Robust Quantum Error Syndrome Extraction by Classical Coding

Alexei Ashikhmin
Bell Laboratories
Alcatel-Lucent, 600 Mountain Ave
Murray Hill, NJ 07974
aea@reseach.bell-labs.com

Ching-Yi Lai
Centre for Quantum Computation
and Intelligent Systems
University of Technology Sydney
New South Wales, Australia 2007
ChingYi.Lai@uts.edu.au

Todd A. Brun
Communication Sciences Institute
University of Southern California
Los Angeles, California, USA
tbrun@usc.edu

***Abstract*—An important issue in the implementation of a quantum computer is to protect quantum information from decoherence. In fault-tolerant quantum computation, the circuits used to measure the error syndromes are themselves faulty; to minimize the effect of syndrome measurement errors, the syndromes are measured repeatedly. This paper introduces a scheme based on classical codes to make this process more robust and/or reduce the needed resources and measurement time. We analyze particular implementations based on low-density generator matrix (LDGM) codes using EXIT functions.**

I. Introduction

In a quantum error-correcting code, quantum information is stored in the joint $+1$ eigenspace of a set of Pauli operators, called stabilizers [1]. To perform quantum error correction, either Shor's or Steane's syndrome extraction method is commonly used [2], [3], [4] to gain information about the errors. That information is the error syndrome.

Realistically, the quantum gates used to perform quantum error correction are themselves faulty. The measurement outcomes for the error syndrome can be wrong due to faulty measurements or newly introduced errors from faulty gates. Usually, the error syndrome is determined by repeated syndrome measurements and a majority vote.

In this article, we are interested in eliminating the effect of faulty syndrome measurement. In the case of Shor's syndrome extraction, repeatedly measuring each syndrome bit is similar to using a classical repetition code. We generalize this approach by introducing the idea of *syndrome measurement (SM) codes* based on classical linear block codes. We analyze the performance of a particular scheme based on SM LDGM codes, designed using EXIT functions [6], [7], [8]. For Steane's syndrome extraction, SM codes cannot be applied in the same way, but we still can use classical coding theory to save resources.

II. Preliminaries

Let $\mathcal{P}_n = \{eM_1 \otimes \cdots \otimes M_n : M_j \in \{I, X, Y, Z\}, e \in \{\pm 1, \pm i\}\}$ be the n-fold Pauli group. Every element in $\mathcal{P}_n$ has eigenvalues ± 1 or $\pm i$. Any element $g = eM_1 \otimes \cdots \otimes M_n \in \mathcal{P}_n$ can be represented by two binary n-tuples $(\mathbf{u}, \mathbf{v})$ (up to a phase) where $(u_j, v_j) = (0,0)$, $(1,0)$, $(0,1)$, or $(1,1)$ if M_j is I, X, Z, or Y, respectively. We write the two binary n-tuples $(\mathbf{u}, \mathbf{v})$ corresponding to g as a binary symplectic vector $\mathbf{g} = (\mathbf{u}, \mathbf{v})$. The weight $\mathrm{wt}(\mathbf{g})$ of $\mathbf{g}$ is the number of j so that $(u_j, v_j) \neq (0,0)$. In this paper we will work almost exclusively in terms of the vectors $\mathbf{g}$ rather than the operators g. Without loss of generality, g can be recovered from $\mathbf{g}$ with phase $+1$.

Suppose $\mathcal{S}$ is an Abelian subgroup of the n-fold Pauli group $\mathcal{P}_n$ that does not include $-I$, with a set of $n-k$ independent generators $\{g_1, g_2, \cdots, g_{n-k}\}$. An $[[n,k,d]]$ quantum stabilizer code corresponding to the stabilizer group $\mathcal{S}$ is defined to be the 2^k-dimensional subspace of the n-qubit state space fixed by $\mathcal{S}$, so that any errors of weight less than d can be detected. For an error operator $E \in \mathcal{P}_n$, the error syndrome is a binary $(n-k)$-tuple $\mathbf{s} = (s_1 \cdots s_{n-k})$, where $s_j = 1$ if E anticommutes with g_j, and $s_j = 0$, otherwise.

In Shor's syndrome extraction, each stabilizer generator is measured in sequence. If we are measuring a generator g_j of weight w, a w-qubit cat state is used to obtain the syndrome bit $s_j = m_1 + \cdots + m_w$, where m_i is the binary measurement outcome on the i-th ancilla qubit. For CSS codes, Steane proposed another scheme for syndrome measurement, which uses only two n-qubit ancilla states $H^{\otimes n}|0\rangle_E$, where $|0\rangle_E$ is the encoded state of $|0\rangle$ and H is the Hadamard gate. However, preparing this ancilla state can be expensive when n is large.

Let p_m be the error rate of the measurement in the Z basis. That is, the measurement outcome is flipped from 0 to 1 or 1 to 0 with probability p_m. Assume all the other quantum gates (such as H, $CNOT$) have depolarizing errors and let p_g be the highest error rate among all quantum gates. For some technologies (e.g., quantum trapped ions) it is reasonable to assume that $p_m >> p_g$. Hence, in this work, as the first step of developing techniques for robust syndrome measurements, we assume $p_g = 0$. Thus the quantum state does not change during the syndrome measurement.

III. Encoded Quantum Syndrome Measurement

The standard approach to reduce the probability of syndrome measurement error is repeated syndrome measurement. That is, we repeat the syndrome measurement several times and take a majority vote. This is the same idea as in classical

978-1-4799-5186-4/14/$31.00 ©2014 IEEE

repetition codes. We propose to generalize this approach by using more powerful linear classical codes.

Suppose we are using an $[[n,k]]$ stabilizer code defined by a stabilizer group $\mathcal{S}$ with generators $g_1, g_2, \cdots, g_{n-k}$ and corresponding vectors $\mathbf{g}_1, \ldots, \mathbf{g}_{n-k}$. Let $\mathbf{s} = (s_1, \ldots, s_{n-k})$ be the correct syndrome measurement outcome. Let $\hat{\mathbf{s}} = (\hat{s}_1, \ldots, \hat{s}_{n-k})$ be the syndrome bits output by Shor's syndrome extraction. Then

$$\begin{aligned} p_{err}(\mathbf{g}_j) &= \Pr(\text{error measurement of } g_j) = \Pr(\widehat{s}_j \neq s_j) \\ &= \sum_{i:i \text{ odd}} \binom{\text{wt}(\mathbf{g}_j)}{i} p_m^i (1-p_m)^{\text{wt}(\mathbf{g}_j)-i} \\ &= \frac{1-(1-2p_m)^{\text{wt}(\mathbf{g}_j)}}{2}. \end{aligned} \quad (1)$$

Define $r = n-k$, and let C be an $[m,r]$ linear binary code with a generator matrix in the systematic form

$$G_C = [I_r \quad A], \quad (2)$$

where $A = [a_{j,l}]$ is an $r \times (m-r)$ binary matrix. We define a new set of $m-r$ stabilizer vectors $\mathbf{f}_j$ by

$$\mathbf{f}_j = a_{1,j}\mathbf{g}_1 + \ldots + a_{r,j}\mathbf{g}_r, \text{ for } j = 1, \cdots, m-r. \quad (3)$$

We can measure the stabilizers $f_j \in \mathcal{S}$ corresponding to $\mathbf{f}_j$ without disturbing the quantum state. For this reason, we call C *the syndrome measurement code*. Denote by s_j and z_j the results of correct measurement of g_j and f_j, respectively. It is not difficult to see that

$$\mathbf{x} = (s_1, \ldots, s_r, z_1, \ldots, z_{m-r}) \quad (4)$$

is a valid codeword of C. After the (imperfect) measurement of $g_1, \ldots, g_r$ and $f_1, \ldots, f_{m-r}$, we obtain a vector

$$\widehat{\mathbf{x}} = (\widehat{s}_1, \ldots, \widehat{s}_r, \widehat{z}_1, \ldots, \widehat{z}_{m-r}). \quad (5)$$

Applying a decoding algorithm of C to $\widehat{\mathbf{x}}$, we obtain bits $\tilde{s}_1, \ldots, \tilde{s}_r$. For a given C and its decoding algorithm, we define

$$P_{se} = \Pr((s_1, \ldots, s_r) \neq (\tilde{s}_1, \ldots, \tilde{s}_r)) \quad (6)$$

and

$$P_{SBER} = \frac{1}{r}\sum_{j=1}^{r} \Pr(\tilde{s}_j \neq s_j). \quad (7)$$

Remark We can also use a nonsystematic generator matrix G in (2). All our results are easily extendable for this nonsystematic case. Usually, however, $\text{wt}(\mathbf{g}_j) < \text{wt}(\mathbf{f}_i)$ and so $p_{err}(\mathbf{g}_j) < p_{err}(\mathbf{f}_i)$. Thus, the systematic form of G allows us to minimize the error probability for the first r measurements.

The t-fold repeated syndrome measurement can be considered as a particular case of an encoded syndrome measurement. It corresponds to the SM code with generator matrix

$$G = [\underbrace{I_r \cdots I_r}_{t \text{ times}}].$$

Choosing a good SM code is often not equivalent to finding a good $[m,r]$ linear code in the usual sense. This is because for a typical $[m,r]$ code with a large minimum distance, the matrix A in (2) will have "heavy" columns. This may result in $\text{wt}(\mathbf{f}_j) >> \text{wt}(\mathbf{g}_l)$ and therefore $p_{err}(\mathbf{f}_j) >> p_{err}(\mathbf{g}_i)$, which, in turn, will lead to large P_{se} and P_{SBER}.

Below we present several families of high rate quantum codes with the property that all their stabilizers $g \in \mathcal{S}$ have the same or almost the same weight and therefore any good linear codes can be used for robust syndrome measurement.

Let S_a be a generator matrix of the $[2^a-1, a, 2^{a-1}]$ simplex code. Let $\mathcal{S}_a$ be the $[[2^a-1, 2^a-1-2a, 3]]$ CSS code defined by the generators $\begin{bmatrix} S_a & 0 \\ 0 & S_a \end{bmatrix}$. Any linear combination of the first (second) a generators is a vector of weight 2^{a-1}. Thus we can use any good $[n,a]$ linear code for syndrome measurement of the first (second) a syndrome bits. For example, let us consider the code $\mathcal{S}_3$, which is the $[[7,1,3]]$ Steane code. Let us use as an SM code the $[15,3]$ code C defined by:

$$G_C = \begin{bmatrix} 100001111111000 \\ 010010011110110 \\ 001101100110111 \end{bmatrix}.$$

The code C requires 15 measurements, which is the same as for the 5-fold repeated measurements of three bits. The corresponding probabilities P_{se} are shown in Fig.1. One can see that the code C has significantly lower P_{se}.

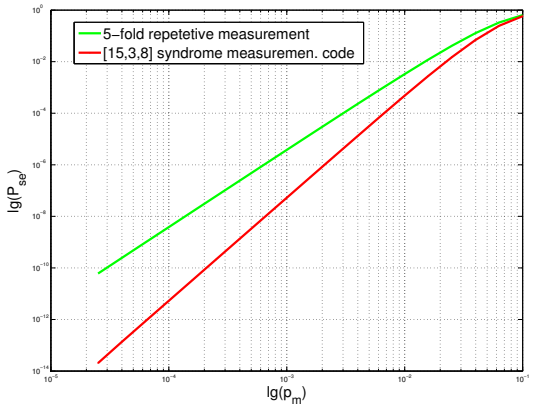

Fig. 1. The probabilities P_{se} for the $[15,3]$ code C and 5-fold Repeated Measurement of the syndrome of the $[[7,1,3]]$ Steane code

Another important family is the $[[n, n-2a, 3]], n = (4^a - 1)/3$, quantum Hamming codes $\mathcal{H}_a$, [5, V]. It is not difficult to prove that all stabilizers of $\mathcal{H}_a$ have weight 4^{a-1}.

In [5, Thm 11] a family of $[[n, n-a-2, 3]]$ codes with $n = \sum_{i=1}^{(a-1)/2} 2^{2i+1}$ is defined for odd a. The stabilizers of these codes can have only weights $2^a - 2$ and 2^a.

Finally, a Gottesman $[[2^a, 2^a - a - 2, 3]]$ code, see [5, Thm 10], has $4(2^a - 1)$ stabilizers of weights $3 \cdot 2^{a-2}$ and three stabilizers of weight 2^a. Hence here it is desirable to use an SM code that does not produce $\mathbf{f}_j$ of weight 2^a.

IV. Syndrome Measurement LDGM Codes

In this section we assume that r is relatively large and that the weights $\text{wt}(\mathbf{f}_i)$ are typically larger than the weights $\text{wt}(\mathbf{g}_j)$. We present a construction of LDGM SM codes that takes into account the weights $\text{wt}(\mathbf{g}_j)$ and $\text{wt}(\mathbf{f}_i)$.

Long low density parity check (LDPC) codes are among the best currently known classical codes. Since we assumed large r it seems natural to try to construct a SM code C as an $[m, r]$ LDPC code. This turns out to be a difficult problem, however. If C is an LDPC code, then its parity check matrix H_C is sparse, but its generator matrix most likely will have "heavy" columns that results in large $p_{err}(\mathbf{f}_j)$. For a typical LDPC code C, the probabilities $p_{err}(\mathbf{f}_j)$ are so large that syndrome measurement with such C has very bad performance. For this reason, we consider LDGM codes, i.e. codes with $G = [I_r \ A]$ for some sparse A.

A parity check matrix of an LDGM code C can be written in the form $H_C = [A^T I_{m-r}]$. Thus, it is convenient to represent C with the help of the Tanner graph. For the matrix

$$H_C = \begin{bmatrix} 1010100 \\ 0110010 \\ 1001001 \end{bmatrix}, \tag{8}$$

the corresponding graph is shown in Fig. 2.

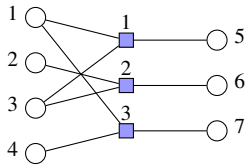

Fig. 2. The Tanner graph for the code defined by (8).

For our purposes it is convenient to work only with the left part of the graph, which we call the *reduced graph*. The reduced graph in Fig. 2 is obtained by omitting variable nodes $5, 6, 7$. The variable nodes of the reduced graph correspond to stabilizers g_l and the check nodes correspond to f_l. Let us combine all vectors $\mathbf{g}_l$ ($\mathbf{f}_l$) into sets $\mathcal{G}_1, \ldots, \mathcal{G}_a$ ($\mathcal{F}_1, \ldots, \mathcal{F}_b$) so that for any $\mathbf{g} \in \mathcal{G}_i$ ($\mathbf{f} \in \mathcal{F}_i$) we have $\mathrm{wt}(\mathbf{g}) = w_i^v$ ($\mathrm{wt}(\mathbf{f}) = w_i^c$). Hence $p_{err}(\mathbf{g}) = p_i^v$ ($p_{err}(\mathbf{f}) = p_i^c$), where p_i^v and p_i^c are computed according to (1). Let us further denote by $\lambda_{i,j}$ ($\rho_{i,j}$) the fraction of edges in the reduced graph connected to the variable (check) nodes of degree j and corresponding to $\mathbf{g} \in \mathcal{G}_i$ ($\mathbf{f} \in \mathcal{F}_i$). It is not difficult to show that the code rate of C is equal to or greater than

$$R = 1 - \frac{\sum_{i,j} \rho_{i,j}/j}{\sum_{i,j} \rho_{i,j}/j + \sum_{i,j} \lambda_{i,j}/j}. \tag{9}$$

In the standard classical scenario all p_i^v and p_i^c are equal to the same channel error probability. Hence $a = b = 1$ and we can use $\lambda_j = \lambda_{1,j}$ and $\rho_j = \rho_{1,j}$. Good LDPC codes can be constructed as random codes with optimized distributions λ_j and ρ_j. The usual methods for optimization of λ_j and ρ_j are not directly applicable for our purposes. First, we need LDGM rather than LDPC codes. Second, in the classical scenario the degree distributions of a code have no effect on the bit error probability of the vector $\widehat{\mathbf{x}} = (\widehat{s}_1, \ldots, \widehat{s}_r, \widehat{z}_1, \ldots, \widehat{z}_{m-r})$. In the quantum case, $\Pr(\widehat{z}_j \neq z_j)$ heavily depends on the matrix A, and therefore on $\lambda_{i,j}$ and $\rho_{i,j}$.

In what follows we generalize the EXIT function method from [6], [7], [8] to design SM LDGM codes. The EXIT functions of an LDPC code allows one to predict the convergence behavior of belief propagation (BP) decoding. An LDPC code has the EXIT functions $I_{E,vnd}(x)$ and $I_{E,cnd}(x)$, for variable and check nodes, respectively. These functions depend on the distributions λ_j and ρ_j, and on the channel error probability p. For a given p, λ_j, and ρ_j, if

$$I_{E,vnd}(x) > I_{E,cnd}^{-1}(x), x \in [0, 1), \tag{10}$$

then BP decoding of a random and sufficiently long LDPC code with these λ_j and ρ_j successfully converges to a correct code vector. Another important observation is that the closer $I_{E,vnd}(x)$ is to $I_{E,cnd}^{-1}(x), x \in [0, 1)$ (as in Fig. 4), the larger the code rate. In [6] it is proven for the binary erasure channel that if $I_{E,vnd}(x) = I_{E,cnd}^{-1}(x), x \in [0, 1)$, then the corresponding LDPC code achieves the Shannon capacity.

In what follows, $H(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

Assumption We assume that the messages passed between variable and check nodes in BP decoding (but not the measurement results of g_j and f_j) have Gaussian distributions. This assumption, while not exact, is a good approximation and is typically used for LDPC codes.

Under the above assumption we have

Theorem 1: $I_{E,vnd}(x) = \sum_{i,j} \lambda_{i,j} I_{E,vnd}(x, j, p_i^v)$, where

$$\begin{aligned} &I_{E,vnd}(x, j, p) \\ =&1 - \frac{1-p}{\sqrt{2\pi u}} \int_{-\infty}^{\infty} e^{-(z+u/2)^2/2u} \log_2(1 + \frac{p}{1-p} e^z) dz \\ &- \frac{p}{\sqrt{2\pi u}} \int_{-\infty}^{\infty} e^{-(z+u/2)^2/2u} \log_2(1 + \frac{1-p}{p} e^z) dz, \end{aligned}$$

where $u = (j-1)u_0$, and where u_0 is chosen such that

$$x = 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi u_0}} e^{-(z-u_0/2)^2/2u_0} \log_2(1 + e^{-z}) dz.$$

Theorem 2: $I_{E,cnd}(x) = \sum_{i,j} \rho_{i,j} I_{E,cnd}(x, j, p_i^c)$, where

$$I_{E,cnd}(x, j, p) = \frac{1}{\ln(2)} \sum_{i=1}^{\infty} \frac{1}{2i(2i-1)} \Phi_i (u/2)^{j-1} (1-2p)^{2i},$$

$$\Phi_i(y) = \frac{1}{\sqrt{4\pi y}} \int_{-1}^{1} \frac{2z^{2i}}{(1-z^2)} \exp(-\frac{(\ln\left(\frac{1+z}{1-z}\right) - y)^2}{4y}) dz,$$

and u is such that

$$x = 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi u}} e^{-(z-u/2)^2/2u} \log_2(1 + e^{-z}) dz.$$

Unfortunately, in the case of LDGM codes we cannot satisfy the conditions (10). It is not difficult to prove that for any choice of $\lambda_{i,j}$ and $\rho_{i,j}$ there exist $\hat{x} \in [0, 1 - H(\min_j\{p_{err}(\mathbf{f}_j)\}))$ such that $I_{E,vnd}(\hat{x}) = I_{E,cnd}^{-1}(\hat{x})$. For this reason we replace (10) by

$$I_{E,vnd}(x) \geqslant I_{E,cnd}^{-1}(x), x \in [0, x^*] \text{ for some } x^* < \hat{x}. \tag{11}$$

BP decoding can approach $P_{SBER} = 0$ only if $I_{E,vnd}(x^*) = 1$, but $I_{E,vnd}(x) = 1$ only at $x = 1$. Since $x^* < 1$ we conclude that even infinitely long SM LDGM codes have $P_{SBER} > 0$. Achieving small, but nonzero, P_{SBER} is often good enough

since some decoders of stabilizer codes are robust to a small number of syndrome errors, or possibly remaining errors can be removed by an outer code (we omit details). The larger $I_{E,vnd}(x^*)$, the smaller P_{SBER}, but the more difficult to design an LDGM code with high rate (again we omit details).

Let us denote $\gamma_i = |\mathcal{G}_i|/r$, choose some x^*, and assume, for the moment, that wt $(\mathbf{f}_j)$ are fixed. Then we can formulate the following optimization problem to maximize the code rate R defined in (9):

$$\text{maximize } \sum_{i,j} \lambda_{i,j}/j \text{ subject to the constraints:}$$

$\frac{\sum_j \lambda_{i',j}/j}{\sum_{i,j} \lambda_{i,j}/j} = \gamma_{i'}$, for $i' = 1, \cdots, a$, $\sum_{i,j} \lambda_{i,j} = 1$, and $I_{E,vnd}(x) \geqslant I^{-1}_{E,cnd}(x), x \in [0, x^*)$.

However, weights wt $(\mathbf{f}_l)$, and further $I^{-1}_{E,cnd}(x)$, depend on $\lambda_{i,j}$s. The situation becomes simpler if wt$(\mathbf{g}_j) = w$, $j = 1, \cdots, r$, as, for example, in regular quantum LDPC codes. Let us further assume that we design an LDGM code so that all rows of A^T have the same weight d_c. Then wt$(\mathbf{f}_j) \leqslant d_c w$. This upper bound is equivalent to $\rho_{1,d_c} = 1, w_1^c = d_c w$. Using these parameters in Theorem 2 we obtain an upper bound (the worst case) on $I^{-1}_{E,cnd}(x)$, which can be used in the above optimization problem. Computer simulations applied to regular quantum LDPC codes show that typically wt$(\mathbf{f}_j) = d_c w - 2$ or $d_c w$. Hence our upper bound on $I^{-1}_{E,cnd}(x)$ is quite tight and can be used for designing efficient SM LDGM codes.

With the above settings we have $a = b = 1$. Thus we can use $\lambda_j, \rho_{d_c}, p^v, p^c$ instead of $\lambda_{1,j}, \rho_{1,d_c}, p_1^v, p_1^c$ and the optimization problem becomes a linear programming problem.

Example 1: Let us consider a regular quantum LDPC code with wt $(\mathbf{g}_j) = 10$ and let $p_m = 10^{-3}$. Let us choose $d_c = 12$. Then wt $(\mathbf{f}_j) \leqslant 120$. Using this upper bound, we find p^v and p^c. By solving the linear programming problem, we get $\lambda_2 = 0.0763, \lambda_7 = 0.9237$. Hence $R = 0.6712$. The EXIT functions of a random SM LDGM code with these λ_2, λ_7 are shown in Fig. 3. We also plot the evolution of the mutual information during BP decoding, obtained by computer simulation. One can see that the EXIT function predicts the behavior of the mutual information relatively accurate.

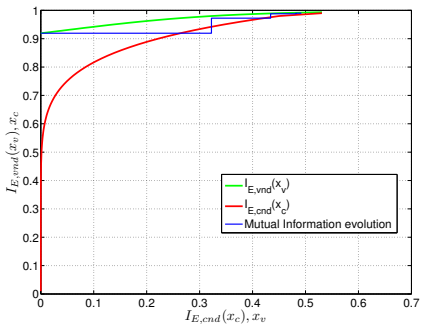

Fig. 3. The evolution of the mutual information during the BP decoding.

V. Punctured LDGM SM codes

In Example 1, despite of the optimized λ_j, the EXIT functions are not well matched. Therefore, potentially, R can be increased, or equivalently, the number of measurements can be decreased. Usually, for better matching of the EXIT functions we take large d_c. In our case, however, this will result in very heavy $\mathbf{f}_j$, which is very undesirable. Below we propose puncturing to get better matched EXIT functions.

The idea is to drop measurements of certain g_j. An LDGM code and its reduced graph would not change because of that, but the corresponding variable nodes, which we call *punctured* nodes, will have uncertainty $1/2$. Let $\hat{r}$ be the number of punctured nodes, and $\hat{\lambda}_i$ be the fraction of edges connected to punctured variable nodes of degree i. The number of measurements needed is $m - \hat{r}$, and hence we define $R_{pun} = r/(m - \hat{r})$. Using the above definitions, assuming $\rho_{d_c} = 1$, we get

$$R_{pun} = 1 - \frac{1 - d_c \sum_j \hat{\lambda}_j/j}{1 + d_c \sum_j \lambda_j/j}. \tag{12}$$

The EXIT function of variable nodes will have the form

$$I_{E,vnd}(x) = \sum_j \lambda_j I_{E,vnd}(x, j, p^v) + \sum_j \hat{\lambda}_j I_{E,vnd}(x, j, 1/2).$$

To find good degree distributions λ_j and $\hat{\lambda}_j$, we use the following algorithm, where Δ is a small real number.

1) For $s = 0 : \Delta : 1$ solve the optimization problem

$$\text{maximize } \sum_j \lambda_j/j \text{ with the constraints:}$$
$$\sum_j \hat{\lambda}_j = s, \quad \sum_j \lambda_j = 1 - s,$$
$$I_{E,vnd}(x) \geqslant I^{-1}_{E,cnd}(x), x \in [0, x^*).$$

2) Among the obtained solutions, take the one that maximizes R_{pun} in (12).

Example 2: We consider an example with the same parameters as in Example 1. The optimized values are $\lambda_6 = 0.608$, $\lambda_7 = 0.102$, $\hat{\lambda}_9 = 0.274$, $\hat{\lambda}_{10} = 0.016$. The EXIT functions are shown in Fig. 4. We can see that they are better matched compared to Example 2. Thus, according to (12), we get $R_{pun} = 0.7426$. This means that the total number of measurements is reduced by about 10%. At the same time, we still keep the same $p_m = 10^{-3}$. Let $r = 19190$. We designed a random $[30000, 19190]$ LDGM code with these λ_j and $\hat{\lambda}_j$. The total number of needed measurements is 25844. In Fig. 5 we plot P_{SBER} for this code and for the repeated syndrome measurement approach with the same total number of measurements. One can see that the punctured SM LDGM code provides significantly lower P_{SBER}.

VI. Using Fewer Ancillas in Syndrome Measurement for Steane Syndrome Extraction

In the previous sections we measured encoded stabilizer generators to obtain robust syndrome measurement with Shor's syndrome extraction. However, SM codes cannot be applied to Steane's syndrome extraction. In this section, we develop another idea from classical coding theory. Since the ancilla states $H^{\otimes n}|0\rangle_E$ are an expensive resource, we would like to

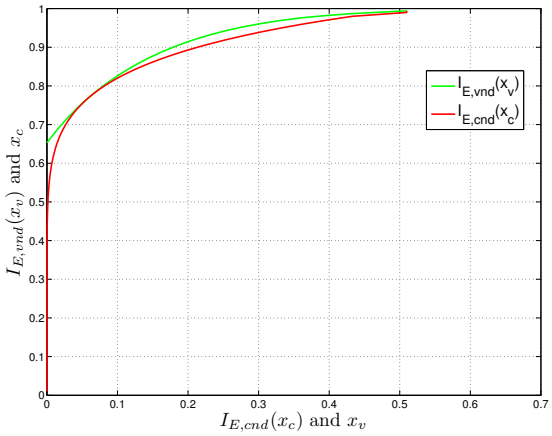

Fig. 4. The EXIT functions for punctured SM LDGM code

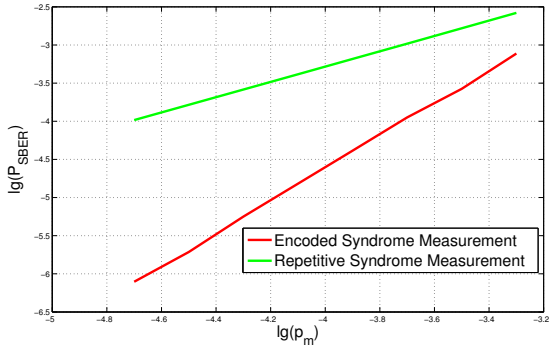

Fig. 5. Simulation Results of the punctured SM LDGM code.

share them during syndrome measurement as long as errors do not accumulate seriously. Suppose we have m quantum code blocks. We wish to determine the m error syndromes for bit-flip errors using only q $(< m)$ ancilla states $H^{\otimes n}|0\rangle_E$ (and similarly for phase-flip errors).

Let $u_1, \cdots, u_m$ be m unknowns in a field $\mathcal{F}$. Consider the linear system $v_i = \sum_{j=1}^{m} a_{i,j} u_j$ for $i = 1, \cdots, q$ and $a_{i,j} \in \mathcal{F}$. It is known that given $v_1, \cdots, v_q$, we cannot uniquely recover $u_1, \cdots, u_m$. However, the scenario is different if the unknowns $u_1, \cdots, u_m$ are binary vectors of length N.

Suppose u_i for $i = 1, \cdots, m$ are random vectors in $\mathbb{Z}_2^N$. Assume the bits of u_i are identically and independently distributed, and let p be the probability that a bit is 1. It is possible to recover the vectors $u_1, \cdots, u_m$, given $v_i = \sum_{j=1}^{m} a_{i,j} u_j$ for $i = 1, \cdots, q$ and a "proper" choice of $a_{i,j} \in \mathbb{Z}_2$ with a certain probability of success when p is small.

Suppose G is the $(m-q) \times q$ generator matrix of a $[q, m-q, d]$ linear binary block code. We choose $a_{i,j}$ as follows:

$$\left[v_1 \cdots v_q\right] = \left[u_{q+1} \cdots u_m\right] G + \left[u_1 \cdots u_q\right]. \qquad (13)$$

Viewed as a communication system, $[v_1 \cdots v_q]$ is the received vector, $[u_1 \cdots u_q]$ is the noise vector, and $[u_{q+1} \cdots u_m]$ is the information vector. We use a decoder to identify the noise vector and then recover the information vector. If p is small, we can successfully decode $u_1, \cdots, u_m$.

Note that the u_i's, and v_j's are binary vectors of length N, and that we decode each bit separately. If $N = 1$, it reduces

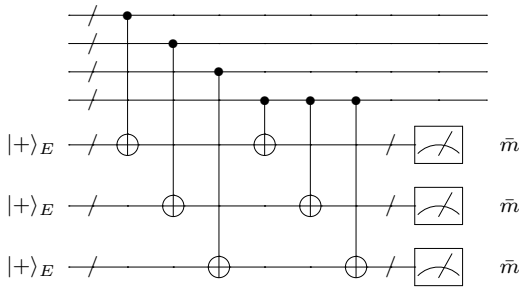

Fig. 6. The circuit for syndrome measurement of four data blocks with three ancilla blocks by a classical $[3, 1, 3]$ repetition code.

to the case of a standard error-correcting code. Therefore, we repeat the decoding procedure N times.

Example 3: Assume we have unknowns $u_1, \cdots, u_6 \in \mathbb{Z}_2^3$. Consider the generator matrix $G = [11111]$ of a $[5, 1, 5]$ repetition code. Let $v_1 = u_1 + u_6$, $v_2 = u_2 + u_6$, $v_3 = u_3 + u_6$, $v_4 = u_4 + u_6$, and $v_5 = u_2 + u_6$. By (13),

$$\begin{aligned} &\left[v_1 \quad v_2 \quad v_3 \quad v_4 \quad v_5\right] \\ &= \left[u_1 + u_6 \quad u_2 + u_6 \quad u_3 + u_6 \quad u_4 + u_6 \quad u_5 + u_6\right]. \end{aligned}$$

For example, assume $v_1 = 100$, $v_2 = 100$, $v_3 = 110$, $v_4 = 101$, and $v_5 = 001$. We take a majority vote on each bit, and then we have $\hat{u}_6 = 100$. The rest are $\hat{u}_1 = \hat{u}_2 = 000$, $\hat{u}_3 = 010$, $\hat{u}_4 = 001$, and $\hat{u}_5 = 101$. We use $\hat{u}_i$ to denote the decoder output of u_i.

However, errors propagate in this scenario. If $u_6 = 000$, there is a one-bit error on u_6 if $\hat{u}_6 = 100$. However, we would have $u_1 = 100$, $u_2 = 100$, $u_3 = 110$, $u_4 = 101$, and $u_5 = 001$, which means that there is one bit error on each of $u_1, \cdots, u_5$. So long as the error rate is reasonably low, this error propagation is not a problem; the errors remain correctable, and can be fixed at the next round.

Fig. 6 demonstrates the circuit for syndrome measurement of four data blocks with three ancilla blocks according to a classical $[3, 1, 3]$ repetition code.

REFERENCES

[1] Frank Gaitan, Quantum Error Correction and Fault Tolerant Quantum Computing. CRC Press.

[2] D. P. DiVincenzo, P. W. Shor, "Fault-tolerant error correction with efficient quantum codes," *Phys. Rev. Lett.* **77**, pp.3260–3263, 1996.

[3] P. W. Shor, "Fault-tolerant quantum computation," in *Proceedings of the 37th Annual Symposium on the Theory of Computer Science*. Los Alamitos: IEEE Press, 1996, pp. 56–65.

[4] A. M. Steane, "Active stabilization quantum computation, and quantum state synthesis," *Phys. Rev. Lett.*, vol. 78, no. 11, pp. 2252–2255, 1997.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over $GF(4)$," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[6] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic Information Transfer Functions: a Model and Properties," *IEEE Trans. on Inform.Theory,* **50**, pp. 2657–2674, 2004.

[7] S. ten Brink, G. Kramer, A. Ashikhmin, "Design of Low-Density Parity-Check Codes for Modulation and Detection," *IEEE Trans. on Communications,* **52**, pp.670–678, 2004.

[8] E. Sharon, A. Ashikhmin, S. Litsyn, "Analysis of Low-Density Parity-Check Codes Based on EXIT Functions," *IEEE Trans. on Communications,* **54**, pp.1407–1414, 2006.