Performance of non-CSS LDGM-based quantum codes over the misidentified depolarizing channel

Patricio Fuentes, Josu Etxezarreta Martinez
and Pedro M. Crespo
Department of Basic Sciences and Bioengineering
Tecnun - University of Navarra
San Sebastian, Spain
{pfuentesu, jetxezarreta, pcrespo}@tecnun.es

Javier Garcia-Frías
Department of Electrical and Computer Engineering
University of Delaware
Newark, USA
jgf@udel.edu

***Abstract*—Quantum Low Density Generator Matrix (QLDGM) codes based on Calderbank-Steane-Shor (CSS) constructions have shown unprecedented error correction capabilities in the paradigm of quantum communication. Recently, a strategy based on non-CSS quantum codes derived from QLDGM CSS codes has been shown to surpass other Quantum Low Density Parity Check (QLDPC) schemes proposed in the literature over the depolarizing channel. Given the importance of quantum channel estimation and the impact it has on the performance of QLDPC codes, in this article, we study the behaviour of non-CSS QLDGM codes under the umbrella of channel mismatch. We begin by showing how a relatively accurate estimate of the quantum channel is pivotal for these codes to perform appropriately. We follow this by analyzing an off-line and an on-line quantum channel parameter estimation technique, as well as discussing how these methods affect the Quantum Error Correction (QEC) codes under consideration. Finally, we show how the on-line methodology yields similar performance to the perfect channel knowledge scenario despite its relative simplicity.**

***Index Terms*—Quantum Error Correction, Quantum Low Density Parity Check codes, Depolarizing Channel, Channel Mismatch.**

I. Introduction

In the realm of classical communications, turbo codes [1] and Low Density Parity Check (LDPC) codes [2], [3], [4], are known to exhibit capacity-approaching performance at a reasonable decoding computational complexity. Turbo codes offer great flexibility in terms of their block length and rate. The first quantum codes based on turbo codes appeared in [5], [6], and have since been modified and improved [7]- [13]. Aside from their block length and rate flexibility being on par with that of turbo codes, the sparse nature of LDPC codes guarantees that their quantum equivalents will require small numbers of quantum interactions per qubit during the error correction procedure [14], avoiding additional quantum gate errors and facilitating fault-tolerant computations. These traits make QLDPC codes especially well suited for quantum error correction.

Quantum LDPC codes are built by casting classical LDPC codes in the framework of stabilizer codes [15], which enables the design of quantum codes from any arbitrary classical binary and quaternary codes. Oftentimes, this is accomplished by designing QLDPC codes based on a particular subset of the family of stabilizer codes known as CSS codes [16], [17], which provides a straightforward method to design quantum codes from existing classical codes. In [18] and [19] CSS QLDPC codes based on Low Density Generator Matrix (LDGM) codes [20], a specific type of LDPC code whose generator matrix is also sparse, were shown to yield performance and code construction improvements. In [21] and [22], the performance of these codes was substantially improved by using a parallel concatenation of two regular LDGM codes. However, it is important to note that the performance of CSS codes is limited by an unsurpassable bound, referred to as the *CSS lower bound* [23]. This inspires the search for non-CSS stabilizer codes, as they should theoretically be able to outperform CSS codes if designed optimally. Non-CSS LDPC-based codes were proposed in [24] and [25] but they failed to outperform existing CSS QLDPC codes for comparable block lengths. Recently, the non-CSS inspired LDGM-based strategy proposed in [26] was shown to outperform all other CSS and non-CSS codes of similar complexity.

Most of the research related to the performance of QLDPC codes has been conducted under the tacit premise that perfect knowledge of the quantum channel in question is available. In reality, such a scenario is highly unlikely, meaning that analyzing how the behaviour of these codes changes in terms of the existing information about the quantum channel is of significant relevance. Such a study was conducted for the quantum depolarizing channel by Y. Xie et al in [27]. In [28], the same authors designed an improved decoding strategy for QLDPC codes when only an estimate of the channel depolarizing probability is available. The aforementioned method makes use of quantum channel identification, which requires the introduction of a probe (a known quantum state) into the quantum channel and the subsequent measurement of the channel output state to produce an accurate estimate of the depolarizing probability. This procedure typically makes use of additional qubits and results in a latency increase. Thus, the design of methodologies capable of minimizing this overhead while yielding performance similar to the perfect channel knowledge scenario is germane to this field of research. In [13], a so-called on-line depolarizing probability estimation technique is derived for Quantum Turbo Codes (QTCs). This

978-1-7281-8969-7/20/$31.00 ©2020 IEEE
DOI 10.1109/QCE49297.2020.00022

method yields similar performance to that obtained when using the same QTCs with perfect channel information but without the need for additional resources. In light of this outcome, a similar on-line estimation procedure for QLDPC codes is proposed in this article.

The remainder of this paper is structured as follows. In section II a brief review of the necessary preliminaries on stabilizer codes and quantum LDGM-based codes is provided. This is followed by a succint description of how good non-CSS LDGM-based codes are designed in section III. In section IV, the depolarizing channel is introduced, the off-line and on-line estimation techniques are presented, and the simulation results are discussed. Section V concludes our discourse.

II. Preliminaries

In this section, a brief review of important concepts, definitions, and notation related to stabilizer codes and QLDGM codes is provided.

A. Quantum Information

The simplest quantum mechanical system and the basic unit in quantum information is known as the qubit. In the state vector formulation, it is denoted by $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathcal{H}_2$; where α, $\beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$ and $\mathcal{H}_2$ refers to the complex Hilbert space of dimension 2. A quantum state of N qubits is written as $\sum_{i=0}^{2^N-1} \alpha_i\,|i\rangle$, where $\alpha_i \in \mathbb{C}$ and $\sum_i |\alpha_i|^2 = 1$. Suppose an N-qubit quantum state $|\omega\rangle \in \mathcal{H}_2^{\otimes N}$ is transmitted through a noisy quantum channel[1]. The output of the channel can be written as $E\,|\omega\rangle$, where the error operator E represents an N-fold tensor product of single qubit error operators e_j, where $j = 1, \ldots, N$. In QEC, these one-qubit error operators are represented by the X, Y, and Z Pauli operators, which together with the 2×2 identity matrix I define the set of single qubit Pauli operators $\{I, X, Y, Z\}$. We then define the *N-fold Pauli group* $\mathcal{G}_N$ by computing the N-fold tensor product of these single qubit Pauli operators and including the possible overall factors $\pm 1, \pm i$, i.e $\mathcal{G}_N = \{\beta_1 I, \beta_2 X, \beta_3 Y, \beta_4 Z\}^{\otimes N}$, where $\beta_k = \{\pm 1, \pm i\}$.

B. Stabilizer codes

Stabilizer codes are a class of QEC codes that can be efficiently designed based on existing classical codes. A stabilizer code $C(S)$ is defined by a set of operators S that generate an abelian subgroup of the N-fold Pauli group $\mathcal{G}_N$ under multiplication. The codespace defined by the stabilizer group is

$$C(S) = \{|\psi\rangle \in \mathcal{H}_2^{\otimes N} : S_i|\psi\rangle = |\psi\rangle, \forall i\},$$

i.e, the simultaneous $+1$-eigenspace defined by the elements of the stabilizer group S.

The generators of a stabilizer code, or more generally, Pauli operators on N qubits, can be described in terms of their symplectic representation [29]. Using this representation, each element of the N-fold Pauli group can be written as a unique binary string of length $2N$, which is built by joining two separate binary strings of length N. Individually, each of the length N binary strings represents the presence or absence of a Z or X operator on each of the N qubits with a '1' or a '0', respectively. Considered jointly, the strings also represent I and Y operators. For example,

$$YZXIX = (11000|10101).$$

Applying this representation to the generators S_i of a stabilizer code enables the definition of a Quantum Parity Check Matrix (QPCM) for the code. The parity check matrix of a quantum stabilizer code will be in the form $H_Q = (H_z|H_x)$, where row i of matrix H_Q is the symplectic representation of stabilizer generator S_i.

Using this QPCM notation, the requirement that stabilizer generators must commute can be re-expressed for the entire stabilizer code as

$$H_z \star H_x = (H_z H_x^T + H_x H_z^T)\text{mod}2 = 0\,, \tag{1}$$

where the $\star$ operator, known as the symplectic product, represents the operation itself. This expression, referred to as the *Symplectic Criterion*, is significant because it determines which existing classical codes can be used to design stabilizer codes.

In most quantum channels, decoherence is modelled by means of errors that belong to the N-fold Pauli group, which either commute or anticommute with each of the stabilizer generators S_i of a given stabilizer code $C(S)$ [29]. An error sequence E can be described using the symplectic representation as the length $2N$ binary string e. If we write e as $(e_z|e_x)$, when multiplying e in terms of the symplectic product (mod2) by a row of the parity check matrix of a stabilizer code, 0 will be obtained if E and the generator associated to that row commute, whereas 1 will be obtained if they anticommute. Multiplying this symplectic representation of the error operators by the quantum parity check matrix of a stabilizer code will yield the quantum syndrome s. That is,

$$s = H_Q \star e = (H_z e_x + H_x e_z)\text{mod}2\ , \tag{2}$$

where $e = (e_z|e_x)$ is the symplectic representation of the error pattern, $H_Q = (H_z|H_x)$ is the quantum parity check matrix of a stabilizer code, and s represents the quantum syndrome. We will later use this syndrome in the decoding process to estimate the symplectic representation of the error sequence e.

C. CSS Codes

Two binary classical LDPC codes can only be used to construct a stabilizer code if they satisfy the symplectic criterion (1). The first design strategy one could devise to construct stabilizer codes would be the random selection of pairs of classical LDPC codes. However, finding two LDPC codes of reasonable block size that satisfy (1) is highly unlikely. Calderbank-Shor-Steane codes [16], [17], provide a more efficient design strategy than random selection of classical

[1] $\mathcal{H}_2^{\otimes N}$ denotes the complex Hilbert space of dimension 2^N.

codes. The quantum parity check matrix of these codes is written as

$$H_Q = (H_z|H_x) = \begin{pmatrix} H_z^{'} & 0 \\ 0 & H_x^{'} \end{pmatrix}, \quad (3)$$

where $H_z = \begin{pmatrix} H_z^{'} \\ 0 \end{pmatrix}$ and $H_x = \begin{pmatrix} 0 \\ H_x^{'} \end{pmatrix}$.

In this construction, H_z' and H_x' are the parity check matrices of two classical LDPC codes C_1 and C_2, respectively, where each matrix is used to correct either bit-flips (H_z') or phase-flips (H_x'). The classical codes are chosen so that $C_2^{\perp} \subseteq C_1$, where $C_2^{\perp}$ is the dual of the classical LDPC code C_2. This design constraint, generally referred to as the *CSS condition*, reduces (1) to $(H_z^{'} H_x^{'T})\text{mod}2 = 0$.

D. Systematic classical LDGM codes

Let C be a systematic LDGM code. Then, its generator matrix $\tilde{G}$ and its parity check matrix $\tilde{H}$ can be written as

$$\begin{aligned} \tilde{G} &= (\mathbb{I}\ P) \\ \tilde{H} &= (P^T\ \mathbb{I}), \end{aligned} \quad (4)$$

where $\mathbb{I}$ denotes the identity matrix, and $P = [p_{lm}]$ is a sparse matrix. Because LDGM codes belong to the family of linear block codes, these matrices satisfy $(\tilde{G}\tilde{H}^T)\text{mod}2 = (\tilde{H}\tilde{G}^T)\text{mod}2 = 0$, ensuring that if they are used in (3), the resulting QPCM satisfies the symplectic criterion. Those systematic LDGM codes in which the rows and columns of the PCM have degrees[2] X and Y, respectively, are denoted as (X, Y) regular LDGM codes. Regular LDGM codes are known to be asymptotically bad [3], displaying error floors that do not decrease with the block length. However, in [30], codes built via the parallel concatenation of two regular LDGM codes[3] were shown to yield significant reduction in these error floors.

Classical LDPC decoding is performed by solving the equation $s = H_c e$, where s represents the received syndrome, H_c is the PCM of the code, and e is the symplectic representation of the error pattern we wish to recover. Given that LDGM codes are a specific subset of LDPC codes, they are decoded in exactly the same manner as generic LDPC codes, by applying belief propagation [31] (BP) [31] or the sum-product algorithm (SPA) [32] over the factor graph [32] associated to the equation $s = H_c e$.

E. Quantum LDGM CSS codes

Intuition calls for the QPCM of a QLDGM CSS code to be built by simply taking the classical LDGM code with parity check and generator matrices $\tilde{H}$ and $\tilde{G}$, and setting $H_z' = \tilde{H}$ and $H_x' = \tilde{G}$ in (3), since the property $(\tilde{G}\tilde{H}^T)\text{mod}2 = (\tilde{H}\tilde{G}^T)\text{mod}2 = 0$, ensures the fulfilment of the symplectic criterion. However, this results in a QPCM H_Q of size $N \times 2N$ and a code of quantum rate $R_Q = 0$, which cannot be used for encoding purposes. To build a valid quantum code, the number of rows in H_Q must be reduced while ensuring that (1) is fulfilled. In [18], this was achieved by applying the following theorem.

Theorem 1: Given the generator and parity check matrices of a systematic LDGM code (4), define $H_{m_1 \times N} = [M_1]_{m_1 \times n_1}[\tilde{H}]_{n_1 \times N}$ and $G_{m_2 \times N} = [M_2]_{m_2 \times n_2}[\tilde{G}]_{n_2 \times N}$, where $n_1 + n_2 = N$ and M_1 and M_2 are low-density full-rank binary matrices whose number of rows satisfy $m_1 < n_1$ and $m_2 < n_2$, respectively. Then, the quantum PCM shown in (5), obtained by setting $H_z' = H$ and $H_x' = G$ in (3), is the quantum PCM of an LDGM-based CSS code with rate $R_Q = \frac{N - m_1 - m_2}{N}$.

$$H_Q = (H_z|H_x) = \begin{pmatrix} H & 0 \\ 0 & G \end{pmatrix} = \begin{pmatrix} M_1\tilde{H} & 0 \\ 0 & M_2\tilde{G} \end{pmatrix}. \quad (5)$$

Quantum CSS LDGM codes are decoded by solving the quantum analogue of equation $s = H_c e$, which is shown in (2). This is achieved by running the SPA over the factor graph defined by the QPCM given in (5) and which characterizes the aforementioned equation. This specific factor graph is derived in [18], by splitting the symplectic representation of the error pattern into two parts, $e = (e_z|e_x)$, and relating it to the syndrome via a two step process[4]. In the following, we illustrate this derivation for e_x, the part of the symplectic representation of the error sequence related to the X operators. The procedure for e_z is identical but using G instead of H in (6).

$$s = He_x = M_1\tilde{H}e_x = M_1[P^T\ \mathbb{I}]e_x. \quad (6)$$

If we now split e_x into $e_x = (e_{x_1}\ e_{x_2})^T$, we can write

$$\begin{aligned} d_x = [P^T\ \mathbb{I}]e_x &= [P^T\ \mathbb{I}]_{n_1 \times N} \begin{pmatrix} e_{x_1} \\ e_{x_2} \end{pmatrix}_{N \times 1} \\ &= P^T_{n_1 \times n_2}[e_{x_1}]_{n_2 \times 1} + [e_{x_2}]_{n_1 \times 1}. \end{aligned} \quad (7)$$

We then relate d_x to the syndrome as

$$s_{m_1 \times 1} = M_{1_{m_1 \times n_1}} d_{n_1 \times 1} \quad (8)$$

Based on expressions (7) and (8), as well as their equivalents when using e_z and G in (6), we can obtain the generic factor graph of a quantum CSS LDGM-based code. Such a graph is shown in Figure 1.

The matrix multiplications used to perform the linear row operations on $\tilde{H}$ and $\tilde{G}$ generate a middle layer, represented by the c and d nodes, in both decoding subgraphs of Figure 1. This new layer hampers the decoding algorithm, especially during the initial decoding iterations, since *a priori* information regarding the aforementioned middle layer nodes is

[2]The degree of the columns is the number of nonzero entries per column of the PCM. The degree of the rows is given by the number of nonzero entries per row of the PCM. An LDGM code is said to be regular when all the rows of its PCM have the same number of nonzero entries, X, and so do its columns, Y.

[3]The parallel concatenation of regular LDGM codes is equivalent to an LDGM code with an irregular degree distribution.

[4]The syndrome is obtained as shown in (2).

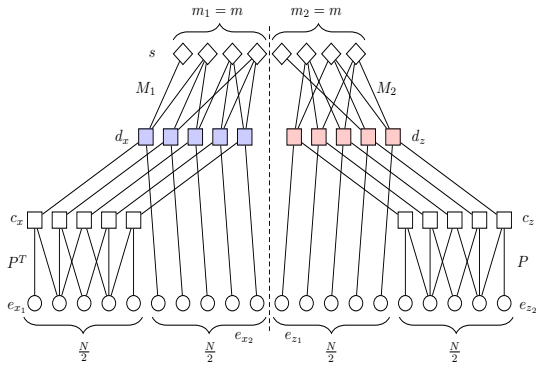

Fig. 1. Generalized factor graph for a QLDGM CSS scheme. The dotted line is included to emphasize the separation of the two constituent subgraphs. The leftmost subgraph decodes the X errors while the one on the right decodes the Z errors. We have assumed that $m_1 = m_2 = m$ and $n_1 = n_2 = \frac{N}{2}$.

not available. In [18], the authors circumvent this lack of information by using the so-called *doping* technique of [33]. This method introduces degree-1 syndrome nodes into the decoding graph, known as s_A nodes, that transmit correct information to the d nodes they are connected to, ultimately pushing the decoding process in the right direction.

III. Non-CSS LDGM-based Quantum Codes

Non-CSS codes are appealing due to their ability to exploit redundancy more efficiently than CSS schemes. Moreover, given that this type of code is not limited by the stringent CSS design constraints, non-CSS codes can theoretically surpass the *CSS bound* and get closer to the Hashing bound of a quantum channel. In [26], the LDGM-based CSS schemes of [19] - [22] are transformed into a non-CSS structure that outperforms other existing quantum codes of comparable complexity. In said work, different methods of constructing such non-CSS codes are provided. Here, we will be using a code based on the first structure proposed in [26].

A. Syndrome node combination to design non-CSS codes

The non-CSS design process begins by taking a CSS quantum code based on classical LDGM codes [19]- [22] as the starting point. As shown by the CSS factor graph of Figure 1, the code used as a starting point will be associated to two separate decoding subgraphs, one for H and the other for G. The upper layers of these subgraphs (the number and degree distribution of the d, s_A, and s_B nodes) will be defined by two identical matrices $M(y;1,x)$ of size $m \times \frac{N}{2}$. These matrices are described by the notation $(y;1,x)$ and the parameter t, which allows us to appropriately represent the upper layer of the CSS decoding graph. The notation is interpreted as follows: y represents the degree[5] of the d nodes, t is the number of syndrome nodes that are forced to have degree 1 (as required by the *doping* technique mentioned earlier) which we refer to as s_A nodes, and x represents the degree of the remaining syndrome nodes, referred to as s_B nodes. The non-CSS scheme is constructed as follows:

1) First, generate a new matrix, M_d:

$$M_d = \begin{pmatrix} M_{m\times\frac{N}{2}} & 0_{m\times\frac{N}{2}} \\ 0_{m\times\frac{N}{2}} & M_{m\times\frac{N}{2}} \end{pmatrix}_{2m\times N}. \tag{9}$$

2) Select q nodes out of the $2t$ s_A nodes of matrix M_d[6], which we will refer to as s_C nodes, and add an edge from these nodes to the d nodes on the side of the decoding graph they are not connected to. We apply a criterion to ensure that these new connections are not made randomly: *the edges added to the q selected s_A nodes can only be made to a d node (d_x or d_z) that is a d_A node*. We define d_A nodes as any d nodes that are connected to an s_A node. Of the q s_C nodes, half of them proceed from s_A nodes in the CSS subgraph used to decode the X operators, while the other half come from s_A nodes in the CSS subgraph used to decode the Z operators. Figure 2 illustrates how an s_C node is generated.

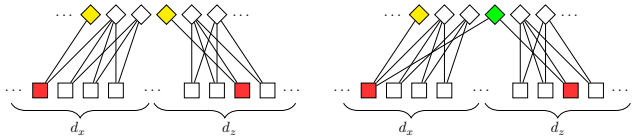

Fig. 2. Generation of an s_C node. The upper nodes represent the syndrome nodes while the bottom nodes represent the d nodes (d_x and d_z denote the d nodes associated to each of the separate CSS decoding subgraphs). The s_A nodes are represented in yellow, the d_A nodes are shown in red, and the s_C node is pictured in green.

At this stage, M_d has been transformed into a new matrix M'_d. We multiply M'_d by the QPCM of the CSS code to derive the QPCM of the non-CSS code. This matrix product morphs the upper layer of the original CSS decoding graph of figure 1 into a new version characterized by the following novelties:

- There are q s_C nodes that serve to join both sides of the graph.
- Some d nodes are connected to both s_A and s_C nodes.

These modifications force the s and d nodes of the non-CSS decoding graph to have a somewhat irregular edge distribution. Indeed, the "regularity" of the d nodes has been broken in order to connect the separate CSS decoding subgraphs, resulting in $\frac{q}{2}$ d_x nodes and $\frac{q}{2}$ d_z nodes having an additional edge. Furthermore, now q s nodes have two edges, one of them directed towards a d_x node and the other towards a d_z node. It is important to mention that decoding of these quantum LDGM-based schemes, independently of their CSS or non-CSS nature, is based on complete factor graphs like the one shown in Figure 1. This is different from decoding over the factor graph associated to the final matrix obtained from the product $M'_d H_{\text{CSS}}$. The rationale is the same as in serial concatenated LDGM schemes used in classical error

[5]The degree of a node is the number of edges it is connected to.

[6]Note that M_d, as defined in (9), is a simple algebraic representation of the upper layer of the graph in Figure 1.

correction, where decoding on the factor graph associated to the product of the matrices of the constituent codes also results in worse performance. This occurs because the product eliminates edges in the factor graph, introduces more cycles, and increases the density of ones [35] thus degrading the performance of the message passing algorithm.

The performance of this novel non-CSS structure will be heavily influenced by the value of q. If we select $q << m$, the decrease in the number of s nodes providing perfect information will be small and should have negligible impact in the decoding process[7]. On the contrary, the degree-2 s_C nodes allow the exchange of information between both sides of the graph as the iterative decoding process progresses, potentially improving the decoding performance. In [26], for a $R_Q = \frac{1}{4}$ non-CSS code of block length $N = 19014$ the optimum value of q was found to be 500.

IV. The Quantum Depolarizing Channel and Channel Estimation

A. The Quantum Depolarizing Channel

The effects quantum decoherence has on quantum information are usually described by means of quantum channels, $\mathcal{N}$. A widely applied quantum channel model used to represent the decoherence effects suffered by quantum information described by a density matrix ρ, is the generic Pauli channel $\mathcal{N}_P$. The effect of the Pauli channel $\mathcal{N}_P$ upon an arbitrary quantum state is described by

$$\mathcal{N}_P(\rho) = (1 - p_x - p_y - p_z)\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z.$$

A qubit then experiences a bit-flip (X operator) with probability p_x, a phase-flip (Z operator) with probability p_z or a combination of both (a Y operator) with probability p_y.

Most of the work conducted on quantum error correction considers the independent depolarizing channel model [5], [7], [24], [25]. This model is a specific instance of the Pauli Channel in which the individual depolarizing probabilities are all equal, i.e $p_x = p_z = p_y = \frac{p}{3}$, and the channel is characterized by the depolarizing probability p. When quantum states of N qubits are considered, the errors that take place belong to the N-fold Pauli group $\mathcal{G}_N$. Because we are considering the independent instance of the Pauli channel, these errors will act independently on each qubit causing an X, Z, or Y error with probability $p/3$ and leaving them unchanged with probability $(1 - p)$.

B. Quantum Channel Identification

A common assumption in the field of QEC is that perfect knowledge of the quantum channel under consideration is available prior to decoding. In reality, this information cannot be readily obtained, and estimates of the corresponding quantum channel parameter must be derived. In this paper, given that we only consider the depolarizing channel, the decoder must be provided with an estimate of the channel depolarizing probability. If the estimated value of the depolarizing probability $\hat{p}$ is different to its actual value p, i.e. $\hat{p} \neq p$, channel mismatch occurs, which leads to performance degradation.

To study the sensitivity of the non-CSS QLDGM scheme to the channel mismatch phenomenon, we consider a scenario where $\hat{p}$ is varied while the true depolarizing probability remains fixed. Figure 3 shows the results for the Qubit Error Rate (QBER), which represents the fraction of qubits that experience an error. For the simulations we have used the $R_Q = \frac{1}{4}$ $q = 500$ non-CSS code derived based on the first methodology presented in [26], and we have selected values of p that gradually get closer to the waterfall region of the code ($p = [0.05, 0.06, 0.07, 0.075, 0.0775, 0.08]$). Utilizing this simulation structure allows us to study the sensitivity of the code to the accuracy of $\hat{p}$ when the actual value of the depolarizing probability is varied. The specific code we have employed is based on an underlying parallel-concatenated LDGM code that has degree distribution $P[(8, 8)(3, 60)]$. The notation $P[(y_1, y_1); (y_2, z_2)]$ indicates the degree distributions of the constituent regular LDGM codes utilized in the parallel concatenation, i.e they are both regular LDGM codes with degree distributions (y_1, y_1) and (y_2, z_2), respectively. We have chosen the parallel concatenation with the smallest degrees tested in [26] in order to ease simulation requirements. Finally, the $q = 500$ M'_d matrix is obtained from two identical matrices defined by the configuration $M(3; 1, 8.72)$ and $t = 4361$, which are the same to those used in [26].

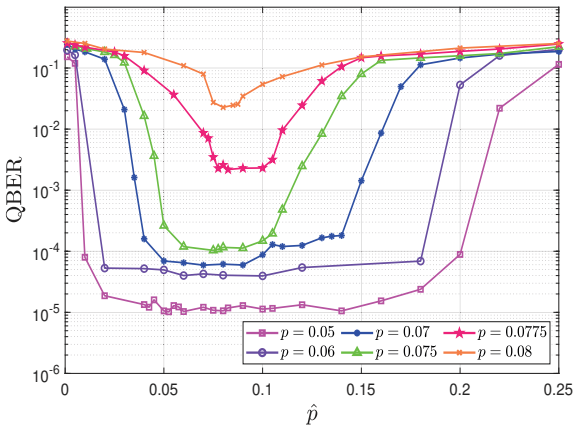

Fig. 3. Simulated QBER as a function of the estimated depolarizing probability $\hat{p}$ when the true depolarizing probability p is fixed.

As shown in Figure 3, for smaller values of p, i.e $p \leq 0.075$ (the error floor region of the code), the less accurate $\hat{p}$ needs to be to attain a performance similar to when perfect channel knowledge is available, i.e, when $\hat{p} = p$. On the contrary, when the waterfall region of the code is considered by setting $p > 0.075$, higher accuracy of the estimate $\hat{p}$ will be necessary to achieve the best possible performance. This is reflected by the decrease in width of the flat regions of the QBER curves as p is increased, where the flat region is defined as the part of

[7]A total of q s_A nodes get converted into s_C nodes, which do not provide perfect information.

the curve where the QBER is not significantly degraded [13]. This reduction in the size of the flat region indicates that the precision of the estimate $\hat{p}$ becomes increasingly important as p grows. For instance, if instead of estimating the value of the depolarizing probability we fix $\hat{p}$ to $p^* = 0.127$, which corresponds to the Hashing limit for a $R_Q = \frac{1}{4}$ quantum code, Figure 4 shows that for small values of p the resulting performance would be very close to that of a scheme with perfect knowledge of the depolarizing probability, but the performance degradation would increase for larger values of p. It is clear from these results that techniques capable of providing good estimates of $\hat{p}$ are necessary when facing a channel mismatch scenario. This is discussed in the following subsections, where two different estimation methodologies than can be used to obtain $\hat{p}$ are presented.

1) Off-line Estimation Method: In quantum channel identification, a known quantum state σ, referred to as the probe, is exposed to the effects of a specific quantum channel $\Gamma(p)$ which is dependent on some parameter p. Performing quantum measurements on the output quantum state $\sigma_o(p)$ yields classical information from which an estimation of p can be obtained. Numerous experimental schemes have been devised to perform quantum channel identification: the input quantum state can be unentangled, it can be entangled with ancilla qubits or other probes, or even multiple probes could be used. Given that analyzing the performance of these schemes is outside the scope of this paper, we will assume that an estimation set-up capable of obtaining the information-theoretical optimal performance is available. Optimal estimation of the depolarizing probability p of the depolarizing channel has previously been studied by making use of a metric known as the quantum Fisher information. The quantum Fisher information of p is given by

$$J(p) = \text{Tr}[\sigma_o(p)\hat{L}^2(p)],$$

where $\sigma_o(p)$ is the output quantum state and $\hat{L}(p)$ is the symmetric logarithm derivative defined implicitly as

$$\frac{\partial \sigma_o(p)}{\partial p} = \frac{1}{2}[\hat{L}(p)\sigma_o(p) + \sigma_o(p)\hat{L}(p)].$$

Since estimations of p are dependent on statistically distributed quantum measurements obtained from $\sigma_o(p)$, the estimate of the depolarizing probability $\hat{p}$ will be a random variable. Therefore, quantum channel identification comes down to selecting a procedure that provides the most accurate values of p. This is analogous to finding a method that minimizes the variance of the estimation $E\{(\hat{p} - p)^2)\}$, assuming that the estimator is unbiased, $E\{\hat{p}\} = p$. The best possible performance of any estimator is defined by the quantum Cramér-Rao bound. As previously mentioned, we operate under the assumption that our estimator attains the information-theoretical optimal performance, thus, its variance will be bounded by the quantum Cramér-Rao bound

$$var(\hat{p}) \geq \frac{1}{n_m J(p)} = \frac{1}{J_{n_m}(p)},$$

where $J_{n_m}(p) = n_m J(p)$ defines the overall Fisher information for n_m independent quantum measurements [36] and $J(p)$ denotes the Fisher information of p for a single measurement.

Based on the results shown in figure 3, where we studied the QBER in terms of the mismatched depolarizing probability $\hat{p}$, we can now compute the average $\tilde{\text{QBER}}(p)$ with regard to the real depolarizing probability of the channel p. This is shown in (10), where $P(\hat{p})$ is the probability density function of our optimal estimator.

$$\tilde{\text{QBER}}(p) = \int \text{QBER}(\hat{p})P(\hat{p})d\hat{p}. \tag{10}$$

As in [13], we assume that $P(\hat{p})$ is the truncated normal distribution defined between a and b, with mean μ, and variance $\frac{1}{J_{n_m}(p)}$. Choosing the variance of $P(\hat{p})$ as the inverse of the asymptotically achievable Fisher information allows us to assess the best possible accuracy of our quantum channel identification methods. The overall Fisher information $J_{n_m}(p)$ will vary in terms of the type of selected quantum probe. We will only consider the case where unentangled pure states are used as channel probes. In this case, the overall Fisher information is given by $J_{n_m}(p) = n_m\left(\frac{9}{8p(3-2p)}\right)$ [34].

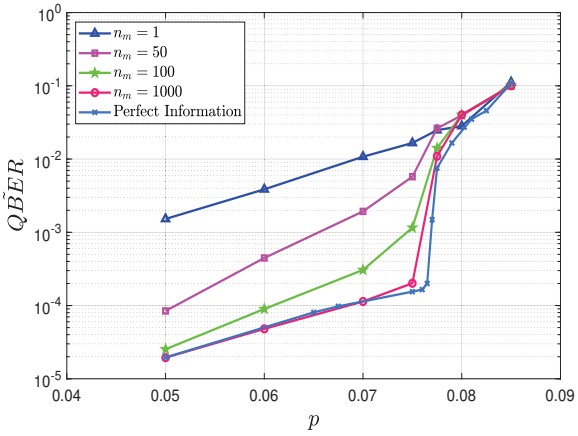

Fig. 4. Average QBER in terms of p when the number of used probes n_m is varied.

Figure 4 shows the result of computing $\tilde{\text{QBER}}(p)$ for the non-CSS QLDGM code considered in this paper as a function of the number of channel probes n_m. In [13], the off-line estimation protocol achieves the same performance as the perfect channel information case when $n_m \approx 1000$. The results shown in Figure 4 indicate that convergence is faster for our codes, since performance close to the perfect information case is obtained for $n_m \approx 100$. Also in [13], methodologies based on using maximally entangled pairs as probes (EPR pairs instead of pure states) resulted in faster convergence to the perfect information case, i.e less probes where required than when using unentangled pure states.

Regardless of the type of quantum probe, the main handicap of off-line estimation protocols is that if the channel varies

for every transmitted block, the overall rate of the QLDPC code that is being used will be severely reduced. Although this reduction in rate is asymptotically negligible for constant channels, it represents a significant drawback when using this estimation method in rapidly varying quantum channels.

2) On-line Estimation Method: In a similar fashion to what is done in [13] for QTCs, slight modifications to the generic sum-product syndrome-based iterative QLDPC decoder allow us to estimate the depolarizing probability while decoding is taking place. This on-line estimation scheme does not require quantum channel identification, meaning that rate reduction is avoided regardless of the type of quantum channel under consideration, be it constant or block-to-block time varying.

Decoding of a non-CSS QLDGM code is performed by running the sum product algorithm over the factor graph associated to the equation $s = H_Q \star e$, where s is the measured syndrome, H_Q is the QPCM of the code[8], and e is the symplectic representation of the error pattern induced by the quantum channel. The decoding objective is to find the most likely estimate of the channel error from the observed syndrome, i.e, the decoder must find the most likely estimate of the channel error, $\hat{E}$, such that the estimated syndrome $\hat{s} = H_Q \star \hat{e} = (M'_d \times H_{\text{CSS}}) \star \hat{e}$, is equal to the observed syndrome s, where $\hat{e}$ is the symplectic representation of $\hat{E}$.

With this purpose, the decoding process works as follows: First, the sum product algorithm is initialized using a "flooding" schedule in which lower layer nodes transmit messages upwards in a layer-by-layer sequential manner until the top-most nodes are reached. These messages are based on an initial estimate of the depolarizing probability of the channel $\hat{p}^{(1)}$, which is used to compute the a priori log likelihood ratios of the algorithm. Once information gets to the top layer, we say that the graph has been "flooded" with information, and decoding can actually begin. Decoding then proceeds using a reversed schedule, in which, starting from the top-most syndrome nodes, messages are exchanged downwards and layer-by-layer until the bottom-most nodes are reached. The messages transmitted by the syndrome nodes are computed considering information of the measured syndrome s. Once two messages have been transmitted over every edge of the factor graph, an iteration of the decoding algorithm has been completed. At the end of each iteration, an estimate of the symplectic representation of the error pattern $\hat{e}$ is produced and used to compute $\hat{s}$. If $s = \hat{s}$, then the algorithm has finished. If $s \neq \hat{s}$, the algorithm continues until it finds a matching syndrome or until a maximum number of iterations is reached. We can obtain an estimate of the depolarizing probability at each iteration j by assessing the number of X, Y, and Z operators present in the estimated error pattern[9] $\hat{E}$ and dividing them by the block length of the code. This is analogous to computing

$$\hat{p}^{(j)} = 1 - \frac{1}{N} \sum_{i=1}^{N} P^{(j)}(\hat{E}_i = I|\hat{s}), \tag{11}$$

where N is the block length of the code, I is the identity operator, $\hat{E}_i$ is the i-th component of the quaternary representation (in terms of I, X, Y, and Z operators) of the estimated error pattern, and $P^{(j)}(\hat{E}_i = I|\hat{s})$ is the probability at iteration j that the i-th component of the estimated error pattern is equal to the identity operator conditioned on the estimated syndrome.

Once $\hat{p}^{(j)}$ is obtained, it is used as the depolarizing probability to compute the necessary sum-product messages in the following iteration. Due to the iterative nature of the decoding algorithm, we expect that each successive estimate $\hat{p}^{(j)}$ will get closer to the actual value of p, leading to better decoding performance.

The last matter to discuss is how an appropriate value for the initial estimate of the depolarizing probability $\hat{p}^{(1)}$ can be obtained. It is intuitive to assume that this initialization might affect the convergence of the estimates $\hat{p}^{(j)}$ to p, thus having an impact on decoder performance. Given that in [13] excellent performance was observed regardless of the value of the initial estimate, we conducted an analysis by varying $\hat{p}^{(1)}$ while p remained fixed. The results are shown in Figure 5, where each dashed curve corresponds to a different value of the true depolarizing probability p. The curves associated to the original decoder, which where previously shown in Figure 3, are also included in Figure 5 as continuous lines.

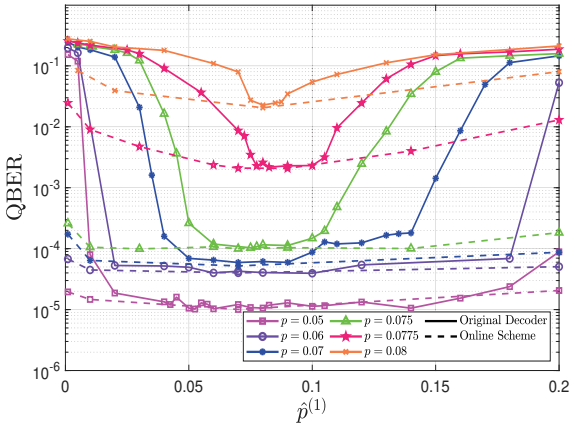

Fig. 5. Simulated QBER as a function of the initial estimate of the depolarizing probability of the channel $\hat{p}^{(1)}$. The continuous lines are associated to the original iterative QLDPC decoder which uses $\hat{p}^{(1)}$ for every iteration as if it were the true depolarizing probability. The dashed lines are obtained when the modified iterative decoder that uses the on-line estimation method is applied.

Upon closer inspection of the above figure, we can see that the performance of the on-line estimation method is similar to that of the perfect information scenario regardless of the value of $\hat{p}^{(1)}$. In fact, the modified on-line decoder significantly

[8]Recall that to reap the benefits of the non-CSS structure, the decoding algorithm must be run over the complete factor graph representation of the matrix product that defines H_Q. Decoding on the factor graph representation of the final matrix obtained from the product $M'_d \times H_{\text{CSS}}$ results in worse performance.

[9]$\hat{E}$ describes the error pattern using Pauli Operators, which can be easily obtained from its symplectic representation $\hat{e}$.

outperforms the original mismatched decoder, as is reflected by the flatter appearance of the curves associated to it. Figure 5 also shows how the sensitivity of the modified on-line decoder to the initial estimate $\hat{p}^{(1)}$ increases as p grows. This is reflected in a reduction of the flatness of the on-line curves as p increases, which is most noticeable for $p = 0.0775$ and $p = 0.08$.

Once the depolarizing probability is higher than a certain threshold ($p > 0.075$ in the scenario we consider), we enter into the waterfall region of the code, where qubit errors occur with much higher probability than in the error-floor region. Even though the on-line method computes $\hat{p}^{(j)}$ during every iteration, our simulations results show that for sufficiently large values of p, if $\hat{p}^{(1)}$ is either too small or too large, the convergence of $\hat{p}^{(j)}$ to p is weakened and performance is hindered. This happens due to a combination of two factors: On one hand, performance of the code is worse outside of the error floor region, and so the estimated error patterns are much more likely to have errors. On the other, small or large enough values of $\hat{p}^{(1)}$ make initial estimates of the error pattern contain either not enough or too many X, Y, and Z operators, corrupting the values of $P^{(j)}(\hat{E}_i = I|\hat{s})$ to the point that subsequent estimates $\hat{p}^{(j)}$ become increasingly inaccurate. This does not occur in the error floor region, where $\hat{p}^{(j)}$ converges to p regardless of the value of $\hat{p}^{(1)}$.

Ideally, we would like to define the value of $\hat{p}^{(1)}$ for which performance with the on-line estimation method is optimal. If we look at the curves corresponding to $p = 0.0775$ and $p = 0.08$, we can see performance is significantly degraded when $\hat{p}^{(1)} \leq 0.05$ or $\hat{p}^{(1)} \geq 0.13$. For the $R_Q = \frac{1}{4}$ code under consideration, the hashing limit is $p^* = 0.127$, which falls within the range $0.05 < p^* < 0.13$. Thus, performance on par with the perfect channel information scenario can be obtained with the on-line estimation method, regardless of the actual value of the depolarizing probability and without any additional resources or reductions in code rate, by setting $\hat{p}^{(1)} = p^*$.

V. Conclusion

In this work we have studied the sensitivity of non-CSS QLDPC codes to the channel mismatch phenomenon in the depolarizing channel. The codes are based on the generator and parity check matrices of regular LDGM codes. Our analysis reveals an increasing impact of channel mismatch on decoder performance as the depolarizing probability of the channel grows. The mismatch effect is especially noticeable in the waterfall region of the code. To combat the lack of channel knowledge that causes this mismatch, we have discussed both an off-line and an on-line estimation protocol to obtain estimates of the channel depolarizing probability. As in the case of QTCs, the on-line estimation scheme outperforms off-line channel identification techniques in terms of overall coding rate, while maintaining excellent performance. In contrast to what happens with QTCs, simulation results show that the on-line estimation method is slightly dependent on the initial estimate of the depolarizing probability when operating in the waterfall region. Selecting the initial estimate of the depolarizing probability as the hashing limit of the code in question yields good performance regardless of the actual value of the depolarizing probability.

VI. Acknowledgements

This work was supported by the Spanish Ministry of Economy and Competitiveness through the ADELE (PID2019-104958RB-C44) and CARMEN (TEC2016-75067-C4-3-R) projects. It has also been funded in part by NSF Award CCF-2007689. Josu Etxezarreta is funded by a Basque Government predoctoral research grant.

References

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes", *Proceedings of ICC '93 - IEEE International Conference on Communications,* Geneva, Switzerland, May 1994.

[2] R. G. Gallagher, "Low-density parity-check codes", IRE Transactions on Information Theory, vol. 8, pp. 21–28, January 1962.

[3] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices", IEEE Transactions on Information Theory, vol. 45, pp. 399–431, March 1999.

[4] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit", IEEE Communications Letters, vol. 5, pp. 58–60, February 2001.

[5] D. Poulin, J. Tillich, and H. Ollivier, "Quantum Serial Turbo Codes," IEEE Transactions on Information Theory, vol. 55, pp. 2776–2798, June 2009.

[6] M. Wilde, M. H. Hsieh, Z. Babar, "Entanglement-assisted quantum turbo codes", IEEE Transactions on Information Theory, vol. 60, pp. 1203–1222, February 2014.

[7] Z. Babar, S. X. Ng, and L. Hanzo, "EXIT-Chart-Aided Near-Capacity Quantum Turbo Code Design," IEEE Transactions on Vehicular Technology, vol. 64, pp. 866–875, March 2015.

[8] H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, "EXIT-Chart Aided Quantum Code Design Improves the Normalised Throughput of Realistic Quantum Devices," IEEE Access, vol. 4, pp. 10194–10209, July 2016.

[9] D. Chandra, Z. Babar, S. X. Ng, and L. Hanzo, "Near-Hashing-Bound Multiple-Rate Quantum Turbo Short-Block Codes," IEEE Access, vol. 7, pp. 52712–52730, April 2019.

[10] I. Granada, P. M. Crespo, and J. Garcia-Frías, "Asymptotic BER EXIT chart analysis for high rate codes based on the parallel concatenation of analog RCM and digital LDGM codes," EURASIP J Wireless Com Network, vol. 11, 2019.

[11] I. Granada, P. M. Crespo, and J. Garcia-Frías, "Combining the Burrows-Wheeler Transform and RCM-LDGM Codes for the Transmission of Sources with Memory at High Spectral Efficiencies," Entropy, vol. 21, pp. 378, April 2019.

[12] J. Etxezarreta, P. M. Crespo, and J. Garcia-Frías, "On the Performance of Interleavers for Quantum Turbo Codes," Entropy, vol. 21, pp. 663, June 2019.

[13] J. Etxezarreta, P. M. Crespo, and J. Garcia-Frías, "Depolarizing Channel Mismatch and Estimation Protocols for Quantum Turbo Codes," Entropy, vol. 21, pp. 1133, November 2019.

[14] D. J. Mackay, G. Mitchison, P. L. McFadden, "Sparse-Graph Codes for Quantum Error Correction", IEEE Communications Letters, vol. 50, pp. 2315–2330, October 2004.

[15] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound", Physical Review A, vol. 54, pp. 1862–1868, September 1996.

[16] A. R. Calderbank and P. W. Shor, "Good Quantum Error-Correcting Codes Exist," Physical Review A, vol. 54, pp. 1098–1105, August 1998.

[17] A. Steane, "Good Quantum Error-Correcting Codes Exist," Proceedings of The Royal Society A Mathematical, Physical and Engineering Sciences, vol. 452, pp. 2551–2577, November 1996.

[18] H. Lou and J. Garcia-Frias, "Quantum error-correction using codes with low-density generator matrix," *IEEE 6th Workshop on Signal Processing Advances in Wireless Communications,* New York, NY, USA, June 2005.
[19] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low-density generator matrix over different quantum channels," *4th International Symposium on Turbo Codes & Related Topics,* Munich, Germany, April 2006.
[20] T. R. Oenning and J. Moon, "A low-density generator matrix interpretation of parallel concatenated single bit parity codes", IEEE Transactions on Magnetics, vol. 37, pp. 737–741, March 2001.
[21] J. Garcia-Frias and K. Liu, "Design of near-optimum quantum error-correcting codes based on generator and parity-check matrices of LDGM codes," *42nd. Annual Conference on Information Sciences and Systems,* Princeton, NJ, USA, March 2008.
[22] K. Liu and J. Garcia-Frias, "Optimization of LDGM-Based Quantum Codes Using Density Evolution," *48th Annual Allerton Conference on Communication, Control, and Computing,* Allerton House, Illinois, USA, October 2010.
[23] D. Maurice, J.-P. Tillich, and I. Andriyanova, "A family of quantum codes with performances close to the hashing bound under iterative decoding," *IEEE International Symposium on Information Theory,* Istanbul, Turkey, July 2013.
[24] T. Camara, H. Ollivier, and J.-P. Tillich, "A class of quantum LDPC codes: Construction and performances under iterative decoding," *IEEE International Symposium on Information Theory,* Aachen, Germany, June 2007.
[25] D. Maurice, J.-P. Tillich, and I. Andriyanova, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," IEEE Transactions on Information Theory, vol. 56, pp. 476–491, December 2009.
[26] P. Fuentes, J. Etxezarreta, P. M. Crespo, and J. Garcia-Frías, "An approach for the construction of non-CSS LDGM-based quantum codes," Physical Review A, vol. 102, pp. 012423, July 2020.
[27] Y. Xie, J. Li, R. Malaney, and Jinhong Yuan, "Improved Quantum LDPC Decoding Strategies for the Misidentified Quantum Depolarization Channel," *2012 Australian Communications Theory Workshop,* Wellington, New Zealand, March 2012.
[28] Y. Xie, J. Li, R. Malaney, and Jinhong Yuan, "Improved Quantum LDPC Decoding Strategies for the Misidentified Quantum Depolarization Channel," *2016 24th European Signal Processing Conference,* Budapest, Hungary, September 2016.
[29] T. Brun, I. Devetak, and M. Hsieh, "Correcting quantum errors with entanglement.", Science, vol. 314, pp. 436-439, October 2006.
[30] W. Zhong, H. Chai, and Javier Garcia-Frias, "Approaching the Shannon Limit through Parallel Concatenation of Regular LDGM Codes," *Proceedings 2005 International Symposium on Information Theory,* Adelaide, Australia, September 2005.
[31] J. Pearl, "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference", Morgan Kauffman, San Francisco, 1988.
[32] F.R. Kschischang, B.J. Frey, and H.A. Loeliger, "Factor graphs and the sum-product algorithm," IEEE Transactions on Information Theory, vol. 47, pp. 498–519, February 2001.
[33] S. ten Brink, "Code doping for triggering iterative decoding convergence," *Proceedings. 2001 IEEE International Symposium on Information Theory,* Washington, DC, USA, June 2001.
[34] A. Fujiwara, "A Quantum channel identification problem," Physical Review A, vol. 63, pp. 042304, March 2001.
[35] W. Zhong and J. Garcia-Frias, "LDGM Codes for Channel Coding and Joint Source-Channel Coding of Correlated Sources," EURASIP Journal on Applied Signal Processing, vol. 6, pp. 942–953, May 2005.
[36] D. Collins and J. Stephens, "Depolarizing-channel parameter estimation using noisy initial states," Physical Review A, vol. 92, pp. 032324, September 2015.