Syndrome-Generalized Belief Propagation Decoding for Quantum Memories

Nithin Raveendran, Mohsen Bahrami, and Bane Vasić
Department of Electrical and Computer Engineering,
University of Arizona, Tucson, AZ 85721, USA.
{nithin, bahrami, vasic}@email.arizona.edu

***Abstract*—Quantum low-density parity check (QLDPC) codes are promising in realization of scalable, fault tolerant quantum memory for computation. Many of the QLDPC codes constructions suffer from unavoidable short cycles in their Tanner graph which degrade the decoding performance of the belief propagation (BP) algorithm. In this paper, we propose a syndrome based generalized belief propagation (GBP) algorithm for decoding of quantum LDPC codes and analyze how the proposed algorithm escapes from short cycle trapping sets effectively compared to the BP algorithm. Simulation results show improved decoding performance of the GBP algorithm over BP for the dual containing Calderbank, Shor and Steane (CSS) codes when cycles of length 4 are considered in the region based approach.**

***Index Terms*—Generalized Belief Propagation decoding, quantum LDPC codes, Syndrome decoding, Maximum Likelihood decoding.**

I. Introduction

Storing quantum information is indeed the primal step toward the objective of manipulating quantum information for computation. Quantum memory is also important for long-distance quantum communication, primarily in the context of implementation of quantum repeaters. Recent experimental results show advances in quantum memories with longer storage times, higher efficiency using new improved systems such as rare-earth ion doped crystals and single atoms [1]. On the theoretical side, research on new and existing quantum memory protocols, promising proposals for quantum error correction and applications for quantum storage are significant milestones towards future quantum computer [2].

Quantum error correction (QEC) is an integral step towards realizing such a fault tolerant quantum memory for computation [2] as it protects quantum information bits (qubits) from quantum noise or decoherance caused by unwanted measurements or undesirable evolution of quantum states. The QEC mechanism proceeds by continuously gathering parity information by quantum measurement followed by classical error correction/processing to apply a corrective quantum operation on the quantum data.

Though surface codes [3], [4] are a prominent pick for the task due to locality of gates required and good error threshold (1%), the number of qubits that can be encoded using these codes is limited. Another prominent class of QEC codes that have asymptotically finite rate are the quantum low density parity check (QLDPC) codes (non-local generalization of toric codes [5], [6]), inspired from the classical LDPC codes. Starting from the work by MacKay *et al.* [7], numerous QLDPC codes [5], [8] have been designed, with an attempt to achieve similar, capacity approaching, properties for quantum channels. Using the stabilizer formalism greatly simplifies the task of obtaining quantum LDPC codes such as the Calderbank, Shor and Steane (CSS) codes [9], [10], from the existing classical codes. However, the symplectic inner product/commutativity constraint [7] among the stabilizer generators limits the design of the best possible QLDPC codes. Optimizing commutativity constraint along with distance properties and sparsity with low weight stabilizers is therefore a challenging task.

Bicycle codes proposed by Mackay [7] provides a simple dual containing CSS code using random sparse cyclic matrices. These codes have shown good performance in comparison to other variants and constructions of CSS codes [11]. However, as mentioned before, the commutativity criterion introduces a large number of unavoidable cycles of length 4 (short cycles) in their Tanner graphs. Decoding of QLDPC codes having such short cycles using iterative decoding techniques such as belief propagation (BP) algorithm [12] is highly sub-optimal. It is quite evident that dealing with short cycles using the standard BP algorithm leads to very shallow error floors and poor decoding performance. Constraining the component codes of the CSS code to avoid short cycles adversely affects the rate and also limits the family of quantum sparse codes. Another decoding concern investigated among QLDPC codes is the symmetric degeneracy problem [13]. Though heuristic and feedback based solutions were proposed in [13], [14] to mitigate symmetric degeneracy, it still remains a challenge for iterative decoding of QLDPC codes. Hence, for generic QLDPC codes, the search for an effective decoding strategy is still a hot research topic.

A natural way of dealing with cycles in the graphical model of a code is to rely on loopy inference algorithms. There have been numerous approaches for dealing with short cycles in case of classical codes. A modified belief propagation algorithm for classical LDPC decoders [15] over graphs with isolated short cycles was proposed. However, modifications of this algorithm for nested cycles would be needed in order to handle generalized dual containing CSS like codes. Also, these short cycles are shown to be harmful trapping sets for

978-1-5386-8088-9/19/$31.00

iterative decoding algorithms [16]. In this paper, we propose using a syndrome-based Generalized Belief Propagation (GBP) decoder for the quantum decoding scenario. GBP relies on extending the cluster variation method introduced by Kikuchi [17], namely the *region graph method* proposed by Yedidia *et al.* [18]. With respect to conventional BP algorithms, GBP benefits from region-to-region message passing instead of node-to-node message passing in BP, and has been shown to dramatically outperform BP in both accuracy and convergence properties [19]–[22].

The paper is organized as follows. In Section II, we introduce quantum stabilizer codes and explain the syndrome based decoding problem. We introduce the notations and describe the syndrome based GBP decoding algorithm in detail with analysis in Section III. This is followed by simulation results for comparing the decoding performance in Section IV. Concluding remarks and future research directions are given in Section V.

II. Quantum Decoding Problem

In this section, we introduce quantum LDPC codes focusing on dual containing CSS codes using the stabilizer formalism (Refer to [10], [23] for detailed description).

A. Stabilizer Formalism

Let us denote by $\mathcal{P}_n = i^r\{I, X, Y, Z\}^{\otimes n}$, $0 \leq r \leq 3$, the n-qubit Pauli group, where $\otimes n$ denotes the n-fold tensor product, X,Y and Z are the Pauli matrices, I is the 2×2 identity matrix, and i^r is the phase factor. Let $S =< S_1, S_2, \ldots, S_m >$, $-\mathbb{1} \notin S$, be an Abelian subgroup of $\mathcal{P}_n$ with generators S_i, $1 \leq i \leq m$. Then, an $[\![n, k]\!]$ stabilizer code [9] is defined as a 2^k-dimensional subspace $\mathcal{C}$ of the Hilbert space $(\mathbb{C}^2)^{\otimes n}$ that is a common $+1$ eigenspace of S. For a stabilizer group with m independent generators, the dimension of the quantum code is $k = n - m$.

The $n-k$ stabilizer generators of an $[\![n, k]\!]$ stabilizer code can be represented using a pair of binary matrices by mapping each element (Pauli I, X, Y or Z) of generators of S to a binary tuple as follows: I $\rightarrow (0,0)$, X $\rightarrow (1,0)$, Z $\rightarrow (0,1)$, Y $\rightarrow (1,1)$. We obtain the rows of the $m \times 2n$ check matrix H_c given by

$$H_c = \left[H_{\mathrm{X}} \; H_{\mathrm{Z}}\right], \tag{1}$$

where H_{X} and H_{Z} represent binary matrices for bit flip and phase flip operators respectively. Each row in H_c denote a stabilizer generator, and a pair of corresponding columns in H_X and H_Z represent a qubit.

Among the class of stabilizer codes, we focus our attention to the CSS codes [24]. They are constructed from two classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$, where $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_1$. Let the corresponding parity check matrices be H_1 and H_2, then the check matrix of CSS code has the form

$$H_c = \begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix}.$$

The commutativity criterion on the stabilizers is satisfied only when $H_1 H_2^{\mathrm{T}} = 0$. Restricting $\mathcal{C}_2 = \mathcal{C}_1$ gives us a $[[n, 2k-n]]$ dual containing CSS code with $H_1 = H_2 = H$, $HH^{\mathrm{T}} = 0$ resulting in a simple form as follows:

$$H_c = \begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}. \tag{2}$$

In this paper, for the Monte Carlo simulation and analysis, we chose dual containing CSS code, constructed similar to Mackay's bicycle codes [7]. The parity check matrix H is obtained by using a matrix $[M \; M^{\mathrm{T}}]$ where M is cyclic matrix obtained from a $n/2$ binary vector of weight $\rho/2$ and then discarding $k/2$ rows. We use this code only a preliminary tool only to compare the efficacy of GBP algorithm over belief propagation and to show how GBP can overcome the problem of short cycles. Now, we describe the channel model.

B. Channel Model

We focus on memory-less channels wherein the error on a qubit is independent of the error on other qubits. A widely studied model is a quantum depolarizing channel (memoryless Pauli channel), characterized by the depolarizing probability p. For simplicity of comparison purposes, we limit our attention to binary decoding and for this case, a depolarizing channel is isomorphic to two independent binary symmetric channels (BSCs). This simplified model ignores the correlation between bit flip error X and phase flip error Z with a cross-over probability of $2p/3$ for the BSCs for X and Z errors [7].

Hence, an error on the n qubits can be expressed as a binary error vector of length $2n$ in the form $[\mathbf{e}_{\mathrm{Z}} \; \mathbf{e}_{\mathrm{X}}]$, where $\mathbf{e}_{\mathrm{Z}}$ and $\mathbf{e}_{\mathrm{X}}$ are binary vectors of length n representing Z and X errors. This gives the syndrome measurement as $H_c[\mathbf{e}_{\mathrm{Z}} \; \mathbf{e}_{\mathrm{X}}]^{\mathrm{T}}$. We can obtain syndrome measurements as $H\mathbf{e}_{\mathrm{X}}^{\mathrm{T}}$ and $H\mathbf{e}_{\mathrm{Z}}^{\mathrm{T}}$ for simulations using dual containing CSS codes. Hence, X and Z errors can be decoded independently by iterative algorithms over a Tanner graph corresponding to H [16].

C. Syndrome Decoding for Stabilizer Codes

The quantum decoding problem consists of determining the most likely recovery operator (up to the coset if degenerate) given the calculated error syndrome by measuring the stabilizer generators. More formally, let the code state $|\psi\rangle$ be subject to a memoryless Pauli channel and the received erroneous quantum state is $|\phi\rangle = W|\psi\rangle$, where $W \in \mathcal{P}_n$. Since Pauli operators square to identity, decoder goal is simply to recover $|\psi\rangle$ by determining W and applying to the system, i.e., $W|\phi\rangle = W^2|\psi\rangle = |\psi\rangle$.

Based on the properties of the Pauli group that each element has eigenvalues of $+1$ and -1 and any two elements commute or anti-commute, the erroneous quantum state $|\phi\rangle$ becomes an eigenstate of the elements in S with eigenvalue $+1$ or -1. The syndrome is computed by concatenating the eigenvalues of $|\phi\rangle$ for the generators of S using the mapping $1 \rightarrow 0$, $-1 \rightarrow 1$. The all-zero syndrome corresponds to no error as each codeword is stabilized by elements of S. A detectable error anti-commutes with some generator in S, otherwise it is called undetectable. The undetected errors are

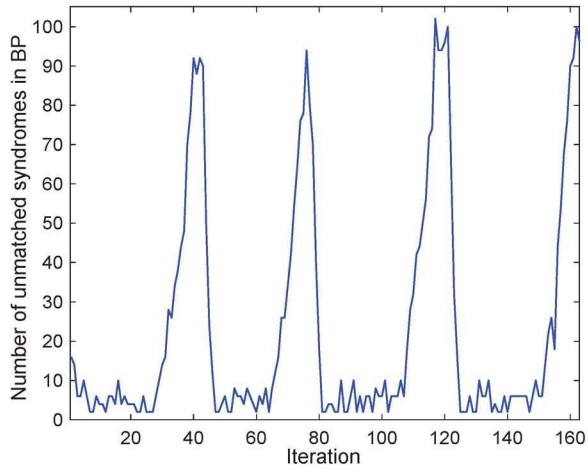


Fig. 1. Fig. shows the number of check constraints whose syndrome computed is not matched to the measured syndrome versus iterations of BP algorithm for a specific error pattern. The oscillatory behavior shows that BP is not able to converge to the initial measured syndrome in the presence of numerous short cycles.

either due to the error operators which take one codeword to another codeword or by those that are degenerate errors, belonging to the stabilizer group.

D. Shortcomings of Iterative Decoding

Syndrome-based belief propagation algorithm [11], [13] and its variants are used for iterative decoding of QLDPC codes. Observe that for a dual containing QLDPC code, the row weights ρ of the parity check matrix H are necessarily even, and every pair of rows of H must have an even overlap of 1's. This ensures that the symplectic inner product criterion is satisfied, but results in numerous *cycles of length* 4 in the Tanner graph. We can guarantee zero length-4 cycles iff the rows of H have disjoint supports, which in turn leads to poor error correction. Thus, short cycles become an unavoidable barrier for the decoding of dual containing QLDPC codes. We now present an example wherein, BP fails to converge.

Oscillations in Syndrome BP: We analyze the messages passed on a factor graph corresponding to the H matrix for dual containing QLDPC code of size $(n-k)\times n$ = (200×400) and $\rho = 8$ having 1200 cycles of length 4, and track the beliefs and syndrome calculated at each iteration. In Fig. 1, observe that the BP algorithm fails to converge to the measured syndrome in these iterations. Such oscillatory behavior occurs when messages pass over short cycles repeatedly and propagate incorrect beliefs.

We propose the syndrome based GBP in Section III which can compute the true beliefs even in the presence of nested cycles and show that the syndrome decoder correctly converges to the initial measured syndrome.

III. Generalized Belief Propagation Algorithm

The GBP [18] is a graph based algorithm which can provide an approximate solution to the problem of minimizing the Gibb's free energy. The algorithm provides a method to approximate marginal probabilities of a probability distribution function. Therefore, GBP can compute the maximum *a posteriori* (MAP) estimates which makes it suitable for soft information symbol-based MAP decoding [18], [25]. In [18], it has been shown that the GBP algorithm provides exact marginal probabilities when the corresponding region graph has no loops. For the region graphs with loops (loopy region graphs), the algorithm is empirically demonstrated to provide a good approximation to true marginals at the expense of large computational complexity [26], [27]. We now describe the factor graph representation and then reformulate the problem of syndrome based iterative decoding adapted for the GBP algorithm.

A. Factor Graph Representation

A factor graph representation for the problem of syndrome based decoding can be formulated as follows. The factor graph of this problem is a bipartite graph consisting of two sets of nodes: variable nodes $\mathbf{V}$ and factor nodes $\mathbf{C}$. The variable nodes represent the error patterns and the factor nodes check the syndrome constraints. There exists an edge between the variable node $V\in\mathbf{V}$ and the check node $C\in\mathbf{C}$ if the variable node V is involved in the syndrome constraint of check node C. We denote the set of variable nodes which are connected to the factor node C by $\mathcal{N}_C$ and the set of factor nodes connected to the variable node V by $\mathcal{N}_V$. Fig. 2(a) shows the factor graph for the H matrix of the classical $(7,4)$ Hamming code used in the dual containing CSS code (Eq. 2): $[\![7,1]\!]$ Steane code as an example.

B. Syndrome Based Generalized Belief Propagation Decoder

We have the observed syndrome $\sigma=(\sigma_1,\sigma_2,\ldots,\sigma_m)\in\{0,1\}^m$ as an input to the decoder. The problem is to find the most-likely error pattern $\hat{\mathbf{e}}=(\hat{e}_1,\hat{e}_2,\ldots,\hat{e}_n)$ which satisfies the observed syndrome. More precisely, we are interested in the most-likely error pattern $\hat{\mathbf{e}}$ such that

$$\hat{\mathbf{e}}=\bigcup_{i=1}^{n}\arg\max_{e_i} p(e_i|\sigma), \tag{3}$$

subject to the constraint that $H\hat{\mathbf{e}}^T=\sigma \bmod 2$, where H is the parity check matrix of code. Assuming the uniform distribution over all possible error patterns satisfying the syndrome σ, the *a-posteriori* probability of error pattern $\mathbf{e}=\{e_1,e_2,\ldots,e_n\}$ given the observed syndrome σ is

$$p\left(\mathbf{e}|\sigma\right)=\frac{p\left(\sigma|\mathbf{e}\right)p(\mathbf{e})}{p(\sigma)}\propto p(\sigma|\mathbf{e}), \tag{4}$$

and

$$p\left(\sigma|\mathbf{e}\right)=\prod_{j=1}^{m}\mathbb{1}\left\{h_j\mathbf{e}^T=\sigma_j \bmod 2\right\}p(\sigma_j|\mathbf{e}_j), \tag{5}$$

where $\mathbf{e}_j$ indicates the bits which are involved in the j^{th} syndrome constraint, h_j is the j^{th} row of H matrix, $p(\sigma_j|\mathbf{e}_j)$ is the probability of satisfying the j^{th} syndrome constraint given $\mathbf{e}_j$ and $\mathbb{1}\{.\}$ is the indicator function which equals one (resp., zero) when its argument is true (resp., false). Therefore, we have

$$p\left(\mathbf{e}|\sigma\right) = \frac{1}{Z(\sigma)} \prod_{j=1}^{m} \mathbb{1}\left\{h_j \mathbf{e}^T = \sigma_j \bmod 2\right\} p\left(\sigma_j|\mathbf{e}_j\right), \quad (6)$$

where the normalization constraint $Z(\sigma)$, so called the partition function, is given by

$$Z(\sigma) = \sum_{\mathbf{e}: H\mathbf{e}^T = \sigma \bmod 2} \prod_{j=1}^{m} \mathbb{1}\left\{h_j \mathbf{e}^T = \sigma_j \bmod 2\right\} p\left(\sigma_j|\mathbf{e}_j\right). \quad (7)$$

We denote by $b(\mathbf{e})$ the belief corresponding to the *a posteriori* probability $p\left(\mathbf{e}|\sigma\right)$. Using the Kullback-Liebler distance properties [28], we can show that $b(\mathbf{e}) = p\left(\mathbf{e}|\sigma\right)$ can be achieved by minimizing the Gibb's free energy F such that

$$F(\mathbf{e}) = U(\mathbf{e}) - H(\mathbf{e}) = \mathcal{D}\left(b\left(\mathbf{e}\right) \parallel p\left(\mathbf{e} \mid \sigma\right)\right) - \ln Z(\sigma), \quad (8)$$

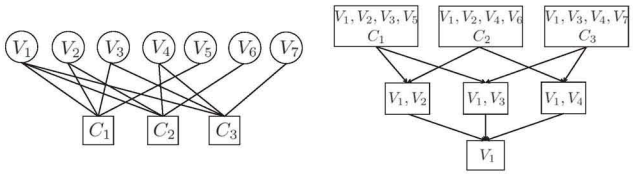
where

$$U(\mathbf{e}) = -\sum_{j=1}^{m} \sum_{\mathbf{e}_j} b(\mathbf{e}_j) \ln p\left(\sigma_j|\mathbf{e}_j\right), \quad (9)$$

$$H(\mathbf{e}) = \sum_{\mathbf{e}} b\left(\mathbf{e}\right) \ln b(\mathbf{e}) \quad (10)$$

are the average energy and entropy of $\mathbf{e}$, respectively. According to [18], [25], the Gibb's free energy can be estimated using the region-based approximation (RBA) method. In order to use the region-based approximation method, we need to construct a valid region graph of the problem in a such way that every variable node and every factor node in the factor graph of the quantum code contain at least in one region.

In [18], a region graph construction for the problem of symbol-based decoding is introduced. We extend it and formulate a method for syndrome based decoding problem with the factorization given in the Eq. (5). Each basic (ancestor) region consists of only one factor node $C \in \mathbf{C}$ and its neighboring variable nodes $\mathcal{N}_C$ such that the region graph is initially made of m basic regions, where m is the number of syndrome constraints. Then, the cluster variation method [18] is applied to establish the remaining of the region graph. We construct the remaining regions by taking the intersection of the basic regions and their intersections. The set of all regions in the region graph is denoted by $\mathcal{R}$. For every region $R \in \mathcal{R}$, we denote the set of variable nodes in the region R by $\mathbf{V}_R$ and the error pattern associated with these variables by $\mathbf{e}_R$. Let $b\left(\mathbf{e}_R\right)$ and $p\left(\mathbf{e}_R\right)$ be the belief and the probability of the error pattern $\mathbf{e}_R$, respectively. Fig. 2 shows the factor and region graphs for the syndrome based decoding problem of the $(7, 4, 3)$ Hamming code as an example of a QLDPC code.



(a) (b)

Fig. 2. The factor and region graphs for the problem of syndrome based decoding of the $(7, 4, 3)$ Hamming code are given. In Fig. 2 (a), the set of variable nodes $\mathbf{V} = \{V_1, V_2, \ldots, V_7\}$ represents the error patterns and the set of factor nodes $\mathbf{C} = \{C_1, C_2, C_3\}$ verify the syndrome constraints. In Fig. 2 (b), first layer of the region graph consists of 3 basic (ancestor) regions with only one factor node and its neighboring variable nodes in the factor graph. The rest of region graph is then constructed using the cluster variation method [18].

According to [18], the Gibb's free energy can be approximated using the RBA method as

$$\hat{F}(\mathbf{e}) = U_{\mathcal{R}}(\mathbf{e}) - H_{\mathcal{R}}(\mathbf{e}), \quad (11)$$

where $U_{\mathcal{R}}$ and $H_{\mathcal{R}}$ are respectively the region average energy and region entropy. The region average energy and region entropy are

$$U_{\mathcal{R}}(\mathbf{e}) = -\sum_{j=1}^{m} \sum_{\mathbf{e}_j} b(\mathbf{e}_j) \ln p\left(\sigma_j|\mathbf{e}_j\right), \quad (12)$$

$$H_{\mathcal{R}}(\mathbf{e}) = \sum_{R} c_R \sum_{\mathbf{e}_R} b\left(\mathbf{e}_R\right) \ln b(\mathbf{e}_R), \quad (13)$$

where $\mathbf{e}_j$ is the set of bits which are involved in the j^{th} syndrome constraint and c_R is the counting number of the region R and obtained from $c_R = 1 - \sum_{p \in \mathcal{A}_R} c_p$, where $\mathcal{A}_R$ is the set of ancestors of region R given by

$$\mathcal{A}_R = \{R' \in \mathcal{R} | R \subset R'\}. \quad (14)$$

We should note that for the region R if $\mathcal{A}_R = \emptyset$, then $c_R = 1$.

The marginal probabilities $\{p(e_i|\sigma)\}_{i=1}^{n}$ can be estimated by minimizing Eq. (11) subject to the edge constraints given by

$$\sum_{U \in \mathbf{e}_{P \setminus R}} b(\mathbf{e}_U) = b(\mathbf{e}_R) \quad \forall P \in \mathcal{P}_R, \forall R \in \mathcal{R} \quad (15)$$

and the normalization constraints given by

$$\sum_{\mathbf{e}_R} b(\mathbf{e}_R) = 1, \forall R \in \mathcal{R}. \quad (16)$$

The edge constraints ensure that the belief of a region can be obtained from its parent regions, where the parent regions of a region R is identified by

$$\mathcal{P}_R = \{R' \in \mathcal{R} | R \subset R', \nexists R'' \in \mathcal{R},\ R \subset R'' \subset R'\}. \quad (17)$$

The message and belief update equations of GBP for the problem of syndrome based decoding are obtained from solving the constrained minimization problem of the approximate Gibb's free energy $\hat{F}(\mathbf{e})$ using Lagrange multipliers. For every region $R \in \mathcal{R}$, the update messages from its parent regions $P \in \mathcal{P}_R$ at iteration $k \geq 1$ is given by

$$m^{(k)}_{P\to R}(\mathbf{e}_R) = \frac{\sum\limits_{\mathbf{e}_{P\setminus R}} b^{(k-1)}(\mathbf{e}_P)}{\prod\limits_{A_j\in\mathcal{A}_R} p(\sigma_j|\mathbf{e}_j)\left(\prod\limits_{P''\in\mathcal{P}_R} m^{(k)}_{P''\to R}(\mathbf{e}_R)\right)\left(\prod\limits_{D\in\mathcal{D}_R}\prod\limits_{P'\in\mathcal{P}_{D\setminus R}} m^{(k)}_{P'\to D}(\mathbf{e}_D)\right)},$$

where $\mathcal{D}_R$ is the descendant regions of the region R identified by

$$\mathcal{D}_R = \{R' \in \mathcal{R} | R \supset R'\}. \tag{18}$$

We set the initial beliefs of regions to be uniform. The belief update equation for every $R \in \mathcal{R}$ at iteration $k \geq 1$ is given by

$$b^{(k)}(\mathbf{e}_R) \propto \prod_{A_j\in\mathcal{A}_R} p(\sigma_j|\mathbf{e}_j)\left(\prod_{P\in\mathcal{P}_R} m^{(k)}_{P\to R}(\mathbf{e}_R)\right) \times \left(\prod_{D\in\mathcal{D}_R}\prod_{P'\in\mathcal{P}_{D\setminus R}} m^{(k)}_{P'\to D}(\mathbf{e}_D)\right). \tag{19}$$

Then, we can obtain the estimated error pattern $\hat{\mathbf{e}}^{(k)}$ at iteration $k \geq 1$ using the beliefs of regions. The iterative algorithm is terminated at iteration k if $\hat{\mathbf{e}}^{(k)}$ satisfies the observed syndrome σ, else is continued till the predefined maximum number of iteration.

IV. Simulation Results

In this section, we compare the syndrome based GBP with BP algorithm by performing Monte Carlo simulations. As explained in Section II-D, we use dual containing CSS codes, constructed similar to Mackay's bicycle codes with the simplified depolarizing noise channel model. Note that the syndrome based GBP algorithm can be used for decoding other classes of QLDPC codes such as the hyper graph product codes [5]. We use this example of bicycle codes for comparison purposes only.

In Fig. 3, we plot the decoding performance curves comparing syndrome GBP with the syndrome BP algorithm for 100 iterations. Result for a hard decision Gallager-B algorithm [16] is also plotted in the figure. There is an improvement of up to an order of magnitude (in FER value) when GBP decoder is used in comparison to the standard BP decoder. This shows superior ability of the GBP and the region based method to achieve significantly low FER values by breaking short cycle trapping sets.

In Fig. 1, observe that the BP algorithm fails to converge to the measured syndrome in these iterations. Such oscillatory behavior occurs when messages pass over short cycles repeatedly and propagate incorrect beliefs. In Fig. 4, we show how correctly computing the beliefs using GBP over the region graph even in presence of nested cycles, helps the decoder syndrome output to converge to the measured syndrome.

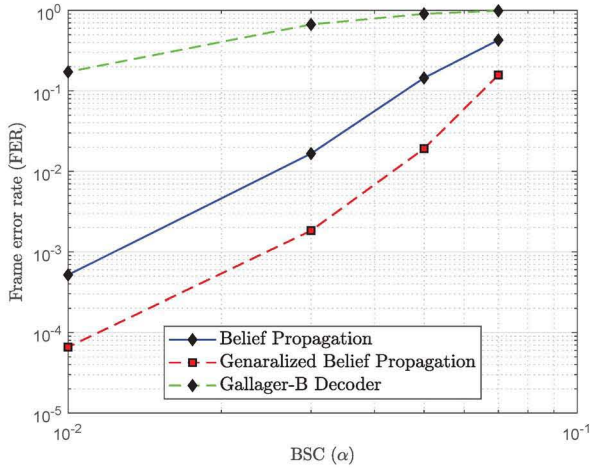


Fig. 3. Frame error rate (FER) vs. BSC($2p/3$) curves comparison between GBP algorithm, BP, and the Gallager-B algorithm for 100 iterations on the Tanner graph of H matrix with size $(n-k)\times n = (200\times 400)$ and $\rho = 8$.

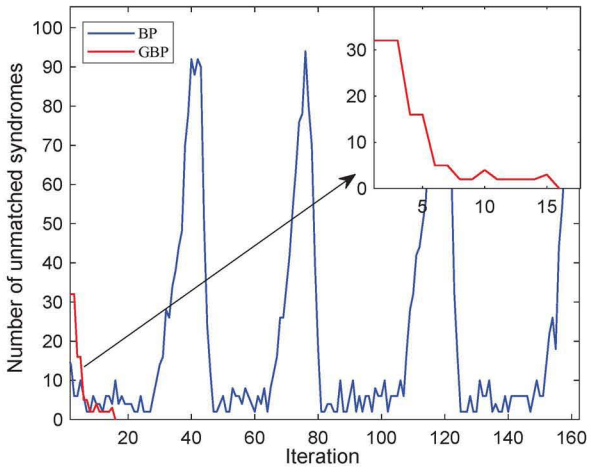


Fig. 4. Fig. shows the number of check constraints whose syndrome computed is not matched to the measured syndrome versus iterations of GBP and BP algorithm for the same error pattern as in Fig. 1. The GBP is able to converge to the initial measured syndrome in 16 iterations even in the presence of numerous short cycles.

V. Conclusions and Future Work

To summarize, we proposed a syndrome based GBP algorithm, to effectively deal with short cycles present in quantum LDPC codes. Simulation results show improved decoding performance of the GBP algorithm over BP for the dual containing CSS codes when cycles of length 4 are considered in the region based approach. Also, we observe that the convergence behavior can be improved by carefully changing the algorithm parameters. The algorithm can be naturally extended to non-binary GBP and also modified to exploit X and Z error correlations for improved performance. Also, hyper-graph product codes may be a suitable candidate for the demonstration of effectiveness of non-binary GBP algorithm.

As another future work, GBP algorithm needs to be reformulated to find the most likely error coset to make use of degeneracy of quantum codes. Also, it would be interesting to find new trapping sets that adversely affect beliefs computed by GBP algorithm. Analyzing the complexity and also finding suitable trade-offs are also considered as our future work.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation under grants ECCS-1500170 and SaTC-1813401.

REFERENCES

[1] G. Brennen, E. Giacobino, and C. Simon, "Focus on quantum memory," *New Journal of Phys.*, vol. 17, no. 5, p. 050201, 2015.

[2] B. M. Terhal, "Quantum error correction for quantum memories," *arXiv:1302.3428v7*, 2015.

[3] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *Journal of Mathematical Phys.*, vol. 43, no. 9, pp. 4452–4505, Aug. 2002.

[4] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Phys. Rev. A*, vol. 86, no. 3, p. 032324, Sept. 2012.

[5] J. Tillich and G. Zémor, "Quantum LDPC codes with positive rate and minimum distance proportional to n^{1/2}," *CoRR*, vol. abs/0903.0566, Jan. 2013.

[6] A. A. Kovalev and L. P. Pryadko, "Fault tolerance of quantum low-density parity check codes with sublinear distance scaling," *Phys. Rev. A*, vol. 87, p. 020304, Feb 2013.

[7] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.

[8] K. Liu and J. Garcia-Frias, "Optimization of LDGM-based quantum codes using density evolution," in *Proc. 48th Annual Allerton Conference on Communications, Control and Computing*, 2010, pp. 881–886.

[9] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum hamming bound," *Phys. Rev. A*, vol. 54, no. 3, pp. 1862–1868, Sept. 1996.

[10] ——, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, 1997.

[11] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. 3, pp. 2492–2519, Nov. 2015.

[12] M. Leifer and D. Poulin, "Quantum graphical models and belief propagation," *Ann. Phys.*, vol. 323, p. 1899, 2008.

[13] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," *Quantum Info. Comput.*, vol. 8, no. 10, pp. 987–1000, Nov. 2008.

[14] Y. J. Wang, B. C. Sanders, B. M. Bai, and X. M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1231–1241, Feb. 2012.

[15] N. Raveendran and S. G. Srinivasa, "A modified sum-product algorithm over graphs with isolated short cycles," *Proc. IEEE. Intl. Symp. Info. Theory*, vol. 54, pp. 2619–2623, Jun. 2014.

[16] N. Raveendran, P. J. Nadkarni, S. S. Garani, and B. Vasić, "Stochastic resonance decoding for quantum LDPC codes," in *2017 IEEE Intl. Conf. on Commun. (ICC)*, May 2017, pp. 1–6.

[17] R. Kikuchi, "A theory of cooperative phenomena," *Physical Review Online Archive (Prola)*, vol. 81, no. 6, p. 988, Mar. 1951.

[18] J. S. Yedidia, W. T. Freeman, and Y. Weiss, "Constructing free energy approximations and generalized belief propagation algorithms," *IEEE Trans. Inform. Theory*, vol. 51, pp. 2282–2312, July 2005.

[19] O. Shental *et al.*, "Discrete-input two-dimensional Gaussian channels with memory: estimation and information rates via graphical models and statistical mechanics," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1500–1513, Apr. 2008.

[20] G. Sabato and M. Molkaraie, "Generalized belief propagation for the noiseless capacity and information rates of run-length limited constraints," *IEEE Trans. Comm.*, vol. 60, no. 3, pp. 669–675, Mar. 2012.

[21] J. Sibel, S. Reynal, and D. Declercq, "An application of generalized belief propagation: splitting trapping sets in LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2014, pp. 706–710.

[22] M. Khatami and B. Vasić, "Constrained coding and detection for TDMR using generalized belief propagation," in *Proc. IEEE Int. Comm. Conf.*, June 2014, pp. 3889–3895.

[23] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, England, 2000.

[24] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug. 1996.

[25] P. Pakzad and V. Anantharam, "Kikuchi approximation method for joint decoding of LDPC codes and partial-response channels," *IEEE Trans. Comm.*, vol. 54, no. 7, pp. 1149–1153, July 2006.

[26] C. Matcha, M. Bahrami, S. Roy, S. Srinivasa, and B. Vasić, "Generalized belief propagation based TDMR detector and decoder," in *Proc. IEEE Int. Symp. Inf. Theory*, July 2016.

[27] C. K. Matcha, S. Roy, M. Bahrami, B. Vasić, and S. G. Srinivasa, "2D LDPC codes and joint detection and decoding for two-dimensional magnetic recording," *IEEE Trans. on Magn.*, vol. 54, no. 2, pp. 1–11, Feb. 2018.

[28] S. Kullback, *Information Theory and Statistics*. New York, NY,: Dover Publications, 1968.