can only send a message to another node after receiving messages from all other nodes. The marginal distribution of a node is proportional to the product of messages it receives, namely,

$$p(x_i) \propto \prod_{k\in n(i)} m_{k\to i}(x_i) \tag{6}$$

for example, in Fig. 4(b), before node x_3 can send a message to x_5, it must receive a message from nodes x_2 and x_4 in advance, and the probability that message $m_{35}(x_5)$ gets to x_5 is $P(x_5)$. Figure 5 shows the diagram of belief propagation algorithm.

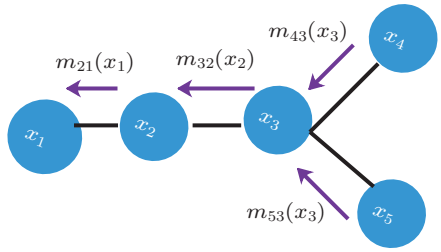


(a) Bayesian network structure

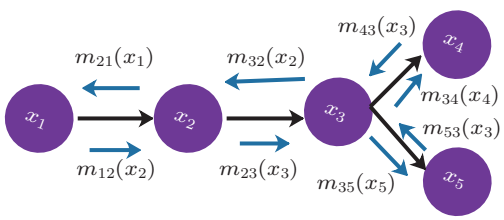


(b) Messaging process

Fig. 4. The variable elimination method and its corresponding messaging process.



(a) The message is propagated to the root node



(b) The message goes out from the root node

Fig. 5. Diagram of belief propagation algorithm.

4.2. The augmented model belief propagation

The augmented model decoder is the one novel decoder, which first appeared in classical binary code.[22] For QLDPC code, an augmented model decoder can be based on any coded GF(4) decoder. Re-decoding is performed by using a randomly generated augmented check matrix

$$H_{\rm A} = \begin{pmatrix} H \\ H_\varepsilon \end{pmatrix}, \tag{7}$$

where a subset of randomly selected rows from H_ε. The proportion of the rows selected is determined by the augmentation density ε. The syndrome used for decoding is

$$z_{\rm A} = \begin{pmatrix} z \\ z_\varepsilon \end{pmatrix}, \tag{8}$$

where z is the measured syndrome and z_ε contains the syndrome values corresponding to the rows selected to form H_ε.

In the GF(2) case, an augmented model decoder is used, and it is employed for the X element. Respectively, the form of parity matrix on the augmented model used by the X decoder and the augmented syndrome are

$$H_{\rm A} = \begin{pmatrix} H'_Z \\ H'_{Z_\varepsilon} \end{pmatrix}, \quad z_{\rm A} = \begin{pmatrix} z_X \\ z_{X_\varepsilon} \end{pmatrix}. \tag{9}$$

In order to further optimize the calculation, the stabilizer code with the theory on the GF(4) field is associated. Suppose Pauli operator group G is generated by $\{I, X, Z, Y = XZ\}$. The quaternion of GF(4) in Galois field is $\{0, 1, \omega, \bar{\omega} = \omega^2\}$. The following mapping is a one-to-one correspondence mapping of the Pauli operator in G to the GF(4) field, namely,

G	$\longrightarrow$ GF(4)
I	0
X	1
Z	ω
Y	$\bar{\omega}$

In this way, the stabilizer generator element matrix $\bar{H}$ of [[5,1,3]] code can be expressed as

$$\bar{H} = \begin{bmatrix} 1 & \omega & \omega & 1 & 0 \\ 0 & 1 & \omega & \omega & 1 \\ 1 & 0 & 1 & \omega & \omega \\ \omega & 1 & 0 & 1 & \omega \end{bmatrix}. \tag{10}$$

Here to be sure, $G \to {\rm GF}(4)$ is not the only one. The relation between the $X \to \omega, z \to \bar{\omega}, Y \to 1$ corresponding relation is adopted in some literatures.

4.3. Classical decoder decoding and GF(4) augmented model BP decoder decoding with Tanner graph

In particular, convolution can be converted to take the product of the Fourier transform and the inverse Fourier transform. The following is the belief propagation algorithm based on fast Fourier transform, namely, FFT-BP algorithm. It

should be noted that the subscript operation of the convolution solution of the probability sequence belongs to the operation of GF(4), so the transformation can be regarded as a series of two-point FFT transformations in the p-dimensional space. In essence, the method adopts the Hadamard transform

$$\begin{aligned} F^0 &= [f^0 + f^1] + [f^2 + f^3], \\ F^1 &= [f^0 - f^1] + [f^2 - f^3], \\ F^2 &= [f^0 + f^1] - [f^2 + f^3], \\ F^3 &= [f^0 - f^1] - [f^2 - f^3]. \end{aligned} \tag{11}$$

Belief propagation effectively approximates these marginal probability distributions by passing the code messages on the Tanner graph. A message is sent from each variable node v_j to the check node in neighbor $\mathcal{M}(v_j) = \{c_i \in C : \{c_i, v_j\} \in E\}$. The message sent to the check node $c_i \in \mathcal{N}(v_j)$ is $\mu_{j\to i}$, where the element corresponding to $b \in \mathrm{GF}(4)$ is

$$\mu^b_{j\to i} = P(e_j = b). \tag{12}$$

Every check node c_i then sends a message back to the variable nodes in the neighborhood $\mathcal{N}(c_i) = \{v_j \in V : \{c_i, v_j\} \in E\}$. In particular, the message sent to variable node $v_j \in \mathcal{N}(c_i)$ is $\lambda_{i\to j}$ with

$$\lambda^b_{i\to j} = K \sum_{\boldsymbol{e}: e_j = b} \delta\left(\sum_{j' \in \mathcal{N}(i)} H_{ij'} e_{j'} = z_i \right) \prod_{j' \in \mathcal{N}(i)\setminus j} \mu^{e_{j'}}_{j'\to i}, \tag{13}$$

where, through slight abuse of notation, $\mathcal{N}(i) = \{j \in \{1, \ldots, n\} : v_j \in \mathcal{N}(c_i)\}$ and K is a normalization factor chosen such that $\sum_b \lambda^b_{i\to j} = 1$.

First, classical decoding is introduced. The check constraint of Eqs. (9) and (11) can be written as

$$\sum_{j' \in \mathcal{N}(i)\setminus j} H_{ij'} e_{j'} = \sum_{j' \in \mathcal{N}(i)\setminus j} \tilde{e}_{j'} = z_i - H_{ij} b, \tag{14}$$

where $\tilde{e}_{j'} = H_{ij'} e_{j'}$. $\tilde{\lambda}^b_{i\to j}$ can be used to define

$$\tilde{\lambda}^b_{i\to j} = \sum_{\boldsymbol{e}: \sum_{j'} \tilde{e}_{j'} = b} \prod_{j'} \mu^{e_{j'}}_{j'\to i} = \sum_{\boldsymbol{e}: \sum_{j'} \tilde{e}_{j'} = b} \prod_{j'} \tilde{\mu}^{\tilde{e}_{j'}}_{j'\to i}, \tag{15}$$

where $\tilde{\mu}^{\tilde{e}_{j'}}_{j'\to i} = \mu^{H^{-1}_{ij'} \tilde{e}_{j'}}_{j'\to i}$ (this corresponds to a permutation of elements) and $j' \in \mathcal{N}(i) \setminus j$. Equation (13) is a convolution and as such can be efficiently computed using a Fourier transform $\mathcal{F}$ as

$$\tilde{\lambda}_{i\to j} = K \mathcal{F}^{-1}\{\prod_{j'} \mathcal{F}\{\tilde{\mu}_{j'\to i}\}\}, \tag{16}$$

where $\mathcal{F}^{-1}$ is the inverse Fourier transform and the product is element-wise (K is a normalized factor). In the binary case, we can use the Hadamard transform. If $\tilde{\mu}_{j'\to i} = (\tilde{\mu}^0_{j'\to i}, \tilde{\mu}^1_{j'\to i})$ is a column vector, then

$$\mathcal{F}\{\tilde{\mu}_{j'\to i}\} = F \tilde{\mu}_{j'\to i}, \tag{17}$$

where

$$F \propto \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{18}$$

The inverse transform can also be achieved by multiplying by F (up to some unimportant scaling factor). $\lambda_{i\to j}$ is a permutation version of $\tilde{\lambda}_{i\to j}$ with

$$\lambda^b_{i\to j} = \tilde{\lambda}^{z_i - H_{ij} b}_{i\to j}. \tag{19}$$

Furthermore, the GF(4) augmented model belief propagation decoder decoding with Tanner graph is introduced. The relationship between commutator and anticommutator is given by using the inner product of the trace above, and then the description of FFT-BP algorithm is obtained. The check constraint of Eqs. (9), (11) and (14) can be written as

$$\begin{aligned} &\mathrm{tr}(H_{ij}\bar{b} + \sum_{j' \in \mathcal{N}(i)\setminus j} H_{ij'} \bar{e}_{j'}) \\ &= \mathrm{tr}(H_{ij}\bar{b} + \sum_{j' \in \mathcal{N}(i)\setminus j} \tilde{e}_{j'}) = \mathrm{tr}(H_{ij}\bar{b} + z_i - H_{ij} b) = z_i, \end{aligned} \tag{20}$$

where $\tilde{e}_{j'} = H_{ij'} \bar{e}_{j'}$. The definition of $\tilde{\lambda}^b_{i\to j}$ is the same as that of $\tilde{\mu}^{\tilde{e}_{j'}}_{j'\to i} = \tilde{\mu}^{(H^{-1}_{ij'} \tilde{e}_{j'})^{-1}}_{j'\to i} = \tilde{\mu}^{H_{ij'} \tilde{e}^{-1}_{j'}}_{j'\to i}$ in Eq. (20). Thus, $\tilde{\lambda}_{i\to j}$ can be calculated by using the Hadamard transformation with

$$F \propto \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes 2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{21}$$

$\tilde{\lambda}^b_{i\to j}$ corresponds to $\sum_{j'} \tilde{e}_{j'} = b$ and as such can be used to determine $\lambda^b_{i\to j}$, which corresponds to $e_{j'} = b$. If $z_i = 0$, then $H_{ij}\bar{b} + \sum_{j'} \tilde{e}_{j'} = 0$ or 1; conversely, if $z_i = 1$, then $H_{ij}\bar{b} + \sum_{j'} \tilde{e}_{j'} = \omega$ or $\bar{\omega}$. Therefore, for $z_i = 0$ the elements of $\lambda^b_{i\to j}$ are

$$\lambda^b_{i\to j} = \frac{1}{2}[\tilde{\lambda}^{-H_{ij}\bar{b}}_{i\to j} + \tilde{\lambda}^{1-H_{ij}\bar{b}}_{i\to j}], \tag{22}$$

and for $z_i = 1$

$$\lambda^b_{i\to j} = \frac{1}{2}[\tilde{\lambda}^{\omega - H_{ij}\bar{b}}_{i\to j} + \tilde{\lambda}^{\bar{\omega} - H_{ij}\bar{b}}_{i\to j}]. \tag{23}$$

These can be combined to give

$$\lambda^b_{i\to j} = \frac{1}{2}[\tilde{\lambda}^{\omega z_i - H_{ij}\bar{b}}_{i\to j} + \tilde{\lambda}^{\omega z_i + 1 - H_{ij}\bar{b}}_{i\to j}]. \tag{24}$$

5. Main results

In this paper, we mainly analyze and calculate the simulation of GF(2) augmented and GF(4) augmented of bicycle code [[450,200]] on the depolarizing channel. Compared with the random perturbation strength of the existing decoders,[47] the FER performance of decoders is as shown in Fig. 6 below.

Figure 6 shows the relationship between p and FER for GF(2), GF(4), GF(2) augmented model and GF(4) augmented

model, respectively. What is remarkable is the degree to which it helps, with a significantly greater relative gain than a novel GF(4) augmented model BP decoder with Tanner graph over other decoders. By comparing 3 and 4 in Fig. 6 horizontally, it can be seen that when $p = 0.0115$–0.0116, the GF(4) augmented decoder is one order of magnitude lower than GF(2) augmented decoder, and the minimum value of FER for GF(4) augmented decoder is 7.1975×10^{-5} when $p = 0.0115$. At this point, FER$= 7.1975 \times 10^{-5}$ is the low-loss decoder of GF(4) augmented model BP decoder compared with the existing decoder. Furthermore, a longitudinal comparison is made to compare 1 and 3 in Fig. 6. It can be seen from the minimum value of each figure that GF(2) augmented model decoder can withstand greater random perturbation strength when FER is of the same order of magnitude, and the decoding effect is better than GF(2) decoder. Therefore, when $p = 0.005$–$0.0115(0.0116)$, it shows a downward trend, and then the decoder plays a vital role. As shown in Fig. 7, when $p = 0.0115$, the FER performance of the decoder is constantly changing under different attempts.

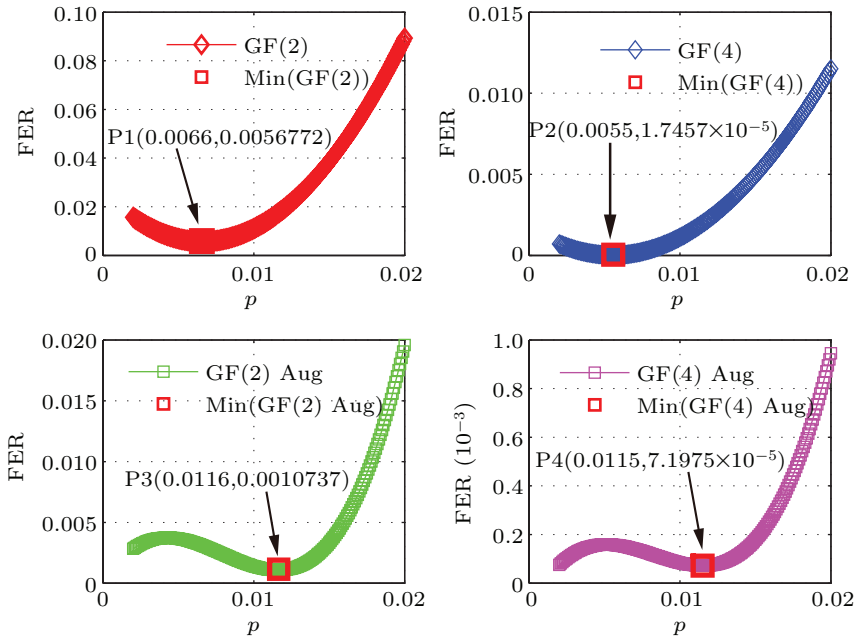


Fig. 6. The relationship between p and FER. As can be seen from the third and fourth pictures of Fig. 6, there is a small increment of FER before $p = 0.005$, which is due to the influence caused by noise in the environment. The decoder also needs some time to adapt to the noise in the environment.

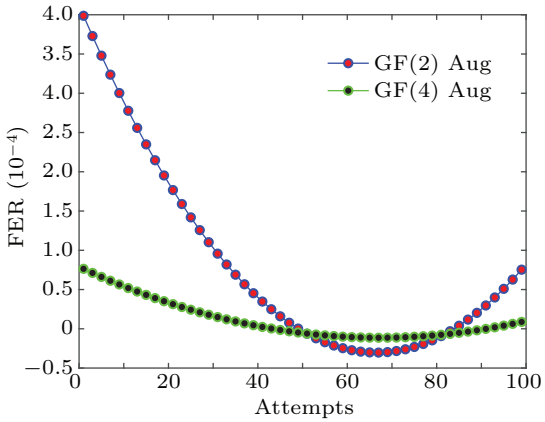


Fig. 7. The relationship of attempts and FER in GF(2) Aug and GF(4) Aug. In the case of certain random perturbation strength, when the number of attempts is 50–80, the FER of GF(2) augmented model decoder appears negative number, at this point, it has a gradient disappearance, which indicates that it has failed.

As can be seen from Fig. 7, the FER of GF(4) augmented model BP decoder does not change significantly with the increase of the number of attempts. However, GF(2) augmented model BP decoder fluctuates greatly. In effect, the novel GF(4) augmented model BP decoder has the highest efficiency and is more suitable to be used as a decoder for quantum error-correction codes. Moreover, at a given random perturbation strength $p = 0.0115$ and the number of attempts $N = 60$–70, its minimum FER can reach an order of magnitude of 10^{-5}. Compared with GF(4) augmented decoder, the stability of GF(2) augmented decoder is far less than its.

6. Conclusion

The paper mainly includes two aspects. On the one hand, Tanner graph plays a key role in the construction of decoding algorithm. On the other hand, the characteristics of cyclic difference sets of QLDPC codes and the construction of sparse matrices provide a solid foundation for the belief propagation algorithm. Therefore, a new GF(4) augmented model belief propagation decoder with Tanner graph is found, which is suitable for the new code. According to the simulation of the GF(2) Aug decoder and the GF(4) Aug decoder of bicycle code [[450,200]] on the depolarizing channel, when $p =$ 0.0115–0.0116 and number of attempts $N =$ 60–70, the FER of the novel decoder is nearly zero decreased to 7.1975×10^{-5}.

The decoder has a wide range of applications, with better FER performance than the random perturbation decoder. Due to the construction of the Tanner graph is not unique, the Tanner graph can be found that is most suitable for this decoder. In the future, quantum fault tolerance and threshold or noise compression information will be further investigated.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 11975132 and 61772295), the Natural Science Foundation of Shandong Province, China (Grant No. ZR2019YQ01), and the Higher Education Science and Technology Program of Shandong Province, China (Grant No. J18KZ012).

References

[1] Ma H Y, Teng J K, Hu T, Shi P and Wang S M 2020 *Wireless. Pers. Commun.* **113** 337
[2] Yang H, Qin L G, Tian L J and Ma H Y 2020 *Chin. Phys. B* **29** 040303
[3] Ma H Y, Xu P A, Shao C H, Chen L B, Li J X and Pan Q 2019 *Int. J. Theor. Phys.* **58** 4241
[4] Bennett C H and Brassard G 2020 *International Conference on Computers, Systems and Signal Processing* **175** 179
[5] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[6] Britt B C 2020 *Quantum Engineering* **2** e29
[7] Long G L, Li X and Sun Y 2002 *Phys. Lett. A* **294** 143
[8] Yang Y, Cao H X and Zhang Z J 2020 *Sci. China Phys. Mech. Astron.* **63** 210312
[9] Valagiannopoulos C 2020 *Quantum Engineering* **2** e52
[10] Zhou L, Liu J, Liu Z K, Zhong W and Sheng Y B 2020 *Quantum Engineering* **3** e63
[11] Qi R Y, Sun Z, Lin Z S, Niu P H, Hao W T, Song L Y, Hang Q, Gao J G, Yin L G and Long G L 2019 *Light. Sci. Appl.* **8** 22
[12] Wu J W, Lin Z S, Yin L G and Long G L 2020 *Quantum Engineering* **1** e26
[13] Cai W Z, Ma Y W, Wang W T, Zou C L and Sun L Y 2021 *Fundamental Research* **1** 50
[14] Hu X M, Huang C X, Sheng Y B, Zhou L, Liu B H, Guo Y, Zhang C, Xing W B, Huang Y F, Li C F and Guo G C 2021 *Phys. Rev. Lett.* **126** 010503
[15] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[16] Long G L 2001 *Phys. Rev. A* **64** 022307
[17] Zhao X L, Li J L, Niu P H, Ma H Y and Luan D 2017 *Chin. Phys. B* **26** 030302
[18] Zhou N R, Li J F, Yu Z B, Gong L H and Farouk A 2017 *Quantum. Inf. Process.* **16** 4
[19] Zhou N R, Zhu K N and Zou X F 2019 *Annalen Der Physik* **531** 1800520
[20] Zhou N R, Huang L X, Gong L H and Zeng Q W 2020 *Quantum. Inf. Process.* **19** 284
[21] Qin L G, Wang Z Y, Ma H Y, Wang S M and Gong S Q 2017 *Chin. Phy. B* **26** 128502
[22] Liu H, Qin L G, Tian L J and Ma H Y 2019 *Chin. Phys. B* **28** 108502
[23] Zhang M, Zhou L and Zhong W 2019 *Chin. Phys. B* **28** 010301
[24] Calderbank A R and Shor P W 1996 *Phys. Rev. A* **54** 1098
[25] Steane A M 1996 *Phys. Rev. Lett.* **77** 793
[26] Rigby A, Olivier J C and Jarvis P 2019 *Phys. Rev. A* **100** 012330
[27] MacKay D J, Mitchison G and McFadden P L 2004 *IEEE Trans. Inf. Theory* **50** 2315
[28] Wang Y J, Sanders B C, Bai B M and Wang X M 2012 *IEEE Trans. Inf. Theory* **58** 1231
[29] MacKay D J 1999 *IEEE Trans. Inf. Theory* **45** 399
[30] Yahalom E B and Etzion T 1997 *IEEE International Symposium on Information Theory IEEE* **80** 247
[31] Holevo A S and Shirokov M E 2013 *IEEE Elect. Lett.* **49** 15
[32] Nielsen M A and Chuang I 2002 *Proc SPIE* **70** 558
[33] Holevo A S 2013 *Physica Scripta* **415** 422
[34] Lenzini L, Mingozzi E and Stea G 2008 *Quantum Information and Computation* **65** 922
[35] MacKay D J 2003 *Information Theory* (Cambridge: Cambridge University Press)
[36] Hagiwara M and Imai H 2007 *IEEE International Symposium on Information Theory*
[37] Tan P Y and Li J 2010 *IEEE Trans. Inf. Theory* **56** 476
[38] Chamberland C, Kubica A, Yoder T J and Zhu G Y 2020 *New J. Phys.* **22** 2
[39] Leifer M S and Poulin D 2008 *Annals of Physics* **323** 1899
[40] Babar Z, Botsinis P, Alanis D, Ng S X and Hanzo L 2015 *IEEE Access* **3** 2492
[41] Calderbank D M J 2000 *Journal of Geometry and Physics* **36** 152
[42] Rigby A, Olivier J C and Jarvis P 2020 *Phys. Rev. A* **15** 204
[43] Calderbank A R, Rains E M, Shor P and Sloane N J 1998 *Applied and Computational Harmonic Analysis* **5** 332
[44] Rigby A, Olivier J C and Jarvis P 2019 *Phys. Rev. A* **100** 062303
[45] Apostolov V, Calderbank D M J and Gauduchon P 2020 *Mathematical Research Letters* **27** 1565
[46] Gottesman 1996 *Phys. Rev. A* **1862** 1869
[47] Poulin D and Chung Y 2008 *Quantum Inf. Comput.* **8** 987