Enhanced Feedback Iterative Decoding of Sparse Quantum Codes

Yun-Jiang Wang, Barry C. Sanders, Bao-Ming Bai, *Member, IEEE,* and Xin-Mei Wang, *Member, IEEE*

arXiv:0912.4546v2 [quant-ph] 23 Nov 2011

Abstract—Decoding sparse quantum codes can be accomplished by syndrome-based decoding using a belief propagation (BP) algorithm. We significantly improve this decoding scheme by developing a new feedback adjustment strategy for the standard BP algorithm. In our feedback procedure, we exploit much of the information from stabilizers, not just the syndrome but also the values of the frustrated checks on individual qubits of the code and the channel model. Furthermore we show that our decoding algorithm is superior to belief propagation algorithms using only the syndrome in the feedback procedure for all cases of the depolarizing channel. Our algorithm does not increase the measurement overhead compared to the previous method, as the extra information comes for free from the requisite stabilizer measurements.

Index Terms—Sparse quantum codes, quantum error correction, quantum channels, belief propagation, stabilizers.

I. INTRODUCTION

COMMUNICATION is limited by noise in channels, but error correction methods can efficiently offset this restriction in both classical [1], [2] and quantum [3], [4], [5], [6], [7] cases. At a simple level, multiple copies of the information can be transmitted, and a majority rule can be applied to discern the correct code, but such coding is neither practical nor efficient. Sparse graph coding, such as Gallager's low-density parity-check (LDPC) codes, offers an efficient alternative that approaches the Shannon information limit [1], [2]. Fortunately quantum coding and decoding strategies can be constructed from their classical counterparts, but unfortunately this mapping from classical to quantum coding can be problematic due to the requirement that quantum codes satisfy the duality-containing condition [8], [9]. Moreover, due to increased challenges posed by these quantum codes, performance improvement requires further progress in the proposed decoding algorithm [10], [11].

The entanglement-assisted (EA) stabilizer formalism adds error-free entangled bits as a consumable resource for performing quantum error correction. This EA approach overcomes the duality-containing requirement and thus offers a rich lode of quantum error correction protocols inspired by classical protocols [12]. Using the EA approach, modern codes for classical channels, such as sparse codes, can easily be imported as quantum error-correcting codes [13], [14].

Our aim is to improve belief propagation (BP) decoding methods so that quantum coding is dramatically improved over existing techniques. Specifically our numerical results presented here show that an improved BP method whose heuristical feedback strategies based on exploiting all accessible information from stabilizer measurements, yield a dramatically improved block error rate (BER) for any depolarizing channel. Our methods should work for any Pauli noise channel.

For n qubits, a Pauli channel is defined by the mapping

$$\mathcal{B}\left(\mathbb{C}^{2^n}\right) \ni \rho \mapsto \sum_{E \in G_n} p_E E \rho E^\dagger, \ p_E \geq 0, \ \sum p_E = 1 \quad (1)$$

with G_n the n-fold tensor product of single-qubit Pauli operators $\Sigma \in \{I, X, Z, Y = XZ\}$. Our interest is focused on memoryless channels wherein the error on each qubit is independent of the error on any other qubit. In particular we consider the depolarizing channel, which is the most-studied case [9], [10], [11], [13], [27]: for fixed channel error probability p, the error on qubit q is given by

$$\mathcal{B}\left(\mathbb{C}^2\right) \ni \rho_q \mapsto p_I \rho_q + (1 - p_I)\left(X\rho_q X + Y\rho_q Y + Z\rho_q Z\right)/3 \quad (2)$$

with $p_I := 1 - p$ denoting the probability of no error occurring.

In quantum settings, due to the inability to measure each and every qubit, syndrome-based decoding is typically chosen. Consequently, decoders using Pauli channels are generally considered to be hard-decision decoders. In other words, in quantum decoding, the conventional soft-decision techniques are not applicable when the channel is in the Pauli channel model. Generally, sparse quantum codes are decoded by using syndrome-based BP decoding algorithms which automatically imply hard-decision decoding. Though there is an equivalence between syndrome-based decoding and a posteriori probability decoding (signal-based decoding) under this setting, the syndrome-based decoding results in a serious drawback to BP decoder: the symmetric degeneracy error [10]. Fortunately, Poulin and Chung (PC08) [10] propose a solution to the symmetric degeneracy error by using the random perturbation method.

Motivated by the soft-decision techniques used in classical settings, which provide extra reliable information on the message nodes thereby yielding a better error correcting capacity [16], we develop a new heuristical feedback adjustment strategy for the standard BP decoder. When used in decoding sparse quantum codes, our method can on one hand solve the symmetric degeneracy error problem, and on the other hand can provide more useful information to the message nodes.

Yun-Jiang Wang is with the State Key Laboratory of Integrated Services Network, Xidian University, Xi'an, Shannxi 710071, P. R. China and with the Institute for Quantum Information Science at the University of Calgary, Alberta T2N 1N4, Canada (e-mail: yunjiang.w@gmail.com).

Barry C. Sanders is with the Institute for Quantum Information Science at the University of Calgary, Alberta T2N 1N4, Canada.

Bao-Ming Bai and Xin-Mei Wang are with the State Key Laboratory of Integrated Services Network, Xidian University, Xi'an, Shannxi 710071, P. R. China.

The difference between PC08 and our approach is that, in PC08, they feed back only the syndrome of the decoder output to adjust prior error probability distributions for received qubits. These adjusted distributions are then fed back into the decoder. We significantly improve this protocol by feeding back not just the syndrome but also the values of the frustrated checks on individual qubits of the code and the channel model; accordingly we introduce a new adjustment strategy. Specifically, our approach, which is based not only on syndromes but also on frustrated checks obtained from full stabilizer measurements and the channel model, yields a better BER for the case of depolarizing quantum channels.

We provide a detailed description of our basic BP decoder for decoding sparse quantum codes. The basic BP decoder introduced here is inspired by the strategy used for decoding sparse classical quaternary codes under the BP algorithm. Using this strategy, we can decode sparse quantum codes directly regardless of whether they arise from classical binary codes or not and regardless of whether they are Calderbank-Shor-Steane (CSS) construction [4], [19] codes or not.

II. BP Iterative Decoding

In this section, we briefly reprise the essential elements of BP iterative decoding for sparse quantum codes. In Subsec. II-A we discuss the key idea of standard BP iterative algorithms. Then we compare decoding of classical codes vs quantum codes, and introduce the standard BP decoding for quantum codes. Finally in Subsec. II-B we show how to decode sparse quantum codes in $GF(4)$ based on the standard BP algorithm.

A. BP decoding algorithm for sparse quantum codes

Consider a k-bit message that is encoded into an n-bit codeword, which is then transmitted through a noisy channel. The received message is an error-prone vector over the output alphabet, and there is no guarantee that decoding will reveal the original codeword. However, the codeword can be guessed with a high probability of being correct by maximizing the probability for this codeword based on the observed output vector [20]. Unfortunately for a linear block code, encoding k information bits into n bits allows 2^k possible n-bit codewords, and calculating conditional probabilities for individual codewords is too expensive in practice.

BP algorithms overcome this inefficiency for sparse codes [1]. The strategy is to represent a linear-block classical error-correcting code (CECC) by a Tanner graph comprising message nodes and check nodes corresponding respectively to received bits and check constraints. Then an iterative algorithm recovers the values of received bits as follows [20], [21]. At each round, probabilities are passed from message nodes $\{v\}$ to check nodes $\{c\}$ and then from $\{c\}$ back to $\{v\}$. The probabilities from $\{v\}$ to $\{c\}$ are computed based on the observed value of the message node and other probabilities passed from the neighboring check nodes to the respective message node. It turns out that, for decoding sparse codes, the BP algorithm can provide a reasonable trade-off between complexity and performance.

For a linear block CECC, the code space can be viewed as the orthogonal projection space (solution space) of its check matrix. The sender Alice transmits her message as a codeword that is encoded according to a specific check (or generator) matrix through the channel. When receiver Bob obtains the channel output, the received vector may not be the solution vector of the check matrix. Therefore Bob needs to apply a smart algorithm to recover the codeword efficiently. As the check matrix is sparse, Bob employs the BP algorithm. First, Bob measures each bit to obtain its posterior probability distribution. Subsequently, he puts these probabilities into the BP decoder, and, based on the constraint that the codeword should be the orthogonal vector of the check matrix, he infers the original message. This procedure extends naturally to sparse quantum codes.

In the quantum case, the stabilizer formalism for a quantum error-correcting code (QECC) is useful. The code space within $\mathbb{C}^{2^n}$ corresponds to the simultaneous $+1$ eigenspace of all m generators of an abelian subgroup [5]

$$S = \{S_1, \ldots, S_m\} \subset G_n. \tag{3}$$

Alice transmits her message as a codeword, which propagates through the depolarizing quantum channel. Due to channel errors, the received codeword may not be the simultaneous $+1$ eigenspace of S. Bob measures S to obtain the syndrome[1] $s = (s_1, \ldots, s_m) \in \{-1, 1\}$ and then estimates which error E from Eq. (1) has occurred based on the noise model and the syndrome, which is effectively a check constraint. Bob redresses the error by applying the same error operation he inferred onto his received codeword to try to recover the quantum code. For Pauli channels all errors are n-fold tensor products of single-qubit Pauli operators hence square to the identity; thus re-applying the same error should restore the original codeword.

Due to the close analogy between CECCs and QECCs as discussed above, it is tempting to extend the BP iterative decoding algorithm to quantum settings. In fact a QECC can also be represented by a decorated Tanner graph [17], [18]. Therefore, it is natural to transmit the messages from $\{c\}$ to $\{v\}$ and the messages from the $\{v\}$ to $\{c\}$ according to the principles of BP algorithms [17], [18].

Here we first briefly review the BP algorithm used for decoding sparse quantum codes [10] but begin with necessary terminology. The probability of Pauli error E_q occurring on qubit q is $p_q(E_q)$. The neighborhood of qubit q is denoted by $n(q)$, and we define $n(c)$ similarly as the set of qubits connected to check S_c. The tensor product of Pauli errors over $n(c)$ is denoted E_c. Then, following PC08's notation, for two 1-qubit case, $E \cdot E' = 1$ means $[E, E'] = 0$ and $E \cdot E' = -1$ means $\{E, E'\} = 0$. For two n-qubit Pauli operators such as $E = E_1 \otimes E_2 \otimes \cdots \otimes E_n$ and $E' = E'_1 \otimes E'_2 \otimes \cdots \otimes E'_n$, we have

$$E \cdot E' := \prod_{k=1}^{n} E_k \cdot E'_k. \tag{4}$$

---

[1]If $[S_c, E] = 0$, $s_c = 1$ or else $s_c = -1$, where $c = 1, \cdots, m$ and S_c can be viewed as a check node in the Tanner graph of a QECC with stabilizer S from Eq. (3).

The messages from check nodes to qubit nodes are denoted

$$m_{c \to q}(E_q) \propto \sum_{\substack{E_{q'} \\ q' \in n(c) \backslash q}} \left(\delta_{s_c, S_c \cdot E_c} \prod_{q' \in n(c) \backslash q} m_{q' \to c}(E_{q'}) \right), \quad (5)$$

which is defined only up to a constant factor. The factor can be fixed by normalization [10]. The messages from qubit nodes to check nodes are similarly denoted as

$$m_{q \to c}(E_q) \propto p_q(E_q) \prod_{c' \in n(q) \backslash c} m_{c' \to q}(E_q), \quad (6)$$

where $p_q(E_q)$ is the initial probability in the definition of the memoryless channel. Then the beliefs $b_q(E_q)$ are constructed by first initializing $m_{q \to c}(E_q) = p_q(E_q)$, then evaluating according to

$$b_q(E_q) = p_q(E_q) \prod_{c \in n(q)} m_{c \to q}(E_q), \quad (7)$$

after the iteration procedure based on Eqs. (5) and (6). In fact, Eqs. (5) and (6) define a sum-product iterative procedure for decoding sparse quantum codes. Hence this algorithm is also called the sum-product algorithm (SPA), which is one of the most important algorithms based on BP.

In order to clarify the BP decoding algorithm for sparse quantum codes, we now show how to implement Eqs. (5) and (6) in GF(4).

B. Decoding sparse quantum codes in GF(4)

There is a convenient isomorphism between the Pauli group G_1 generated by $\{I, X, Z, Y = XZ\}$ and the Galois Field $GF(4)$ generated by $\{0, 1, \omega, \bar{\omega} = \omega^2\}$. The isomorphism is explained by the element identification

$$I \leftrightarrow 0, \, X \leftrightarrow 1, \, , Z \leftrightarrow \omega, \, Y \leftrightarrow \bar{\omega}(\omega^2) \quad (8)$$

and the operation identification *multiplication↔addition* and *commutativity↔trace inner product* [5]. For the one-qubit case, we have,

$$P, Q \in G_1 \leftrightarrow \hat{P}, \hat{Q} \in \text{GF}(4),$$
$$[P, Q] = 0 \Leftrightarrow \text{Tr}(\hat{P} \times \bar{\hat{Q}}) = 0, \, \{P, Q\} = 0 \Leftrightarrow \text{Tr}(\hat{P} \times \bar{\hat{Q}}) = 1 \quad (9)$$

The isomorphism is readily extended to the *n*-qubit case:

$$P, Q \in G_n \leftrightarrow \boldsymbol{u}_P, \boldsymbol{v}_Q \in \text{GF}(4)^n,$$
$$[P, Q] = 0 \Leftrightarrow \text{Tr}(\boldsymbol{u}_P \cdot \boldsymbol{v}_Q) = 0, \, \{P, Q\} = 0 \Leftrightarrow \text{Tr}(\boldsymbol{u}_P \cdot \boldsymbol{v}_Q) = 1. \quad (10)$$

where '$\cdot$' used here (between two vectors) is a regular inner product. That is, for $\boldsymbol{u} = (u_1, u_2, \cdots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$, we have,

$$\boldsymbol{u} \cdot \boldsymbol{v} := \sum_{k=1}^{k=n} u_1 \times \bar{v}_1. \quad (11)$$

The addition and multiplication rules of $GF(4)$ are shown in Tables I and II, respectively.

We can import the strategy used for decoding sparse classical quaternary codes under BP to use for decoding sparse quantum codes. This adaptation to quantum codes is achieved

TABLE I
ADDITION OF GF(4)

+	0	1	ω	$\bar{\omega}$
0	0	1	ω	$\bar{\omega}$
1	1	0	$\bar{\omega}$	ω
ω	ω	$\bar{\omega}$	0	1
$\bar{\omega}$	$\bar{\omega}$	ω	1	0

TABLE II
MULTIPLICATION OF GF(4)

$\times$	0	1	ω	$\bar{\omega}$
0	0	0	0	0
1	0	1	ω	$\bar{\omega}$
ω	0	ω	$\bar{\omega}$	1
$\bar{\omega}$	0	$\bar{\omega}$	1	ω

by transforming the check criterion (5) from commutativity to trace inner product.

For example, suppose $s_c = 1$. Then the check criterion for this check node should be $S_c \cdot E_c = 1$, which is equivalent to $[S_c, E_c] = 0$. According to isomorphism (10), $\text{Tr}(\boldsymbol{u}_{E_c} \cdot \boldsymbol{v}_{S_c}) = 0$, which implies that either $\boldsymbol{u}_{E_c} \cdot \boldsymbol{v}_{S_c} = 0$ or $\boldsymbol{u}_{E_c} \cdot \boldsymbol{v}_{S_c} = 1$ because $\text{Tr}(0) = 0$ and $\text{Tr}(1) = 0$. We define $p_q[x]$ as the probability for $\hat{E}_q \times \hat{\bar{S}}_{c_q}$ to take the value x, with S_{c_q} the qth entry of S_c,[2] and $p[x]$ the probability of $\boldsymbol{u}_{E_c} \cdot \boldsymbol{v}_{S_c} = 0$ (excluding the qth entry) to take the value x. As $q \in n(c)$,

$$S_{c_q} \in \{X, Z, Y\} \implies \hat{S}_{c_q} \in \{1, \omega, \bar{\omega}\}, x \in \{0, 1, \omega, \bar{\omega}\}, \quad (12)$$

Thus,

$$p_q[0] = (p[0] + p[1]) / 2 = p_q[1], \quad (13)$$
$$p_q[\omega] = (p[\omega] + p[\bar{\omega}]) / 2 = p_q[\bar{\omega}]. \quad (14)$$

Similarly, if $s_c = -1$, then $\{S_c, E_c\} = 0$, which implies that either $\boldsymbol{u}_{E_c} \cdot \boldsymbol{v}_{S_c} = \omega$ or $\boldsymbol{u}_{E_c} \cdot \boldsymbol{v}_{S_c} = \bar{\omega}$ because $\text{Tr}(\omega) = 1$ and $\text{Tr}(\bar{\omega}) = 1$. According to Table I,

$$p_q[0] = (p[\omega] + p[\bar{\omega}]) / 2 = p_q[1], \quad (15)$$

$$p_q[\omega] = (p[0] + p[1]) / 2 = p_q[\bar{\omega}]. \quad (16)$$

With this knowledge, the message $m_{c \to q}$ can be computed by:

$$m_{c \to q}(E_q) = p_q[\hat{E}_q \times \hat{\bar{S}}_{c_q}]. \quad (17)$$

Given $m_{c \to q}(E_q)$, $m_{q \to c}(E_q)$ can then be derived directly by substituting Eq. (17) into Eq. (6).

Decoding based on $GF(4)$ affords the advantage that sparse quantum codes can be decoded without losing correlations between errors that would otherwise impact the coding scheme's performance. In particular sparse quantum codes can be decoded directly regardless of whether they arise from a classical binary codes or not and regardless of whether they follow a CSS construction code or not. For comparison, we henceforth refer to the decoder based on this BP decoding algorithm as the 'standard BP decoder'.

---

[2]For $\hat{E}_q$ and $\hat{\bar{S}}_{c_q}$ the mapped elements of E_q and $\bar{S}_{c_q}$ in GF(4), see Eq. (9).

III. ENHANCED FEEDBACK BP ITERATIVE DECODING FOR SPARSE QUANTUM CODES

In 2008 PC08 proposed a random perturbation strategy based on the syndrome of the BP decoder output[3] to overcome the symmetric degeneracy problem. The random perturbation method is simple and efficient but unfortunately overlooks many errors. As pointed out in PC08, all errors in their simulations could be attributed to the decoder rather than to the finite minimal distance of the code.

We observe the same problems as PC08 do when using the random perturbation method. In particular, most errors in the simulations are *detected* errors, not the undetected errors. This result suggests that feeding back useful information to the standard BP decode could help. The feedback would help the BP decoder determine a valid output E_{out}, whose syndrome $s(E_{out})$ is identical with the observed syndrome s. Then E_{out} will equal E with high probability, for E the error occurring on the transmitted quantum state during transmission. In this section, we present our enhanced feedback BP iterative decoding algorithm, which provides useful information to the BP decoder based on exploiting not only the syndrome but also the stabilizer itself and the channel model in the feedback procedure.

Then suppose that, subsequent to the standard BP decoding procedure, $s(E_{out})$ is not identical with the observed syndrome s. Then evidently at least one entry of E_{out} occurring on one of the qubits connected to check S_c has an error, for S_c a frustrated check. If we can reset the initial probability distributions for errors occurring on the qubits connected to S_c in a more reliable way, but not simply by adopting the prior probability distributions obtained from the channel model, more useful information could be provided to the BP decoder. Furthermore symmetric degeneracy could also be overcome as well. Thus it is reasonable to expect that BP decoding ability will be significantly improved.

Our new feedback BP iterative decoder is devised as follows. First the standard BP decoder is used to identify the error E based on the observed syndrome and the prior probability distributions of each entry of E. When the standard BP decoder fails ($s(E_{out}) \neq s$), we randomly choose a frustrated check, say S_c. There are only two results for this frustrated check: $s_c = -1$ and $S_c \cdot E_{out} = 1$ or else $s_c = 1$ and $S_c \cdot E_{out} = -1$. Either way we choose a random qubit that connects to S_c, for example qubit q, and then reset $p_q(E_q)$ according to the value of S_{c_q} (the entry to which qubit q corresponds in S_c) and the channel model as follows.

Let $\Sigma_{1,2,3} \in \{X, Z, Y = XZ\}$ be three distinct elements. Suppose $S_{c_q} = \Sigma_1$, and the channel is the depolarizing channel with crossover probability $p = 1 - p_I$, for p_I established in Eq. (2). Then, if $s_c = -1$ and $S_c \cdot E_{out} = 1$, we reset

$$p_q(I) = (1 - p_I)/2 = p_q(\Sigma_1), \ p_q(\Sigma_2) = p_I/2 = p_q(\Sigma_3). \quad (18)$$

For example, if $S_{c_q} = X$, we obtain

$$p_q(I) = (1 - p_I)/2 = p_q(X), \ p_q(Z) = p_I/2 = p_q(Y). \quad (19)$$

Instead suppose $s_c = 1$ and $S_c \cdot E_{out} = -1$. Then we reset

$$p_q(I) = p_I/2 = p_q(\Sigma_1), \ p_q(\Sigma_2) = (1 - p_I)/2 = p_q(\Sigma_3). \quad (20)$$

In this case, if $S_{c_q} = X$, we obtain

$$p_q(I) = p_I/2 = p_q(X), \ p_q(Z) = (1 - p_I)/2 = p_q(Y). \quad (21)$$

Next, following a similar strategy to PC08's, we feed back this adjustment to the standard BP decoder and let it iterate with this modified probability distribution for T_{pert} (a predetermined fixed number of the reiteration) steps. If BP halts during this period (i.e. $s(E_{out})$ corresponds to the syndrome s), the procedure is complete and terminates.

If c is still frustrated, we restore the probability distribution $p_q(E_q)$ and choose a different qubit connected to c, say qubit q', and reset $p'_q(E'_q)$ based on the same strategy that has already been used for resetting $p_q(E_q)$. If S_c is not frustrated, but the halting condition is not yet satisfied, we choose another frustrated check $S_{c'}$ and adjust the probability distribution of the error occurring on one of its qubits as we do for a frustrated check S_c.

Now suppose that the decoder still cannot yield a valid output after trying a pre-determined number n_a feedback adjustments for qubits according to the procedures mentioned above. In other words, suppose that, after traversing n_a entries associated with frustrated checks, no valid result is yielded by the decoder. In this case, we allow the decoder to terminate this procedure and report a failure. Without the termination condition, the decoder is wasting time traversing all entries associated with frustrated checks and thereby introducing unwanted redundancy into the procedure.

Eqs. (18) and (20) are justified for the following reason. Empirically, the decoder is naturally too biased towards the identity I [10] due to the prior probability distribution obtained from the channel model. This biased probability distribution will lead to $S_c \cdot E_{out} = 1$ while $s_c = -1$. Heuristically, we reset $p_q(E_q)$ to make it anti-commute with S_{c_q} with a greater probability, since at least one entry of E anti-commutes with its corresponding entry in S_c. The channel is depolarizing that is Pauli errors X, Z, Y occur with equal probability, so, in Eq. (18), we let Σ_2 and Σ_3 share the probability as I.[4]

When $s_c = 1$, setting E_q to I is conducive to obtaining $S_c \cdot E_{out} = 1$. Another Pauli operator could also be conducive to making $S_c \cdot E_{out} = 1$ but is ignored by the prior probability distribution. We can readily ascertain this Pauli operator according to the entries of S_c. According to Eq. (20), we let this Pauli operator (Σ_1) share the same probability p_I with I and have Σ_2 and Σ_3 share the small probability $1 - p_I$ equally.

Our strategy retains PC08's capability of breaking the symmetric degeneracy while feeding back more useful information to the BP decoder than PC08 in order to help the decoder determine a valid output. More useful information comes from retaining full information about the entire stabilizer rather

---

[3] In addition to the random perturbation technique, PC08 also proposed freezing and collision techniques. However, their simulations and our own simulations indicate that the random perturbation technique has the best performance of the three approaches. Therefore, we adopt the random perturbation technique as the comparator.

[4] Because $(1 - p_I) \ll p_I$, we let I and Σ_1 share $(1 - p_I)$ equally for simplicity.

than just a syndrome. Specifically, our feedback adjustment strategy is not solely based on the syndrome but also on the channel model and on the individual values of the entries of the frustrated checks (the checks are just the generators of the stabilizer).

IV. A CASE STUDY

In this section we illustrate our enhanced feedback iterative decoding algorithm to show how it succeeds in helping the BP decoder find a valid output. For $[[n, k; c]]$ denoting an EA QECC that encodes k qubits into n qubits with the help of c ancillary ebits [12], we construct a simple EA QECC for $[[4, 1; 1]]$ as follows. According to the EA QECC formalism, we start with a classical $[4, 2]$ quaternary code with check matrix

$$H_c = \begin{pmatrix} 1 & \omega & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}. \tag{22}$$

First we transform H_c to

$$H'_c = \begin{pmatrix} H_c \\ \omega H_c \end{pmatrix} = \begin{pmatrix} 1 & \omega & 1 & 0 \\ 1 & 1 & 0 & 1 \\ \omega & \bar{\omega} & \omega & 0 \\ \omega & \omega & 0 & \omega \end{pmatrix}, \tag{23}$$

then transform H'_c to a set of (perhaps non-commuting) generators

$$H_q = \begin{pmatrix} X & Z & X & I \\ X & X & I & X \\ Z & Y & Z & I \\ Z & Z & I & Z \end{pmatrix}. \tag{24}$$

Next we transform H_q into a canonical form $\hat{H}_q$ by multiplying the third generator by the second generator and by multiplying the fourth generator by the first and second generator. Thus, we obtain

$$\hat{H}_q = \begin{pmatrix} X & Z & X & I \\ X & X & I & X \\ Y & Z & Z & X \\ Z & X & X & Y \end{pmatrix}. \tag{25}$$

Now, it is easy to check that the first generator anti-commutes with the second generator, and the last two generators commute with each other as well as commuting with the first two generators. According to the EA QECC formalism, this coding scheme needs one ebit to assist encoding. The extended commuting set of generators is $\{\tilde{H}_q\}$ for

$$\tilde{H}_q = \begin{pmatrix} X & Z & X & I & X \\ X & X & I & X & Z \\ Y & Z & Z & X & I \\ Z & X & X & Y & I \end{pmatrix}, \tag{26}$$

which is just the stabilizer of $[[4, 1; 1]]$.

It is easy to check that $\tilde{H}_q$ is isomorphic to

$$\tilde{H}'_q = \begin{pmatrix} X & I & I & I & X \\ Z & I & I & I & Z \\ I & Z & I & I & I \\ I & I & Z & I & I \end{pmatrix}, \tag{27}$$

which means we can encode one logical qubit into four physical bits with the help of one entangled pair plus two
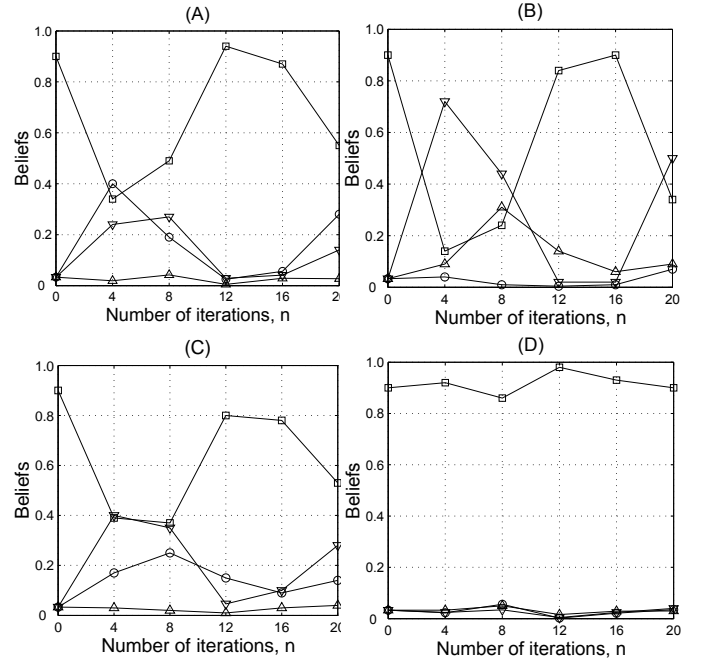

Fig. 1. Beliefs as a function of number of iterations n for an EA QECC with stabilizer generators $XZXIX$, $XXIXZ$, $YZZXI$ and $ZXXYI$ and with syndrome $(-1, +1, +1, +1)$ using the standard BP decoding algorithm. The prior $p_q(E_q)$ of the four sent qubits are obtained from the depolarizing channel with $p = 0.1$. (A), (B), (C) and (D) show the beliefs for qubits 1, 2, 3 and 4, respectively. Qubit 5 is assumed to be held by the receiver and thus to be error-free. The symbols $\square$, $\triangle$, $\bigcirc$ and ∇ indicate the beliefs for I, X, Z and Y, respectively. In this case, the output of the standard BP decoder is $E_{\text{out}} = IYII$, which is a detected error.

ancilla bits via a unitary transformation [12]. As the half of the entangled pair being held by the receiver is assumed to be error-free, the error-correcting capacity of $[[4, 1; 1]]$ only depends on the left part of $\tilde{H}_q$, which corresponds to the four transmitted qubits held by the sender.

Suppose the qubits of $[[4, 1; 1]]$ are sent through a depolarizing channel and error $E = IIZX$ is applied to the four transmitted qubits. Measurement of the stabilizer reveals the error syndrome $s = (-1, +1, +1, +1)$. In Fig. 1, we display the performance of the standard BP decoder under this setting. From Fig. 1, it is easy to check that the syndrome of the output of the standard BP decoder is $(-1, -1, -1, -1)$.[5] We now use the standard BP decoder with PC08's random perturbation. Comparing between the error syndrome $s = (-1, +1, +1, +1)$ and the syndrome of the output of the standard BP decoder $(-1, -1, -1, -1)$, the probability distributions of the errors occurring on the qubits connected to the second, third or fourth checks can be reset. For all these cases, the decoder could not yield an appropriate recovery. Here as an example, we use PC08's random perturbation strategy for the frustrated check S_2 and show the corresponding performance in Fig. 2.

Finally, we use our enhanced feedback BP decoding algorithm. By the same method, our feedback strategy can reset the probability distributions of the errors occurring on the qubits connected to the second, third or the fourth checks. When the decoder chooses the fourth entry (X) of the frustrated check S_2

---

[5]It is not surprising that the standard BP decoder has failed because $[[4, 1; 1]]$ is designed to correct one error but not two errors.
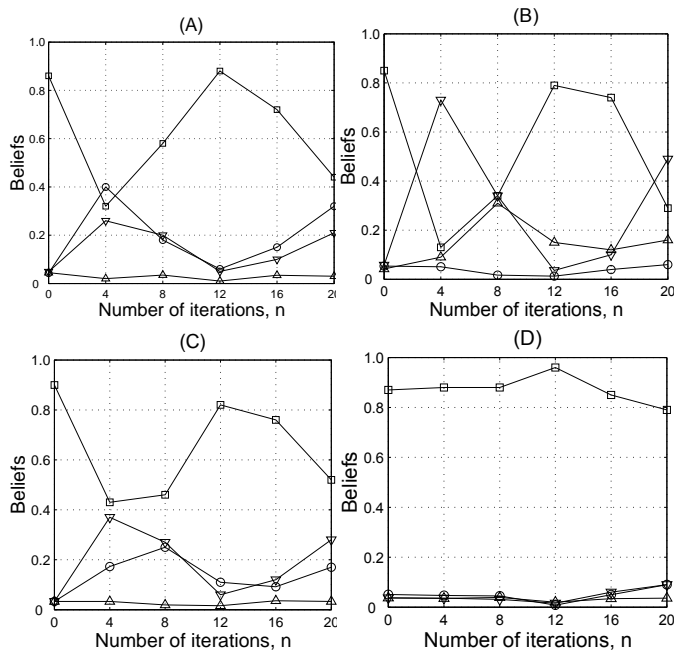
Fig. 2. Same as for Fig. 1 but using the standard BP decoding algorithm replaced by PC08 and applying random perturbation strength $\delta = 1$ to the prior for qubits 1, 2 and 4.
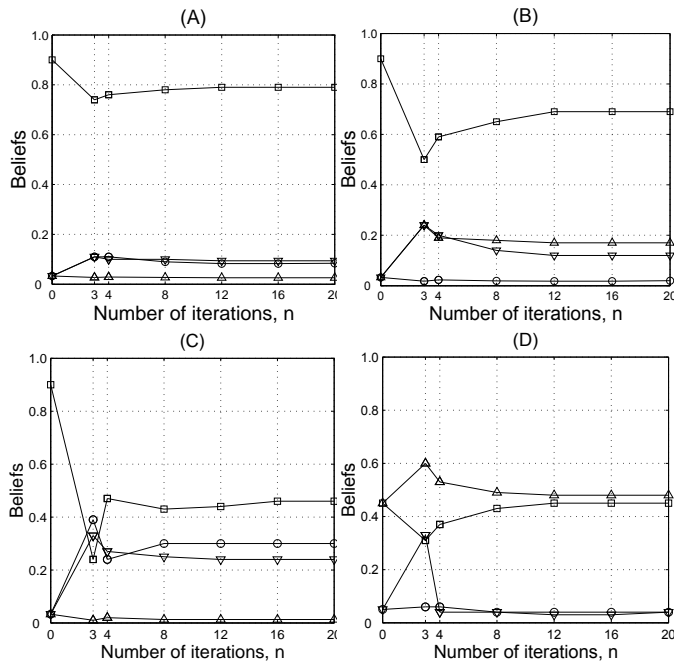

Fig. 3. Same as for Fig. 2 but using our enhanced feedback iterative decoding algorithm. Here we reset $p_4(E_4)$ according to Eq. (20). In this case, only three iterations were required to yield a valid output $E_{\text{out}} = IIZX$, which is exactly the error occurring on [[4, 1;1]] during its transmission.

and resets $p_4(E_4)$ according to Eq. (20), the correct decoding result arises in just a few iterations. We show the performance of our approach in Fig. 3.

In this example, PC08's method could not help the standard BP decoder to yield a valid output, However, our enhanced feedback BP decoding algorithm yields a valid output in just a few iterations. In fact even if the error occurring on the first four qubits is not $IIZX$ but $YZII$, which has the same

syndrome $s = (-1, +1, +1, +1)$ as $IIZX$, our decoding output $IIZX$ can still recover the transmitted quantum state because

$$IIZXI \times YZIII = YZZXI, \tag{28}$$

which is just the third generator of the extended stabilizer. Because it is hard to check whether $E \cdot E_{\text{out}} \in S$ when the number of generators of S is large, we choose $E = E_{\text{out}}$ as the success criterion of the decoding result in our simulations.

V. SIMULATION RESULTS

We have applied our enhanced feedback iterative BP decoding algorithm to a variety of sparse quantum codes, including conventional sparse quantum codes and EA sparse quantum codes over depolarizing channels. In each case, our improved BP decoder yields significantly lower BER over both the standard BP decoder and the BP decoder with PC08's random perturbation. In the following subsections, we simulate decoding of sparse quantum codes with different code parameters (including block lengths, rates, and row weight) under the three decoders to demonstrate the superiority of our approach.

A. Example: Conventional Sparse Quantum Codes

Conventional sparse quantum codes can be constructed from sparse classical dual-containing codes. One of the most successful dual-containing constructions is the so-called "Construction B" [9], which is built as follows. First we take an $n/2 \times n/2$ cyclic matrix C with row weight $L/2$, and define

$$H_0 = \begin{bmatrix} C, C^T \end{bmatrix}. \tag{29}$$

Then we delete some rows from H_0 to obtain a matrix H with m rows. By construction, H is dual-containing. A conventional sparse quantum code with length n can thus be given according to CSS construction.

Our first example is based on this strategy. We first construct a cyclic binary LDPC code [63, 37] with row weight 8 based on finite geometries [26]. This code has a 63×63 cyclic check matrix with 26 independent rows and 37 redundant rows. Hence, we can construct a conventional sparse quantum code with $n = 126$, $m = 26$, and $L = 16$. We refer to this [[126, 74]] quantum LDPC code with rate $k/n = 74/126$ and row weight 16 as 'Conventional'.[6] We show the performance of the standard BP decoder, the BP decoder with PC08's random perturbation and our enhanced feedback BP decoder when applied to Conventional over depolarizing channels in Fig. 4.[7]

---

[6]Note that in order to improve the performance of this code, we have preserved those redundant rows.

[7]In our simulation, we take the maximum number of entries traversed by the enhanced feedback decoder round down to one fifth of the code length for short codes, one tenth of the code length for medium codes and one fortieth for long codes.
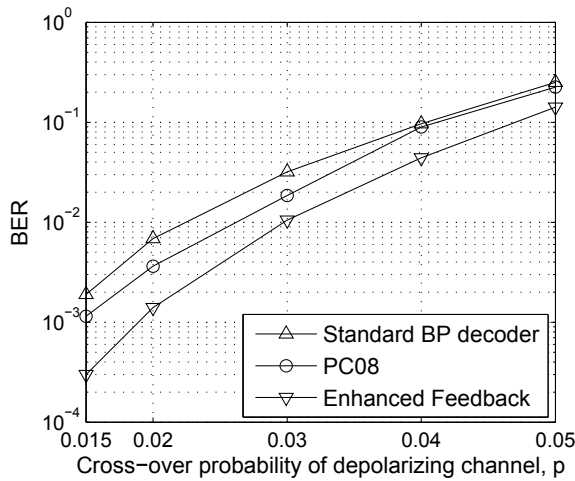
Fig. 4. Block error rate vs cross-over probability of depolarizing channel p for three different BP decoders when applied to Conventional. The maximum number of iterations is 90. The maximal number of iterations between each perturbation is 40. The strength of the random perturbation used here is $\delta = 0.1$. The maximal number of entries traversed by enhanced feedback decoder round down to one fifth of the code length, which equals 25 here.

B. Examples: EA Sparse Quantum Codes

EA sparse quantum codes can be constructed from arbitrary binary or quaternary sparse classical codes [12]. Here we present the decoding of three EA sparse quantum codes that are constructed in the same way as the construction of [[4, 1; 1]] discussed in Sec. IV. These three codes have different net rate (including positive, zero and negative net rates), different block lengths and different row weight distributions.

The first EA sparse quantum code we consider is [[128, 79; 49]], which is constructed from an irregular quaternary sparse classical code [128, 79] with girth $g \geq 6$. The classical code [128, 79] is designed by using the progressive-edge-growth (PEG) algorithm under the constraint that the degree distribution of bit nodes is [14]

$$\{2 : 33\%, 3 : 33\%, 4 : 22\%, 5 : 22\%\}. \tag{30}$$

As there are 49 pairs of anti-commuting generators in $\hat{H}_q$ according to the construction method of Eq. (25), then the EA formalism yields the EA sparse quantum code

$$[[n, 2k - n + c; c]] = [[128, 2 \times 79 - 128 + 49; 49]], \tag{31}$$

which can be constructed from the classical quaternary code $[n, k] = [128, 79]$ [12]. The code [[128, 79; 49]] has a positive net rate

$$\frac{k - c}{n} = \frac{79 - 49}{128}. \tag{32}$$

Here we refer to this code as "EA-1" and show the performance of the three decoders with respect to EA-1 over depolarizing channels. The performance, in terms of block error rate, is summarized in Fig. 5.

Our second EA sparse quantum code is [[816, 404; 404]], which is constructed from a binary regular sparse classical code [816, 408]. The classical [816, 408], which has a rate 0.5, row weight 6 and column weight 3, was constructed by MacKay [22]. As there are $c = 404$ pairs of anti-commuting
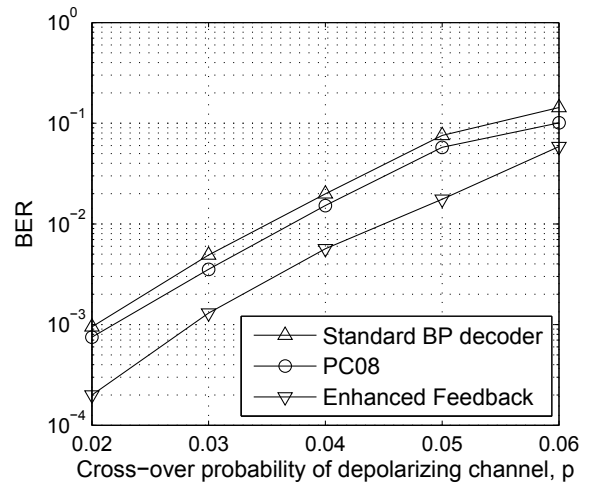

Fig. 5. Same as for Fig. 4 but replacing Conventional by EA-1.

generators and 8 commuting generators in $\hat{H}_q$, we obtain an EA sparse quantum code [[816, 404; 404]] according to the EA stabilizer formalism. Here we take this code as our second example of EA sparse quantum codes whose net rate is

$$\frac{k - c}{n} = \frac{404 - 404}{816} = 0, \tag{33}$$

and call it "EA-2". We show the performance of the three decoders when applied to EA-2 over depolarizing channels in Fig. 6 in terms of BER.[8]
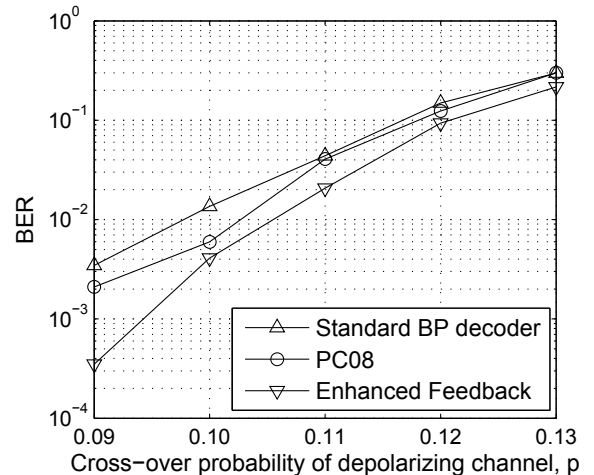

Fig. 6. Same as for Fig. 4 but replacing Conventional by EA-2 and changing the maximum number of entries traversed by the enhanced feedback decoder round down to one tenth of the code length, which equals 81 here.

The third EA sparse quantum code is [[1920, 638; 1278]], which is constructed from [1920, 640], a famous sparse classical code proposed as the international standard for cellular telephones. The [1920, 640] code, which has a rate 1/3 and row weight 4, was also constructed by MacKay [23]. Following the construction procedure mentioned in Sec. IV, the number of anti-commuting pairs in $\hat{H}_q$ is 1278; thus, we obtain

---

[8]Net rates for EA quantum codes can be negative or zero. See Appendix for more detail.

an EA sparse quantum code [[1920, 638; 1278]]. Here we take this code as our third example of EA sparse quantum codes, this time with a negative net rate

$$\frac{k - c}{n} = \frac{638 - 1278}{1920} = -\frac{1}{3}. \tag{34}$$

We name it "EA-3" and show the performance of the three BP decoders when applied to EA-3 over depolarizing channels in Fig. 7.
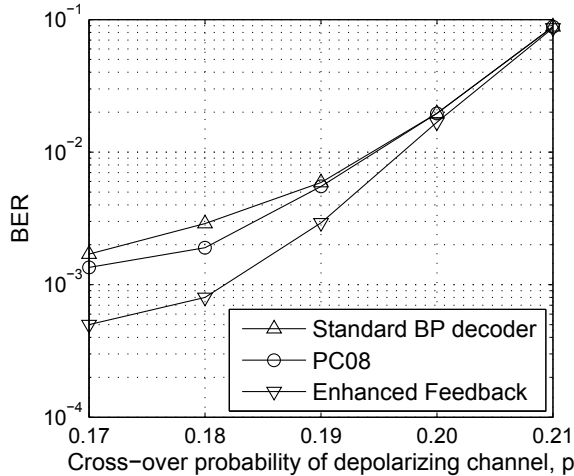

Fig. 7. Same as for Fig. 4 but using Conventional replaced by EA-3 and changing the maximal number of entries traversed by enhanced feedback decoder round down to one fortieth of the code length that is 43.

C. Time efficiency simulation

We evaluate and compare the time consumed by each decoder according to the average number of iterations

$$\text{ANoI} := \frac{n_t}{n_b}, \tag{35}$$

consumed by one codeword, with n_t the total number of iterations to finish decoding n_b blocks. In our simulation $n_b = 20000$. In Figs. 8 and 9 we show the time efficiency (complexity) comparison for the three decoders applied to Conventional, EA-1, EA-2 and EA-3. Evidently our algorithm has a smaller ANoI than PC08, which shows improved decoding efficiency when compared to PC08.

D. Discussion

From Figs. 4-9, it is evident that our strategy yields a significantly lower BER with a lower ANoI for both conventional sparse quantum codes and EA sparse quantum codes. As an example of the effectiveness of our new decoder, consider the case $p \approx 0.015$, Fig. 4 shows that the enhanced-feedback BP decoder yields a 6 dB gain over PC08 and an 8 dB gain over the standard BP decoder while reducing the ANoI from 3.1 for PC08 to 2.2 for our enhanced-feedback BP decoder as seen in Fig. 8.

For another point of view, in Fig. 5, we can see that to guarantee EA-1 having a decoding error below 10^{-3}, the standard BP decoder allows $p \approx 0.020$ and PC08 allows $p \approx 0.022$. This value is increased dramatically to $p \approx 0.029$
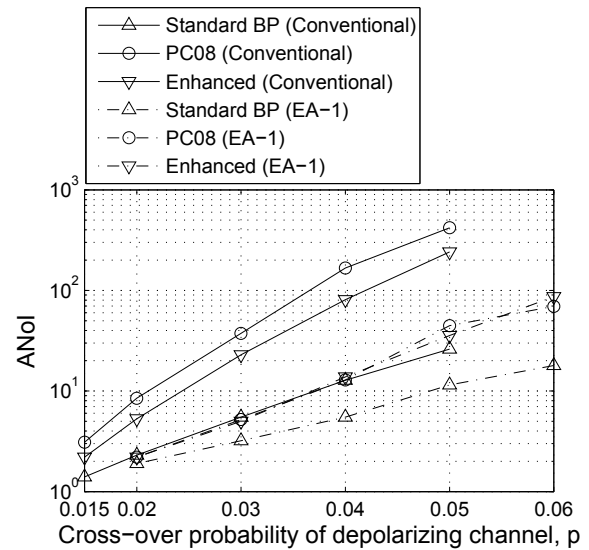

Fig. 8. Same as for Fig. 4 but replacing block error rate by average number of iterations and adding EA-1 as another example.
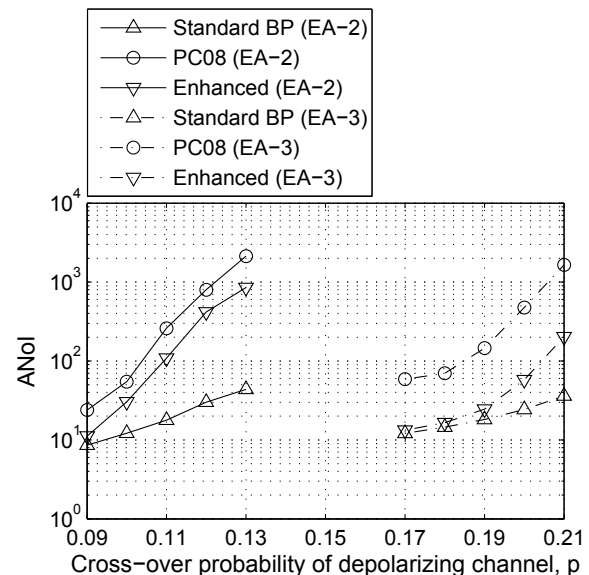

Fig. 9. Same as for Fig. 8 but replacing Conventional and EA-1 by EA-2 and EA-3 and changing the maximal number of entries traversed by enhanced feedback decoder from rounding down to one fifth of the code length to one tenth of the code length for EA-2 and to one fortieth of the code length for EA-3.

using our enhanced feedback BP decoder with a similar ANoI performance as PC08. As for the decoding of EA-2 (Fig. 6), when $p = 0.09$, the BER performance of PC08's method is 1.75 times better than that of the standard BP decoder with 2.78 times more ANoI, and the BER performance of our approach is approximately 10 times better than that of the standard BP decoder with only 1.3 times more ANoI.

Notably, interesting results appear in the decoding of EA-3. From Fig. 7 and 9 we see that PC08 could not significantly improve the standard BP decoder even with high ANoI, yet our approach does improve the performance of EA-3 significantly with almost the same ANoI as the standard BP decoder excepting the last two nodes.

Our algorithm is capable of turning the detectable errors into new outputs whose syndromes are identical with corresponding observed syndromes. We refer to these outputs as *valid* outputs can be classified into three cases: (1) $E_{out} = E$; (2) $E_{out} \neq E$ but $E_{out} \times E \in S$; (3) $E_{out} \times E \notin S$. The first two cases will yield correct outputs that can recover the sent quantum states successfully. However, it is hard to check whether $E_{out} \times E \in S$ which makes distinguishing cases (2) and (3) difficult. Therefore, we choose (1) as the success criterion for the decoding result in our numerical simulation.

Some detectable errors are turned into undetectable errors by our decoder. In order to show how often our algorithm results in an undetectable error, we classify all the results yielded by our algorithm (not just valid outputs) when the original BP protocol fails[9] into three cases: (1); cases (2) or (3); remain as detectable errors. In Fig. 10, we take Conventional as an example to depict the number of blocks that fall into each whereas the original BP protocol fails 50 times. It is evident
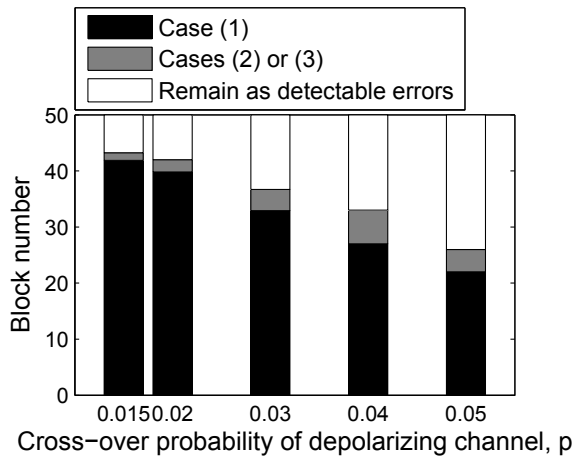

Fig. 10. Block numbers fall into the three cases mentioned in context vs cross-over probability of depolarizing channel p for our enhanced BP decoder when applied to Conventional while the original BP decoder fails 50 times. The maximum number of iterations is 90. The maximal number of iterations between each perturbation is 40. The maximal number of entries traversed by enhanced feedback decoder round down to one fifth of the code length.

to see from Fig. 10 that most of the detectable errors will be turned to correct output but not undetectable errors by using our enhanced feedback BP decoder.

VI. CONCLUSION

We have developed an enhanced feedback BP decoding algorithm whose feedback adjustment strategy is not based solely on the syndrome but also on the channel model and on the individual values of the entries of the frustrated checks. Our approach retains the capability of breaking the symmetric degeneracy while also feeding back extra useful information to the BP decoder. Therefore, our feedback adjustment strategy yields a better error correcting capacity with relative less iterations compared to the proposed decoding algorithms for sparse quantum codes. We have considered three cases: the

---

[9]The 'fails' means that the syndrome of the output of the original BP decoder is not identical with the observed syndrome. In other words, a detected errors yielded by the original BP decoder.

standard BP decoder adapted from classical decoding to decode quantum codes, the superior BP decoder with Poulin and Chung's random perturbation [10], and the BP decoder with our new feedback adjustment strategy introduced here.

We used the $GF(4)$ representation of quantum codes to construct our feedback-based algorithm and exploit not just the syndrome but all the measurement resulting from stabilizer measurements. Then we used the block error rate (BER) and average number of iterations (ANoI) to demonstrate a dramatic better error correcting capacity improvement with relative less iterations. This result was achieved using new feedback adjustment strategy vs the two alternatives: standard BP decoder and the BP decoder with random perturbation.

APPENDIX

As shown in Section V, the net rate for EA-2 and EA-3 are 0 and $-1/3$ respectively. As pointed out by Brun, Devetak and Hsieh, "in general, net rates for EA quantum codes can be positive, negative, or zero. The zero rate does not mean that no qubits are transmitted by this code! Rather, it implies that a number of bits of entanglement is needed that is equal to the number of bits transmitted." Compared to quantum codes with high net rates, EA quantum codes with zero or negative net rates employ many more physical qubits including a great number of bits of entanglement that being assumed to be error-free,[10] thus these codes can tolerate stronger noise. Therefore, it is not surprising that EA-2 and EA-3 greatly increase p the cross-over probability of depolarizing channel when compared to quantum codes with similar code length and higher net rates.

For comparison, based on "Construction B" [9] (same as the construction of Conventional), we construct a quantum code with a similar code length as EA-2 but having a relative higher net rate. We name this example as EX which has a code length of 800 and a net rate $1/2$. In Fig. 11, we see that EX has comparable BER performance to other examples presented in existing literatures which have similar parameters as EX but significantly worse than EA-2.[11]

REFERENCES

[1] R. G. Gallager, "Low density parity-check codes," IRE Trans. Inform. Theory, vol. IT-8, pp. 21-28, Jan. 1962.

---

[10]The part of ebits held by the receiver is assumed to be not subject to errors according to usual practices.

[11]Please refer to [10] and [28]. We can see that the BER performance of EX is similar with the example presented in [10] and a little worse than the example presented in [28] by using standard BP decoder.
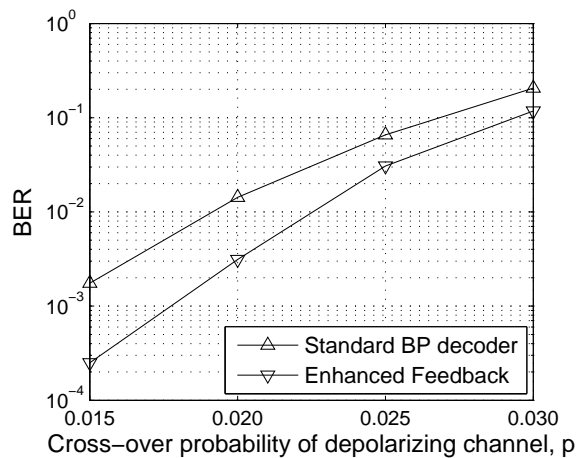
Fig. 11. Block error probability vs cross-over probability of depolarizing channel p for the standard BP decoder and for our algorithm when applied to EX. The maximum number of iterations is 90. Both the number of iterations between each perturbation and the maximal entries traversed by our decoder are 40.

[2] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399-431, March 1999.

[3] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. R2493-R2496, 1995.

[4] A. M. Steane, "Error-correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.

[5] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. thesis, California Institute of Technology, Pasadena, CA 1997; D. Gottesman. (2007) Lecture notes: Quantum error correction. [Online]. Available: http://www.perimeterinstitute.ca/personal/dgottesman/QECC2007

[6] C. H. Bennett, D. P. Divincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824-3851, 1996.

[7] E. Knill and R. Laflamme, "A theory of quantum error-correcting codes," *Phys. Rev. A.*, vol. 55, pp. 900-911, 1997.

[8] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369-1387, July 1998.

[9] D. J. C. MacKay, G. J. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2315-2330, Oct. 2004.

[10] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," *Quantum Inform. Comput.*, vol. 8, pp. 987-1000, 2008.

[11] D. Poulin, J.-P Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2776-2798, June 2009.

[12] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, pp. 436-439, October 2006.

[13] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasi-cyclic low-density parity-check codes," *Phys. Rev. A*, vol. 79, 032340, 2009.

[14] Y.-J. Wang, B.-M. Bai, W.-B. Zhao, and X.-M. Wang, "Entanglement-assisted quantum error-correcting codes constructed from irregular repeat accumulate codes" *Int. J. Quantum Inf.*, vol. 7, no. 7, pp. 1373-1389, 2009.

[15] J. Preskill, *Lecture Notes for Physics 219: Quantum Computation (2001)*. [online]. Available: www.theory.caltech.edu/people/preskill/ph219.

[16] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms.* New Jersey, U.S.A.: John Wiley & Sons, Inc., 2005.

[17] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: Construction and performances under iterative decoding," in *Proc. Int. Symp. Inf. Theory*, Nice, France, June 2007, pp. 811-815.

[18] M. S. Leifer and D. Poulin, "Quantum graphical models and belief propagation," *Annals of Physics*, vol. 323. pp. 1899-1946, 2008.

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

[20] A. Shokrollahi, "LDPC codes: An introduction," Tech. Rep. Fremont, CA: Digital Fountain, Inc., Apr. 2, 2003.

[21] D. J. C. MacKay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399-431, Mar. 1999.

[22] This regular LDPC check matrix is available at: http://www.inference.phy.cam.ac.uk/mackay/codes/EN/C/816.3.174.

[23] This regular LDPC check matrix is available at: http://www.inference.phy.cam.ac.uk/mackay/codes/EN/C/1920.1280.3.303.gz.

[24] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, pp. 198-201, 1996.

[25] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 498-519, Feb. 2001.

[26] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2711-2736, Nov. 2001.

[27] M. Hagiwara and H, Imai, "Quantum quasi-cycli ldpc codes" in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, June 2007, pp. 806-810.

[28] M.-H Hsieh, W.-T Yen, and L-Y Hsu, "High performance entanglement-assisted quantum LDPC codes need little entanglement," *IEEE Trans. Inform. Theory*, vol. 57, no. 3, pp. 1761-1769, Mar. 2011.