Channel Identification and its Impact on Quantum LDPC Code Performance

Yixuan Xie, Jun Li, Robert Malaney and Jinhong Yuan

School of Electrical Engineering and Telecommunications
The University of New South Wales, Sydney, Australia
Email: Yixuan.Xie@student.unsw.edu.au, Jun.Li@unsw.edu.au, R.Malaney@unsw.edu.au, J.Yuan@unsw.edu.au

Abstract—In this work we probe the impact of channel estimation on the performance of quantum LDPC codes. Our channel estimation is based on an optimal estimate of the relevant decoherence parameter via its quantum Fisher information. Using state-of-the-art quantum LDPC codes designed for the quantum depolarization channel, and utilizing various quantum probes with different entanglement properties, we show how the performance of such codes can deteriorate by an order of magnitude when optimal channel identification is fed into a belief propagation decoding algorithm. Our work highlights the importance in quantum communications of a viable channel identification campaign prior to decoding, and highlights the trade-off between entanglement consumption and quantum LDPC code performance.

I. INTRODUCTION

A quantum error correction code (QECC) is intended to protect fragile quantum states from unwanted evolution and allow for robust implementations of quantum processing devices. Compared to classical communication systems, error correction in quantum communication channels is challenging, since a quantum bit, namely a qubit, has continuous states rather than two discrete states. Implementation of practical encoders and decoders in quantum codes is further complicated by the fact that a quantum state is usually affected by measurement, and that an unknown quantum state cannot be duplicated.

For classical error correction, it is well known that practical decodable codes exist. When an optimal decoder is applied, classical codes can achieve information rates close to the Shannon limit. Low-density parity-check (LDPC) codes are an example of such codes. The sparseness of the parity-check matrices makes the codes easy to encode and decode, even when communicating very close to the Shannon limit. It is established that the sum-product message passing algorithm is an optimal decoding algorithm for LDPC codes provided that the factor graph of LDPC codes is a tree structure, i.e. no cycles exist.

Following the discovery of CSS (Calderbank, Shor and Steane) codes and stabilizer codes, it has been known how quantum error-correction codes can be developed in a similar manner to classical codes. Quantum LDPC codes based on finite geometry were first proposed in [6]. However, a key constraint on the matrix representing the stabilizers (arising from commutativity requirements) makes the design of quantum LDPC codes difficult. In [7], Mackay et al. proposed the bicycle codes and explored the conjecture that the best quantum error-correcting codes will be closely related to the best classical codes, and in [8] Poulin et al. proposed serial turbo codes for quantum error correction. A more detailed history on the development of QECC can be found elsewhere e.g. [9]. More recently, many works attempting to improve quantum LDPC code performance have been published, and in this regard the recent codes of [11], [12], and [13] based on quasi-cyclic structure can be considered as representative of state-of-the-art quantum LDPC codes.

Hitherto, in investigations of the performance of quantum LDPC codes it has been assumed that perfect knowledge of the quantum channel exists. Of course in practice this is not the case. In this work we probe the impact of imperfect channel knowledge on the performance of quantum LDPC codes. We will utilize optimal estimates of the channel derived from quantum Fisher information about the channel parameters. More specifically, we will investigate the performance of quantum codes over the depolarization channel when optimal estimates of the depolarizing parameter are available.

In section II we first briefly review quantum communications and the stabilizer formalism for describing QECCs, and discuss their relationship to classical codes. In section III we review quantum channels and quantum channel identification. In section IV we present our simulation results using existing quantum stabilizer codes from [11] over the commonly used quantum Depolarizing Channel, showing how the imperfect channel identification impacts the codes performance. Lastly, we draw some conclusions and discuss future works.

II. QUANTUM CODES

The analog of classical ‘bit’ is a ‘qubit’, which can be represented as a quantum state $|\psi\rangle$ in a two-dimensional complex vector space. This can be written as a superposition

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

where $\alpha_0$ and $\alpha_1$ are complex numbers satisfying $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The quantum state of $N$ qubits has the form

$$\sum_{s} \alpha_s |s\rangle,$$

where $s$ runs over all binary strings of length $N$. The $2^N$ independent complex coefficients $\alpha_s$ then satisfy the normalization constraint $|\alpha_0|^2 + |\alpha_1|^2 + \ldots + |\alpha_{2^{N-1}}|^2 = 1$. Each of the $2^N$ states $|000\ldots0\rangle, |000\ldots1\rangle, \ldots, |111\ldots1\rangle$ is shorthand for the $N$-fold tensor product $|0\rangle \otimes |0\rangle \ldots \otimes |0\rangle$. 

...
Consider now a set of error operators \( \{ E_\alpha \} \) taking a state \( |\psi\rangle \) to the corrupted state \( E_\alpha |\psi\rangle \). A given error operator either commutes or anti-commutes with each stabilizer \( S_i \) (row of the generator \( S \)) where \( i = 1 \ldots N - K \). If the error operator commutes with \( S_i \), then
\[
S_i E_\alpha |\psi\rangle = E_\alpha S_i |\psi\rangle = E_\alpha |\psi\rangle
\]
and therefore \( E_\alpha |\psi\rangle \) is a +1 eigenstate of \( S_i \). Similarly, if it anti-commutes with \( S_i \), the eigenstate is −1. The measurement outcome of \( E_\alpha |\psi\rangle \) is known as the syndrome.

B. Conversion between Quantum and Classical Codes

To connect quantum stabilizer codes with classical LDPC codes it is useful to describe any given Pauli operator on \( N \) qubits as a product of an X-containing operator, a Z-containing operator and a phase factor \((+1, -1, i, -i)\). For example, the first row of matrix (2) can be expressed as
\[
\begin{pmatrix}
Z & Z & X & I & X \\
X & Z & Z & X & I \\
I & X & Z & Z & X \\
X & I & X & Z & Z
\end{pmatrix} = (I I X I X) \times (Z Z I Z I).
\]

Thus, we can directly express the X-containing operator and Z-containing operator as separate binary strings of length \( N \).

In the X-containing operator a 1 represents the X operator (likewise for the Z operator), and 0 for \( I \). The resulting binary formalism of the stabilizer is a matrix \( A = (A_1|A_2) \) of \( 2N \) columns and \( M = N - K \) rows, where \( A_1 \) and \( A_2 \) represent X-containing and Z-containing operators, respectively.

**Example 1**: For example, the set of stabilizers in (2) appears as the binary matrix \( A \)
\[
A = (A_1|A_2) = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{pmatrix}.
\]

Due to the requirement that stabilizers must commute, a constraint on a general matrix \( A \) can be written as e.g. (7).

\[
A_1 A_2^T + A_2 A_1^T = 0.
\]

Note that the classical syndrome can be conceptually considered as an equivalent to the classical syndrome \( A e \), where \( A \) is a binary parity-check matrix and \( e \) is a binary error vector.

To summarize, the property of stabilizer codes can be directly inferred from classical codes. Any binary parity-check matrix of size \( M \times 2N \) that satisfies the constraint in (6) defines a quantum stabilizer code with rate \( R = \frac{K}{N} \) that encodes \( K \) qubits into \( N \) qubits.

C. CSS Codes

As mentioned earlier, an important class of codes are the CSS Codes (3)(4). These have the form
\[
A = \begin{pmatrix} H & 0 \\
0 & G \end{pmatrix}
\]
where \( H \) and \( G \) are \( M_H \times N \) and \( M_G \times N \) matrices, respectively, \((M_H \text{ does not necessary equal to } M_G)\). Requiring \( H G^T = 0 \) ensures that constraint (6) is satisfied. If \( G = H \), the resulting CSS code structure is called a dual-containing code. Most classical (good) LDPC codes do not satisfy the constraint (6).

III. QUANTUM CHANNEL MODELS AND ESTIMATION

A. Quantum Channel Models

Given some initial system state \( |\Psi_s\rangle \), a decoherence model can be built by studying the time evolution of the system state’s interaction with some external environment with initial state \( |\Psi_e\rangle \). Without loss of generality we can assume \( |\Psi_s\rangle \) and \( |\Psi_e\rangle \) are initially not entangled with each other.

In terms of the density operators \( \rho_s = |\Psi_s\rangle \langle \Psi_s | \) and \( \rho_e = |\Psi_e\rangle \langle \Psi_e | \), the initial state of the combined total system can be written as \( \rho_s \otimes \rho_e \). The closed evolution of \( \rho_s \otimes \rho_e \) can be described by a unitary \( U \) via \( U (\rho_s \otimes \rho_e) U^\dagger \). To obtain the output system state, \( \rho_s^{\text{out}} \), after some closed evolution \( U \), we use \( \rho_s^{\text{out}} \equiv \varepsilon (\rho_s) = \text{Tr}_e [U (\rho_s \otimes \rho_e) U^\dagger] \) where \( \text{Tr}_e \) is the partial trace over the environment’s qubits. The channel \( \rho_s^{\text{out}} \equiv \varepsilon (\rho_s) \) is a completely positive, trace preserving, map which...
provides the required evolution of $\rho_s$. It is possible to describe such maps directly using an operator-sum representation,
\[
\varepsilon(\rho_s) = \sum_{a=1}^{N_o} K_a \rho_s K_a^\dagger, \quad \text{where} \quad \sum_{a=1}^{N_o} K_a^\dagger K_a = I, \tag{8}
\]
and where $K_{a=1...N_o}$ represent the so-called Kraus operators, with $N_o$ being the number of Kraus operators \cite{14}.

There are of course decoherence channels modeled on specific qubit-environment interactions (e.g. see \cite{9}). In this work we will consider only the depolarization channel. Let us introduce the depolarization parameter, $f$, of a qubit where $0 \leq f \leq 1$, with $f = 1$ meaning complete depolarization and $f = 0$ meaning no depolarization. In terms of the Pauli matrices $\sigma_i$ (here $i = 0, 1, 2, 3$), the depolarization channel for a single qubit can be defined as $\varepsilon(\rho_s) = (1 - f)\rho_s + f \frac{1}{4} \rho_s$.

Using the relation $\sigma_o = \frac{1}{2} \left( \rho_s + \sum_{j=1}^{3} \sigma_j \rho_s \sigma_j \right)$, we see that the Kraus operators for the depolarization channel can be written $K_1 = \sqrt{1 - f} \sigma_o$, $K_2 = \sqrt{f} \sigma_x$, $K_3 = \sqrt{f} \sigma_y$, and $K_4 = \sqrt{f} \sigma_z$. Note that it is also possible to parameterize the depolarization channel as $\varepsilon(\rho_s) = (1 - f')\rho_s + f' \frac{1}{3} \sum_{j=1}^{3} \sigma_j \rho_s \sigma_j$, where $f' = \frac{3}{4} f$. This latter form is more convenient for decoding purposes, and below we term $f'$ as the flip probability.

B. Quantum Channel Estimation

The issue of quantum channel identification (quantum process tomography) is of fundamental importance for a range of practical quantum information processing problems (e.g. \cite{20}). In the context of LDPC quantum error correction codes, it is normally assumed that the quantum channel is known perfectly in order for the code design to proceed. In reality of course, perfect knowledge of the quantum channel is not available - only some estimate of the channel is available. The key focus of this work is an investigation of this issue. To make progress we will assume a depolarization channel with some parameter $f$. However, we assume the true value of $f$ is unknown a priori, and must first be measured via some channel identification procedure. This estimate of $f$ will then be used in the decoder in order to measure its performance relative to a decoder in which the true $f$ is utilized.

In general, quantum channel identification proceeds by inputting a known quantum state $\sigma$ (the probe) into a quantum channel $\Gamma_p$ that is dependent on some parameter $p$ (in our case $p = f$). By taking some quantum measurements on the output quantum state $\Gamma_p(\sigma)$ which leads to some result $R$, we then hope to estimate $p$. The input quantum state may be unentangled, entangled with an ancilla qubit (or qudit), or entangled with another probe. Multiple probes could be used, or the same probe can be recycled (i.e. sent through the channel again). As can be imagined many experimental schemes could be developed along these lines, and the performance of each scheme (i.e. how well it estimates the true value of the parameter $p$) could be analyzed. However, in this study we will take a different tact. Here we will simply assume an experimental set-up that obtains the information-theoretical optimal performance.

Optimal channel identification via the use of the quantum Fisher information has been well studied in recent years, particularly in regard to the determination of the parameter $f$ of the depolarizing channel (e.g. \cite{15,16,17,18,19}). Defining $\rho_f = \Gamma_f(\sigma)$, the quantum Fisher information about $f$ can be written as
\[
J(f) = J(\rho_f) = \text{tr} \left[ \rho_f L_f^2 \right],
\]
where $L_f$ is the symmetric logarithmic derivative defined implicitly by
\[
2\partial_f \rho_f = L_f \rho_f + \rho_f L_f,
\]
and where $\partial_f$ signifies partial differential w.r.t. $f$. With the quantum Fisher information in hand, the quantum Cramer-Rao bound can then be written as
\[
\text{mse} \left[ \hat{f} \right] \geq (N_m J(f))^{-1}
\]
where $\text{mse} \left[ \hat{f} \right]$ is the mean square error of the unbiased estimator $\hat{f}$, and $N_m$ is the number of independent quantum measurements. In the simulations pursued here we will assume the channel is constant over the block length of the codeword, and unless otherwise stated we assume $N_m = 1$. Further, we will assume two different cases for the quantum probe. In case A we will assume the qubit probe is in a pure unentangled state, and as such \cite{15} the quantum Fisher information about $f$ relevant to each codeword can be shown to be $J(f) = \frac{1}{2} \left( 2 - f \right)^{-1}$. In case B we adopt the scenario where one pair of maximally entangled qubit particles is consumed per transmission of each codeword (one of the qubits traverses the channel). In this latter case the quantum Fisher information about $f$ relevant to each codeword can be shown to be $J(f) = \frac{1}{2} \left( 2 - f \right)^{-1}$ \cite{15}. Similar expressions for qudit probes are available \cite{19}.

IV. Simulations

From the discussion in Section II, a stabilizer generator can be described in the binary form, $A = (A_1|A_2)$. It is also worthwhile to note that it can also be described in a quaternary form, where $A_1$ and $A_2$ are packed into a single matrix with elements $I$, $X$, $Y$, $Z$. Since a close link between $\{I, X, Y, Z\}$ and $\{0, 1, \omega, \omega^2\}$ exists, where $\omega$ is the primary element in GF(4), a quantum stabilizer code can be thought of as an analog to a GF(4) classic code. Thus, a Belief Propagation (BP) decoding algorithm in GF(4) \cite{20} can be applied to quantum stabilizer codes. For lower computational complexity, we applied BP-decoding in GF(2). However, the decoder was modified from the pure classical decoder in order to break the degeneracy problem of stabilizer codes. To break the degeneracy, a heuristic method presented in \cite{20} was adopted.
where is the flip probability known at the decoder.

The standard BP algorithm operates by sending messages along the edges of the Tanner graph. Let and denote the messages sent from bit node to check node and messages sent from check node to bit node, respectively. Also denote as the number of neighbors of bit node, and define as the number of neighbors of check node.

To initialize our algorithm, each qubit node sends out a message to all its neighbors equal to its initial probability value obtained according to equation (9). Upon reception of these messages, each check node sends out a message to its neighboring qubit node given by

\[ u_{c_j \rightarrow b_i} = \sum_{t_{1 \ldots n} \in \{1 \ldots M\}} \prod_{b_j \in N(b_i) \backslash b_i} u_{b_j \rightarrow c_j} \]  

(10)

where denotes all neighbors of check node except qubit node, and the summation is over all possible error sequences . Each bit node then sends out a message to its neighboring checks given by

\[ u_{b_i \rightarrow c_j} = p_i \prod_{c_j' \in N(b_i) \backslash c_j} u_{c_j' \rightarrow b_i} \]  

(11)

where denotes all neighbors of qubit node except check node. Equations (10) and (11) operate iteratively until the message is correctly decoded or the maximum predetermined iteration number is reached.

Fig.1 illustrates the performance - i.e. the qubit error rate (QBER) - of our BP decoder achieved for an existing quantum stabilizer code, namely the code (rate=1/2) of [11]. The lower solid line indicates the performance of our decoder with perfect channel information. Whereas, the upper solid line shows the performance of the decoder when no channel information has been made available at the decoder. The corresponding frame error rate (FER) is also shown for each case. Note, the QBER is the fraction of the qubits that possess an error, whereas the FER is the fraction of qubit blocks of length that contain at least one qubit error.

**A. Iterative BP-Decoding Algorithm**

Given our previous discussions, the decoding algorithm applied in our simulations can be viewed as a variation of the standard BP message-passing decoding algorithm taking place in the binary field, with the decoder treating the depolarizing channel as two independent binary symmetric channels. The received values (here ) and (where ) are either 0 or 1. These can be mapped to measurement outcomes (syndrome) of the received qubit sequence, and this syndrome is then used in error estimation and recovery. Assuming an initial quantum state representing a codeword, the initial probabilities for the th qubit of the state undergoing an error are

\[ p_i = \begin{cases} f' \text{ for } X, Y, \text{ or } Z \\ 1 - f' \text{ for } I \end{cases}, \]  

(9)

where is the flip probability known at the decoder.

For imperfect channel knowledge

Consider now the case where a decoder can only attain partial channel information by probing the quantum channel using un-entangled and entangled quantum states (only one measurement each, i.e. ). To simulate case and discussed in section for each encoded block of qubits of length transmitted through the depolarizing channel, an estimated flip probability is randomly chosen at the receiver side from a normal distribution (truncated in a range of 0 to 1) characterized by mean and variance .

Simulation results using imperfect channel knowledge as discussed above are illustrated in Fig2. The quantum LDPC code used here is the same code adopted for Fig1. The decoding process terminates if 100 block errors are collected or the maximum iteration number is reached. Contrary to Fig1 the results in Fig2 show the QBER and FER of the stabilizer code when only partial channel information on the channel is available at the decoder. We can clearly see that using entangled quantum states for estimation yields a better performance. Although not shown, as the mean value of approaches zero, the performance gap between the entangled and un-entangled estimation methods approaches the expected theoretical performance discussed in II-B.

In Fig3 we collect the above results into the one plot for direct comparison purposes. Note that as the number of quantum states used to probe the channel goes to infinity, the performance of the code will approach to the performance of the curves marked as “perfect channel information”. As we can see from the figure, even optimal channel identification using one probe measurement leads to roughly an order of magnitude hit on performance. We anticipate similar performance hits for any state-of-the-art quantum LDPC code. That the increase in the number of probing states leads to a better code performance, demonstrates the trade-off between the number of qubit probes (or entanglement consumption) and code performance.
It is important to note that, as is the normally the case, our performance curves are determined from simulation only. We have not developed any theoretical framework that can predict our new performance curves. In this context we note the work of [21] in which LDPC code error performance is theoretically predicted for the binary symmetric channel as a function of a crossover probability $p_c$ and a different initialization probability. It would be interesting to investigate whether extensions of the concepts introduced in [21] could deliver the necessary theoretical framework for directly predicting quantum LDPC code performance as a function of the quantum Fisher information on the channel parameters.

V. CONCLUSION AND FUTURE WORK

Utilizing quantum probes which are either in un-entangled pure quantum states or maximally entangled qubit pairs, we have explored how channel identification in the quantum depolarizing channel affects the performance of quantum LDPC codes. Our results show the importance in quantum communications of a viable channel identification campaign prior to the decoding of any quantum codeword. Our work also highlights the trade-off between entanglement consumption and quantum LDPC code performance. Future work will investigate similar issues for other quantum codes, consider more generic quantum channels, and pursue quantum LDPC code designs where uncertainty in the quantum channel is directly embedded.

REFERENCES

[1] R. G. Gallager, “Low-density parity-check codes,” PhD, MIT, 1963.
[2] D. MacKay, “Good error-correcting codes based on very sparse matrices,” IEEE Transactions on Information Theory, vol. 45, pp. 399-431, 1999.
[3] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A, vol. 54, pp. 1098-1105, 1996.
[4] A. M. Steane, “Error Correcting Codes in Quantum Theory,” Phys. Rev. Letters, vol. 77, pp. 793-797, 1996.
[5] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound,” Phys. Rev. A, vol. 54, pp. 1862-1866, 1996.
[6] M. S. Postol, “A proposed quantum low density parity check code,” arXiv:quant-ph/0010131v1, 2001.
[7] D. MacKay, G. Mitchison, and P. McFadden, “Sparse-graph codes for quantum error correction,” IEEE Transactions on Information Theory, vol. 50, pp. 2315-2330, 2004.
[8] D. Poulin, J. P. Tillich, and H. Ollivier, “Quantum serial turbo codes,” IEEE Transactions on Information Theory, vol. 55, pp. 2776-2798, 2009.
[9] M. Nielsen and I. Chuang, “Quantum computation and quantum information,” Cambridge Series on Information and the Natural Sciences, Cambridge University Press, 2000.
[10] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola and W. H. Zurek, “Introduction to Quantum Error Correction,” arXiv:quant-ph/0207170v1, 2002.
[11] P. Tan and J. Li, “Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions,” IEEE Transactions on Information Theory, vol. 56, pp. 476-491, 2010.
[12] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, “Spatially coupled quasi-cyclic quantum LDPC codes,” IEEE Proc. on International Symposium in Information Theory, pp. 638-642, 2011.
[13] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, “Quantum Error Correction beyond the Bounded Distance Decoding Limit,” IEEE Transactions on Information Theory, arXiv:1007.1779v2 [cs.IT], 2011.
[14] Kraus, K. “States, Effects and Operations: Fundamental Notions of Quantum Theory”, Lecture Notes in Physics, vol. 190, Springer-Verlag, Heidelberg, Germany, 1983.
[15] A. Fujiwara, “Quantum channel identification problem,” Phys. Rev. A, vol. 63, 042304, 2001.
[16] M. Sasaki, M. Ban, and S. M. Barnett, “Optimal parameter estimation of a depolarizing channel,” Phys. Rev. A, vol. 66, 022308, 2002.
[17] A. Fujiwara and H. Imai, “Quantum parameter estimation of a generalized Pauli channel,” Journal of Physics A: Mathematical and General, vol. 36, no. 29, pp. 8093–8103, 2003.
[18] M. R. Frey, A. L. Miller, L. K. Mentch, and J. Graham, “Score operators of a qubit with applications,” Quantum Information Processing, vol. 9, no. 6, 629-641, 2010.
[19] M. R. Frey, D. Collins, and K. Gerlach, “Probing the qudit depolarizing channel,” Journal of Physics A: Mathematical and Theoretical, vol. 44, no. 20, 205306, 2011.
[20] D. Poulin and Y. Chung, “On the iterative decoding of sparse quantum codes,” Quantum Information Computation, vol. 8, pp. 987–1000, 2008.
[21] M. Hagiwara, M. P. C. Fossorier, H. Imai, “LDPC Codes with Fixed Initialization Decoding over Binary Symmetric Channel,” IEEE Proc. on International Symposium in Information Theory, pp. 784-788, 2010.