

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

Universal Decoding of Quantum Stabilizer Codes via Classical Guesswork

DARYUS CHANDRA¹, ZEYNEP B. KAYKAC EGILMEZ¹, YIFENG XIONG¹, SOON XIN NG¹,
ROBERT G. MAUNDER¹, LAJOS HANZO¹

¹School of Electronics and Computer Science, University of Southampton, UK.

Corresponding author: Lajos Hanzo (email: lh@ecs.soton.ac.uk).

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/W016605/1 and EP/X01228X/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom (Grant No. 789028)

ABSTRACT

A universal decoding scheme is conceived for quantum stabilizer codes (QSCs) by appropriately adapting the 'guessing random additive noise decoding' (GRAND) philosophy of classical domain codes. We demonstrate that the generalized quantum decoder conceived is eminently suitable for different QSC decoding paradigms, namely for both stabilizer-measurement-based as well as the inverse-encoder-based decoding. We then harness the resultant decoder for both quantum Bose-Chaudhuri-Hocquenghem (BCH) codes and quantum polar codes and quantify both their quantum block error rate (QBLER), and QBLER per logical qubits as well as their decoding complexity. Furthermore, we provide a parametric study of the associated design trade-offs and offer design guideline for the implementation of GRAND-based QSC decoders.

INDEX TERMS

 quantum error correction codes, quantum stabilizer codes, quantum noise, decoding

I. INTRODUCTION

Quantum error-correction codes (QECCs) [1]–[3] constitute a potent solution of mitigating the quantum decoherence prevalent in quantum systems. The primary concept of QECCs is reminiscent of that of classical forward error-correction (FEC) codes. Specifically, the quantum state of logical qubits is mapped into the encoded state of physical qubits by incorporating auxiliary qubits during the encoding step. These auxiliary qubits are then exploited by the decoder for determining the appropriate recovery operator. However, due to the short coherence time of the quantum bits (qubits), the QECCs encoding and decoding procedures should be completed before the qubits decohere further. Unfortunately, most of the QECCs available in the open literature require a high number of physical qubits and exhibit a very low quantum coding rate because, in contrast to classical FEC codes, QECCs have to correct not only bit-flip errors, but also phase-flip errors as well as the combination of both. Thus, it is a challenge to conceive QECCs for a moderate number of physical qubits, while maintaining a very low quantum bit error ratio (QBER).

Although at first sight seemingly unrelated, the de-

velopment of ultra-reliable low-latency communications (URLLCs) faces similar challenges to those encountered in quantum error correction coding (QECCs) research. For example, one of the challenges is that the decoding of the QECC must be completed before the qubits start to lose coherence, since the coherence time of the qubits is very limited. In other words, similar to URLLC, QECCs also require prompt and reliable decoding. Another challenge is finding an error correction code with a short to moderate length codeword that has a high error correction capability and hence attains a low bit error ratio (BER).

In the classical regime, the powerful maximum-likelihood (ML) decoder has been proposed for meeting the stringent requirements imposed by URLLC. However, ML decoding exhibits potentially excessive complexity, which hinders its hardware implementation. As a remedy, an innovative decoder based on classical guesswork was proposed as an attractive solution for short- to moderate-length classical FEC codes, but without imposing the excessive complexity of the standard ML decoder, which is referred to as guessing random additive noise decoding (GRAND) [4]–[7]. The

complexity reduction achievable by GRAND exploits the classical guesswork concept, where the decoder generates the channel induced error patterns from the most likely to the least likely and in turns verifies whether the sequence that remains after the error removal is part of the legitimate codebook. As an additional benefit, GRAND is eminently suitable for a large family of classical FEC codes, since it operates in an error-pattern-centric manner. Thus, GRAND might be utilized for a wide range of classical FEC codes having no efficient decoder.

Inspired by this solution advocated in the classical domain, we aim for conceiving a universal decoder for QECCs. As a benefit of the classical-to-quantum isomorphism, a wide range of classical FEC codes can be transplanted into the quantum domain. More specifically, we focus our attention on the family of quantum stabilizer codes (QSCs), which constitute the family of syndrome-based QECCs [8]–[11].

Against this background, our contributions can be summarized as follows:

- 1) We devise a universal decoding scheme for QSCs by further evolving the GRAND decoding philosophy. We demonstrate that the decoding scheme conceived may be adopted for two different QSC decoding paradigms, namely for both stabilizer-measurement-based as well as the inverse-encoder-based decoding.
- 2) We then apply the resultant decoder for both quantum BCH codes as well as quantum polar codes and quantify their quantum block error ratio (QBLER), QBLER per logical qubits as well as their decoding complexity.
- 3) We conclude with a parametric study of the associated design trade-offs and provide the design guideline for the implementation of Quantum-GRAND-aided QSC decoding.¹

The rest of this treatise is organized as follows. Section II introduces the decoding classical FEC codes via guesswork while Section III introduces the quantum stabilizer codes. Then, a pair of Quantum-GRAND-aided QSC decoding paradigms are discussed in Section IV, namely the stabilizer-measurement-based decoder and the inverse encoder-based decoder. Sections V provides simulation results for characterizing the family of quantum BCH and polar codes. Explicitly, we portray the performance versus complexity of Quantum-GRAND-aided QSC decoders, relying on both stabilizer-measurement-based as well as on inverse-encoder-based schemes. Finally, Section VI offers our conclusions and some future research directions.

II. DECODING CLASSICAL FEC CODES VIA GUESSWORK

Let $\mathcal{C}(n, k, d)$ denote a classical FEC code mapping the information word of length k bits into the codeword of length n bits. Let c^n denote the legitimate codeword $c \in \mathbb{F}_2^n$ as an input of the channel and y^n denote the received word

¹Please note that the similar term of QGRAND was used by the authors of [12] to represent “quantized” GRAND in a different context.

after an error pattern e^n is inflicted by the channel. The transformation can be explicitly written as

$$y^n = x^n \oplus e^n, \quad (1)$$

where \oplus denotes modulo-2 addition. If the error pattern e^n is known, the legitimate codeword c^n is recoverable by applying the following transformation:

$$x^n = y^n \oplus e^n. \quad (2)$$

In this scenario, the standard ML decoding is defined as

$$c^{n,*} = \arg \max_{c_i^n} p(y^n | c_i^n), \quad \forall c_i^n \in \mathcal{C}, \quad (3)$$

where $c^{n,*}$ is the codeword solution c^n that maximizes the conditional probability $p(y^n | c_i^n)$ over all possible values of c_i^n , so that c_i^n is an element of the codebook \mathcal{C} .

Based on (3), the number of evaluation of $p(y^n | c_i^n)$ required for finding the solution $c^{n,*}$ is equal to the cardinality of the codebook $\mathcal{C}(n, k, d)$, which is given by $C = |\mathcal{C}| = 2^k$. It is clear that exhaustive sequential evaluation of all entries in the codebook \mathcal{C} using ML decoder is excessively complex.

Recently, a new classical paradigm of ML decoding was introduced by exploiting the concept of classical guesswork [6], [7], which is formulated as follows:

- Given the received word y^n , initialize $i = 1$ and set g^n to be the first guess based on the most likely error pattern.
- While $x^n = y^n \oplus g^n \notin \mathcal{C}$, increase i by 1 and set g^n to be the next guess based on next most likely error pattern.
- The process ends when we find $x^n = y^n \oplus g^n \in \mathcal{C}$ in this while loop and the final value of i determines the computational complexity of this decoder.

A compelling benefit of hard-decision GRAND is its ability to verify whether the sequence left behind after the error removal x^n is part of the legitimate codebook. We can observe that since GRAND operates in an error-pattern-centric manner, the decoder does not require the entire codebook to be stored in memory. The decoder simply needs the parity check matrices H or the generator matrices G or even only the kernel of the codes in case of polar codes. It has been proven in the seminal paper of GRAND [6] that the average complexity of GRAND for the binary symmetric channel (BSC) is given by

$$C = 2^{n \cdot \min\{1-k/n, H_{1/2}(p)\}}, \quad (4)$$

where p is the flip probability of the BSC, and $H_\alpha = H_{1/2}$ is the Rényi entropy for $\alpha = 1/2$ [13]. The complexity expression of (4) demonstrates the significant complexity reduction against the standard ML decoder. Furthermore, the hardware complexity of the hard-decision GRAND has been demonstrated to be appealingly low, as presented in [14].

To explicitly portray the complexity reduction achieved by GRAND, Fig. 1 depicts the complexity of standard ML decoding compared to the average complexity of GRAND for classical FEC codes having codeword lengths of $n = \{128, 64, 32\}$ in the face of the BSC. The complexity is

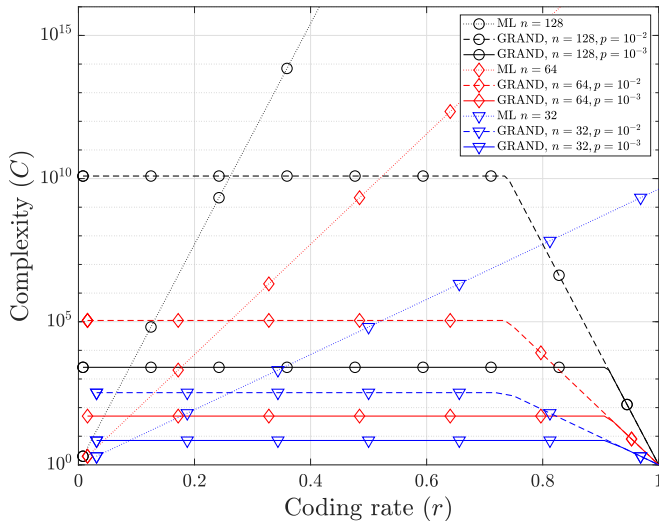


FIGURE 1: The complexity C of standard ML decoding compared to the average complexity of ML GRAND for classical error-correction codes having codeword length of $n = \{128, 64, 32\}$ over BSC.

portrayed as the function of coding rate $r = k/n$. Observe in Fig. 1 that since GRAND is an error-pattern-centric decoder, its complexity is driven by the channel’s error probability. For the BSC, it is given by the flip probability p . For instance, let us observe in Fig. 1 the average complexity of GRAND for $n = 128$, which is significantly lower for $p = 10^{-3}$ than that of $p = 10^{-2}$. Similar trends can also be observed for $n = 64$ and $n = 32$. For the BSC, the likelihood of the error patterns is rank-ordered based on their Hamming weight. Thus, for a lower value of p , the probability that the channel inflicts an error sequence e^n having a high Hamming weight is extremely low. Consequently, the number of error patterns that have to be evaluated before finding the legitimate codeword is also lower, since it is far more likely that the channel inflicts a lower Hamming weight error pattern than a higher one.

As the coding rate decreases, we can see that the complexity of the standard ML decoding also decreases. Thus, we can find the cross-over point below which the standard ML decoder has a lower complexity than GRAND. For instance, for $n = 128$, the ML decoder exhibits a lower complexity when $k < 34$ for $p = 10^{-2}$ and $k < 12$ for $p = 10^{-3}$. Similarly, for $n = 64$, we find that the complexity of the ML decoder is lower than GRAND when $k < 18$ for $p = 10^{-2}$ and $k < 6$ for $p = 10^{-3}$. Finally, the cross-over point for $n = 32$ is given by $k < 9$ and $k < 3$, for $p = 10^{-2}$ and $p = 10^{-3}$, respectively. In the region where the ML decoder exhibits a lower complexity, the size of the legitimate codebook \mathcal{C} is significantly smaller than the average number of evaluations required by GRAND for finding the correct solution.

III. QUANTUM STABILIZER CODES

Since the concept of protecting quantum information is similar to that of classical FEC codes, it is natural to aim for transplanting the classical FEC codes philosophy into the quantum domain. In this treatise, we focus our attention on the QSCs, which constitute a class of syndrome-based QECCs. Specifically, QSCs can be constructed by exploiting the so-called classical-to-quantum isomorphism [8]–[11]. A QSC denoted by $\mathcal{C}[[N, K, D]]$ maps K logical qubits having the original quantum state $|\psi\rangle$ into N physical qubits having the encoded quantum state $|\bar{\psi}\rangle$ with the aid of $(N - K)$ auxiliary qubits. The minimum distance of the QSC is denoted by D and its error correction capability is given by $T = \lfloor (D - 1)/2 \rfloor$.

In this treatise, we consider the class of quantum Pauli channels for modeling the quantum decoherence imposed on the encoded physical qubits. Explicitly, the qubit errors imposed by the quantum Pauli channels may be described by the linear combinations of Pauli matrices $\{I, X, Y, Z\} \in \mathcal{G}$, where \mathcal{G} denotes the Pauli group². Physically, the Pauli X error constitutes a bit-flip error, the Pauli Z error represents the phase-flip error, while the Pauli Y describes the simultaneous bit-flip and phase-flip errors.

The encoded state of physical qubits are designed by ensuring that it is projected onto the (+1) eigenspace of the group of Pauli operators $\mathcal{S} \subset \mathcal{G}_N$ known as the stabilizer group so that we have $\mathcal{S}_i |\bar{\psi}\rangle = (+1) |\bar{\psi}\rangle$ for every stabilizer operator $\mathcal{S}_i \in \mathcal{S}$. If the encoded state of physical qubits is subject to a Pauli error E that anti-commutes with a stabilizer operator $\mathcal{S}_j \in \mathcal{S}$, the measurement of this stabilizer operator will collapse the encoded state of the logical qubits onto its (−1) eigenspace given by

$$\mathcal{S}_j E |\bar{\psi}\rangle = (-1) |\bar{\psi}\rangle. \quad (5)$$

The results of the stabilizer measurements form a “syndrome” that can be used for determining the appropriate recovery operator \mathcal{R} .

A QSC \mathcal{C} that encodes K logical qubits has a set of logical operators \mathcal{L} that are defined as operators that commute with all of the stabilizer operators $\mathcal{S}_i \in \mathcal{S}$, but they themselves do not constitute stabilizer operators. The initial state of the logical qubits $|\psi\rangle$ will experience a so-called logical error if a Pauli error constituted by a logical operator \mathcal{L} is imposed on the encoded state of the physical qubits $|\bar{\psi}\rangle$. The minimum Pauli weight of the logical operator \mathcal{L} therefore defines the minimum distance D of the QSC \mathcal{C} .

By exploiting the classical-to-quantum isomorphism [8]–[11], we may perform the mapping of Pauli operators $\mathcal{P} \in \mathcal{G}_N$ to a classical binary vector in \mathbb{F}_2^{2n} , which allows us to transform various classes of classical FEC codes into QSCs. More specifically, the Pauli-to-binary mapping may

²A single qubit Pauli group $\mathcal{G}_1 = \{I, X, Y, Z\}$ is constituted by the following matrices: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ and $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The N -qubit Pauli group is given by $\mathcal{G}_N = \otimes_{i=0}^N \mathcal{G}_i$.

be explicitly defined as follows:

$$I \mapsto (0|0), X \mapsto (1|0), Y \mapsto (1|1), Z \mapsto (0|1). \quad (6)$$

Therefore, an N -qubit Pauli operator $P \in \mathcal{G}_N$ can be mapped to a $2n$ -bit binary vector as follows:

$$P \in \mathcal{G}_N \mapsto g = (g_x|g_z) \in \mathbb{F}_2^{2n}, \quad (7)$$

where g_x is an n -bit binary vector having an element equal to 1 in the particular location, where the Pauli operator P has a Pauli matrix X . Similarly, g_z is an n -bit binary vector having an element equal to 1 in the specific location, where Pauli the operator P having a Pauli matrix Z . Consequently, a Pauli operator associated with a Pauli matrix Y results in an element equal to 1 in the corresponding position of both vectors g_x and g_z . As an example, the two-qubit Pauli operator $P = X \otimes Y$ maps to the binary representation of $g = (11|01)$.

Again, by exploiting the classical-to-quantum isomorphism, a QSC can be derived from classical FEC codes. Explicitly, given a pair of parity-check matrices (PCMs) H_x and H_z , we may construct a QSC, whose binary PCM H is formulated by

$$H = [H_z \mid H_x]. \quad (8)$$

To conceive a valid QSC, the pair of classical PCMs H_x and H_z have to satisfy the symplectic criterion given by [3], [15]

$$H_z \cdot H_x^T + H_x \cdot H_z^T = 0. \quad (9)$$

Thus, the stabilizer operators of a QSC can be written as a binary PCM having $M \times 2N$ elements, where each row corresponds to one of the M stabilizer operators. Now, let us assume that a Pauli error operator E associated with the corresponding binary vector $e_Q = (e_x|e_z)$ is inflicted by the quantum channel \mathcal{P} . Thus, the stabilizer measurements will generate the syndrome vector given by

$$s_Q = (e_x|e_z) \cdot [H_z|H_x]^T = (s_x|s_z). \quad (10)$$

The subscript x of s_x implies that the syndrome vector is used for determining the number and the location of Pauli X errors and similarly, the subscript z of s_z is for Pauli Z errors.

The Calderbank-Shor-Steane (CSS)-type QSCs [2], [16] constitutes a specific subset of QSCs that have disjoint X and Z stabilizer operators such that the non-identity part of each stabilizer operator is made up either exclusively of X Pauli matrices or exclusively of Z Pauli operators. In the binary representation, the PCM of a CSS-type QSC can be expressed as

$$H_{\text{CSS}} = \left[\begin{array}{c|c} H_z & 0 \\ \hline 0 & H_x \end{array} \right]. \quad (11)$$

For CSS-type QSC codes, the symplectic criterion can be further simplified into

$$H_z \cdot H_x^T = 0. \quad (12)$$

Furthermore, if the construction satisfies $H_z = H_x$, the

resultant QSC is referred to as dual-containing CSS-type QSC.

By accounting for (10) and (11), the syndrome vector of CSS-type QSCs can be obtained as follows:

$$s_Q = e_x \cdot H_z^T + e_z \cdot H_x^T = (s_x|s_z). \quad (13)$$

Consequently, the syndrome vector s_Q of CSS-type QSCs allows the bit-flip and phase-flip errors to be corrected using separate classical FEC codes. Therefore, for the rest of his treatise, we employ the classical GRAND for CSS-type QSCs.

IV. DECODING QUANTUM STABILIZER CODES

In the previous section, we have explicitly demonstrated how to transform classical FEC codes into their quantum domain counterparts. Let us now discuss how to decode QSCs in the presence of quantum impairments by exploiting GRAND. Generally speaking, there is a pair of paradigms that can be utilized for decoding QSCs. The first one is constituted by stabilizer-measurement-based decoding [8], while the second one is by inverse-encoder-based decoding [17]. The stabilizer-measurement-based decoding is widely utilized in the literature for QSCs, where the classical FEC codes forming the basis of the QSCs exploit the symplectic condition of the PCM formulation, as exemplified by quantum linear block codes [18], quantum Bose-Chaudhuri-Hocquenghem (BCH) codes [19], and quantum low-density parity-check codes [20]. By contrast, the inverse-encoder-based decoding is invoked for QSCs, whose classical FEC codes forming the QSCs are defined by their corresponding encoders, such as quantum convolutional codes [21], quantum turbo codes [17], as well as quantum polar codes [22]. In this treatise, we aim for demonstrating that by further evolving the classical-domain GRAND philosophy of [6], we can further develop this decoder for both decoding paradigms.

We will use the Steane's 7-qubit code as an example for both decoding paradigms, where a total of six stabilizer operators are required for correcting a single-qubit error. These stabilizer operators $S_i \in \mathcal{S}$ are given as follows:

$$\begin{aligned} S_1 &= ZZIZZII, \\ S_2 &= ZIZZZI, \\ S_3 &= IZZZIIZ, \\ S_4 &= XXIXXII, \\ S_5 &= XIXXIXI, \\ S_6 &= IXXXIIX. \end{aligned} \quad (14)$$

Thus, based on the Pauli-to-binary mapping of (6) and based on the binary PCM of the CSS-type QSCs of (11), we have

$$H_z = H_x = \left[\begin{array}{cccccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right]. \quad (15)$$

Steane's 7-qubit code has a quantum coding rate of $r_Q = K/N = 1/7$ and a minimum distance of $D = 3$, which

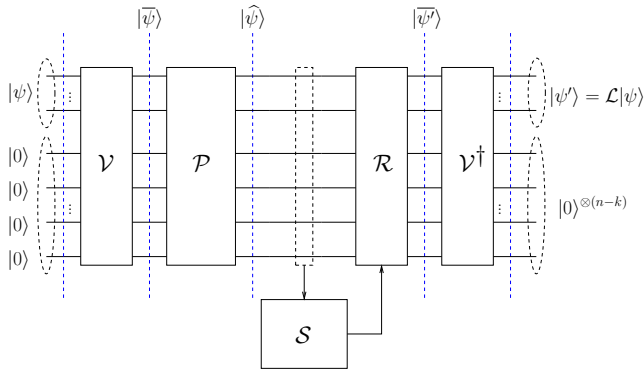


FIGURE 2: The general schematic of the encoding and decoding of QSCs based on the stabilizer measurements.

means that it is capable of correcting a single-qubit error ($T = 1$).

A. STABILIZER-MEASUREMENT-BASED DECODING

The general schematic of QSC encoding and decoding based on stabilizer measurements is depicted in Fig. 2. The initial state of K logical qubits is mapped into the encoded state of N physical qubits with the aid of $(N - K)$ auxiliary qubits using the quantum encoder \mathcal{V} , which can be formulated as follows:

$$|\bar{\psi}\rangle = \mathcal{V} \left(|\psi\rangle \otimes |0\rangle^{\otimes(N-K)} \right). \quad (16)$$

The quantum channel \mathcal{P} imposes errors represented by the N -tuple Pauli operator $\mathbf{E} \in \mathcal{G}_N$, which can be formally expressed as

$$|\hat{\psi}\rangle = \mathbf{E} |\bar{\psi}\rangle. \quad (17)$$

The measurements of the stabilizer operators $\mathbf{S}_i \in \mathcal{S}$ generate the eigenvalues of ± 1 , which are analogous to the classical syndrome values as described in Section III. We have also demonstrated how Pauli-to-binary mapping is utilized for transforming the stabilizer operators $\mathbf{S}_i \in \mathcal{S}$ into the binary PCM \mathbf{H} . Finally, the error recovery \mathcal{R} is applied according to the specific syndrome values and decoding algorithm utilized. Finally, the inverse encoder \mathcal{V}^\dagger transforms the corrected state of physical qubits $|\bar{\psi}'\rangle$ back to the corrected state of logical qubits $|\psi'\rangle$.

Based on the description of the classical-domain GRAND philosophy in Section II, the observation of the of the received word \mathbf{y}^n is pivotal in the evaluation process for determining the legitimate codeword. However, in the quantum domain, such measurements cannot be performed on the physical qubits, since this would collapse the superposition of the encoded quantum states to the classical values. Consequently, the ML decoding of QSCs based on the measurement of stabilizer operators may be reformulated as finding the most likely error pattern \mathbf{e}^{2n} based on the syndrome value \mathbf{s}_Q from the received quantum state as follows:

$$\mathbf{e}^{2n,*} = \arg \max_{\mathbf{e}_i^{2n}} p(\mathbf{e}_i^{2n} | \mathbf{s}_Q), \forall \mathbf{e}_i^{2n} \in \mathbb{F}_2^{2n}, \quad (18)$$

where $\mathbf{e}^{2n,*}$ is the most likely error pattern \mathbf{e}^{2n} imposed on the physical qubits that maximizes the conditional probability $p(\mathbf{e}_i^{2n} | \mathbf{s}_Q)$ over all possible values of \mathbf{e}_i^{2n} , such that \mathbf{e}_i^{2n} is an element of \mathbb{F}_2^{2n} .

For CSS-type QSCs, $\mathbf{s}_Q = (\mathbf{s}_x | \mathbf{s}_z)$ may be obtained using (13). Thus, instead of relying on the measurement of the received quantum states, we may perform GRAND by relying on the syndrome vector \mathbf{s}_Q obtained from the stabilizer measurements. More specifically, the Quantum-GRAND-aided QSC decoder relying on the stabilizer measurements can be described as follows:

- Given the Pauli error operator $\mathbf{E} \in \mathcal{G}_N$ having the binary vector representation of $\mathbf{e}^{2n} = (\mathbf{e}_x^n | \mathbf{e}_z^n)$, calculate $\hat{\mathbf{s}}_x = \mathbf{e}_x^n \cdot \mathbf{H}_z^T$ and $\hat{\mathbf{s}}_z = \mathbf{e}_z^n \cdot \mathbf{H}_x^T$.
- Initialize $i = 1$ and set \mathbf{g}_x^n to be the initial guess based on the most likely error vector for the Pauli \mathbf{X} error pattern and calculate $\mathbf{s}_x = \mathbf{g}_x^n \cdot \mathbf{H}_z^T$.
- While $\hat{\mathbf{s}}_x \neq \mathbf{s}_x$, increase i by 1 and set \mathbf{g}_x^n to be the next guess based on the next most likely error vector for the Pauli \mathbf{X} error pattern and calculate $\mathbf{s}_x = \mathbf{g}_x^n \cdot \mathbf{H}_z^T$.
- The process ends when we find $\hat{\mathbf{s}}_x = \mathbf{s}_x$ in this while loop and the final value of i determines the computational complexity of Pauli \mathbf{X} error decoding.
- Initialize $j = 1$ and set \mathbf{g}_z^n to be the initial guess based on the most likely error vector for the Pauli \mathbf{Z} error pattern and calculate $\mathbf{s}_z = \mathbf{g}_z^n \cdot \mathbf{H}_x^T$.
- While $\hat{\mathbf{s}}_z \neq \mathbf{s}_z$, increase j by 1 and set \mathbf{g}_z^n to be the next guess based on the next most likely error vector for the Pauli \mathbf{Z} error pattern and calculate $\mathbf{s}_z = \mathbf{g}_z^n \cdot \mathbf{H}_x^T$.
- The process ends when we find $\hat{\mathbf{s}}_z = \mathbf{s}_z$ in this while loop and the final value of j determines the computational complexity of Pauli \mathbf{Z} error decoding.
- The recovery operator $\mathcal{R} \in \mathcal{G}_N$ is constituted by the Pauli operator represented by the binary vector $(\mathbf{g}_x^n | \mathbf{g}_z^n)$ and the total complexity is given by $C = i + j$.

Table 1 portrays the syndrome vector associated with the most likely Pauli \mathbf{X} and Pauli \mathbf{Z} error patterns of Steane's 7-qubit code. We have a total of 16 syndromes for correcting both the Pauli \mathbf{X} and Pauli \mathbf{Z} errors. Explicitly, seven of them represent seven single-qubit bit-flip error patterns and seven correspond to single-qubit phase-flip error patterns. Additionally, we have a pair of $(0\ 0\ 0)$ syndrome vectors indicating the absence of bit-flip and phase-flip errors. Thus, each of the syndrome vector is capable of identifying a unique a single-qubit error pattern. The error pattern \mathbf{E} in Table 1 is rank-ordered based on their likelihood in the face of quantum Pauli channels, which means the first error pattern is constituted by the error-free pattern, followed by the single qubit-error patterns. Since all the single-qubit error patterns exhibit an equal probability of occurrence, they can be rank-ordered arbitrarily.

Let us provide a small-scale example of Quantum-GRAND-aided stabilizer-measurement-based QSC decoding by utilizing Steane's 7-qubit code, assuming that the quantum Pauli channel \mathcal{P} induces the error pattern of $\mathbf{E} =$

TABLE 1: Syndrome values and the associated error-recovery operator \mathcal{R} .

Error operator E	Syndrome s_x	Error recovery \mathcal{R}	Error operator E	Syndrome s_z	Error recovery \mathcal{R}
<i>IIIIIII</i>	(0 0 0)	<i>IIIIIII</i>	<i>IIIIIII</i>	(0 0 0)	<i>IIIIIII</i>
<i>XIIIIII</i>	(1 1 0)	<i>XIIIIII</i>	<i>ZIIIIII</i>	(1 1 0)	<i>ZIIIIII</i>
<i>IXIIIII</i>	(1 0 1)	<i>IXIIIII</i>	<i>IZIIIII</i>	(1 0 1)	<i>IZIIIII</i>
<i>IIXIIII</i>	(0 1 1)	<i>IIXIIII</i>	<i>IIZIIII</i>	(0 1 1)	<i>IIZIIII</i>
<i>IIIXIII</i>	(1 1 1)	<i>IIIXIII</i>	<i>IIIZIII</i>	(1 1 1)	<i>IIIZIII</i>
<i>IIIXII</i>	(1 0 0)	<i>IIIXII</i>	<i>IIIZII</i>	(1 0 0)	<i>IIIZII</i>
<i>IIIIIXI</i>	(0 1 0)	<i>IIIIIXI</i>	<i>IIIIZI</i>	(0 1 0)	<i>IIIIZI</i>
<i>IIIIIX</i>	(0 0 1)	<i>IIIIIX</i>	<i>IIIIIZ</i>	(0 0 1)	<i>IIIIIZ</i>

IIXIIZI. Thus, by using the Pauli-to-binary mapping of (6), the syndrome calculation of (13), and the binary PCM of the Steane’s code 7-qubit of (15), we obtain $\hat{s}_x = (0\ 1\ 1)$ and $\hat{s}_z = (0\ 1\ 0)$. Upon relying on these syndrome vectors, GRAND will generate the error patterns commencing the most likely to the least likely one and evaluates the syndrome vector. This evaluation process will stop when the decoder finally finds the error pattern that produces the same syndrome vector as \hat{s}_x and \hat{s}_z . In this example, GRAND will find the specific Pauli X error pattern from Table 1 after four evaluations ($i = 4$) and identify the Pauli Z error pattern after seven evaluations ($j = 7$). Thus, the total complexity of GRAND in this scenario is given by $C = i + j = 4 + 7 = 11$. In a more complex scenario, where a QSC is capable of correcting multiple qubits error, the evaluation process will continue to the two-qubit error patterns, three-qubit error patterns, and so on until GRAND finds the specific error pattern that generates the same syndrome vector as the channel-induced syndrome vector.

In our Quantum-GRAND-aided simulation of stabilizer-measurement-based QSC decoding, the observation of errors is carried out for the quantum state $|\psi'\rangle$ after the error recovery operator \mathcal{R} is applied as shown Fig. 2. For the stabilizer-measurement-based QSC decoder, we declare a quantum block error for every instance when we find $(e_x^n|e_z^n) \neq (g_x^n|g_z^n)$. Thus, the quantum block error rate (QBLER) Q is the ratio between the number of quantum block errors observed to the total number of quantum blocks simulated. Therefore, to compare the performance of various QSCs having different quantum coding rates r_Q as well as different number of logical qubits K , we may utilize the notion of normalized QBLER per logical qubits. The QBLER per logical qubits P inferred from the QBLER Q observed may be calculated as

$$P = 1 - (1 - Q)^{1/K}. \quad (19)$$

B. INVERSE-ENCODER-BASED DECODING

In contrast to Fig. 2, the general schematic of the QSC encoding and decoding based on inverse encoding is depicted in Fig. 3. The quantum encoder \mathcal{V} and the quantum Pauli channel \mathcal{P} act in the same way as those in Fig. 2. The main difference is that instead of applying stabilizer measurements

to the corrupted quantum state $|\hat{\psi}\rangle$, we apply the inverse encoder \mathcal{V}^\dagger . The effect of \mathcal{V}^\dagger can be explicitly expressed as

$$\mathcal{V}^\dagger (E |\bar{\psi}\rangle) = L |\psi\rangle \otimes S |0\rangle^{\otimes(N-K)}. \quad (20)$$

To elaborate briefly on the effect of the inverse encoder \mathcal{V}^\dagger in Fig. 3, it effectively decomposes the error operator E into two components, namely the logical error component L imposed on the K logical qubits and the auxiliary error component S inflicted upon the $(N - K)$ auxiliary qubits. In this case, the measurement of the error operator contaminating the auxiliary qubits $S |0\rangle^{(N-K)}$ may be carried out either by using the computational (Z) basis $\{|0\rangle, |1\rangle\}$ or the Hadamard (X) basis $\{|+\rangle, |-\rangle\}$. The measurement results represent the syndrome vector to be used by the inverse-encoding-based decoder. More specifically, the measurement results are constituted by a syndrome vector $s_Q = (s_x|s_z)$, where s_x is obtained from the measurement of error operators using the Z basis and s_z is from the measurement using the X basis³.

By exploiting the Pauli-to-classical mapping, the quantum encoder \mathcal{V} harnessed for creating N physical qubits from K logical qubits can be unambiguously represented by a binary matrix V having $(2n \times 2n)$ elements. Similarly, the inverse encoder \mathcal{V}^\dagger can be expressed as a binary matrix V^{-1} and the measurement operators \mathcal{M} can be represented by a binary matrix M . Therefore, the effect of the Pauli error operator E after the application of the inverse encoder \mathcal{V}^\dagger and of the measurement operators \mathcal{M} can be represented in binary form as

$$(e_x|e_z) \cdot V^{-1} \cdot M = (l_x : s_x : \mathbf{0} | l_z : \mathbf{0} : s_z). \quad (21)$$

Observe in (21) that there are zero components $\mathbf{0}$ within the vector $(l_x : s_x : \mathbf{0})$ and $(l_z : \mathbf{0} : s_z)$. This is because the measurements performed on the auxiliary qubits in the Z basis make the auxiliary qubits inaccessible in the X basis and vice versa.

Therefore, based on the results in (21), the ML decoding process for inverse-encoder-based QSCs may be formulated as finding the most likely logical error operator $l = (l_x|l_z)$,

³The syndrome vector s_x obtained from the measurement using the Z basis is used for decoding the Pauli X errors because the Pauli Z operator is anti-commute with Pauli X operator and vice versa

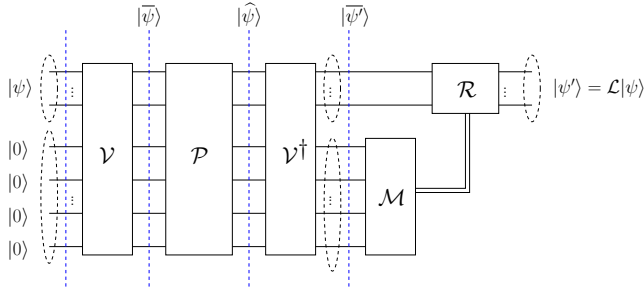


FIGURE 3: The general schematic of the encoding and decoding of QSCs based on the inverse encoding philosophy.

given the syndrome vector extracted from the measurements of the auxiliary qubits $\mathbf{s}_Q = (\mathbf{s}_x|\mathbf{s}_z)$ as follows:

$$\mathbf{l}^{2k,*} = \arg \max_{\mathbf{l}_i^{2k}} p(\mathbf{l}_i^{2k}|\mathbf{s}_Q), \forall \mathbf{l}_i^{2k} \in \mathbb{F}_2^{2k}, \quad (22)$$

where $\mathbf{l}^{2k,*}$ is the most likely logical error operator \mathbf{l}^{2k} that maximizes the conditional probability $p(\mathbf{l}_i^{2k}|\mathbf{s}_Q)$ over all possible values of \mathbf{l}_i^{2k} , so that \mathbf{l}_i^{2k} is an element of \mathbb{F}_2^{2k} .

Thus, the Quantum-GRAND-aided inverse-encoder-based QSC decoder is defined as follows:

- Given the Pauli error operator $\mathbf{E} \in \mathcal{G}_N$ having the binary representation of $e^{2n} = (\mathbf{e}_x^n|\mathbf{e}_z^n)$, calculate $(\hat{\mathbf{l}}_x|\hat{\mathbf{s}}_x|\mathbf{0}_z) = \mathbf{e}_x^n \cdot \mathbf{V}_x^{-1} \cdot \mathbf{M}_z$ and $(\hat{\mathbf{l}}_z|\mathbf{0}_x|\hat{\mathbf{s}}_z) = \mathbf{e}_z^n \cdot \mathbf{V}_z^{-1} \cdot \mathbf{M}_x$.
- Initialize $i = 1$ and set \mathbf{g}_x^n to be the initial guess based on the most likely error vector for the Pauli \mathbf{X} error pattern and calculate $(\mathbf{l}_x|\mathbf{s}_x|\mathbf{0}_z) = \mathbf{g}_x^n \cdot \mathbf{V}_x^{-1} \cdot \mathbf{M}_z$.
- While $\hat{\mathbf{s}}_x \neq \mathbf{s}_x$, increase i by 1 and set \mathbf{g}_x^n to be the next guess based on the next most likely error vector for the Pauli \mathbf{X} error pattern and calculate $(\mathbf{l}_x|\mathbf{s}_x|\mathbf{0}_z) = \mathbf{g}_x^n \cdot \mathbf{V}_x^{-1} \cdot \mathbf{M}_z$.
- The process ends when we find $\hat{\mathbf{s}}_x = \mathbf{s}_x$ in this while loop and the final value of i determines the computational complexity of Pauli \mathbf{X} error decoding.
- Initialize $j = 1$ and set \mathbf{g}_z^n to be the initial guess based on the most likely error vector for the Pauli \mathbf{Z} error pattern and calculate $(\mathbf{l}_z|\mathbf{0}_x|\mathbf{s}_z) = \mathbf{g}_z^n \cdot \mathbf{V}_z^{-1} \cdot \mathbf{M}_x$.
- While $\hat{\mathbf{s}}_z \neq \mathbf{s}_z$, increase j by 1 and set \mathbf{g}_z^n to be the next guess based on the next most likely error vector for the Pauli \mathbf{Z} error pattern and calculate $(\mathbf{l}_z|\mathbf{0}_x|\mathbf{s}_z) = \mathbf{g}_z^n \cdot \mathbf{V}_z^{-1} \cdot \mathbf{M}_x$.
- The process ends when we find $\hat{\mathbf{s}}_z = \mathbf{s}_z$ in this while loop and the final value of j determines the computational complexity of Pauli \mathbf{Z} error decoding.
- The recovery operator $\mathcal{R} \in \mathcal{G}_K$ is constituted by the Pauli operator represented by the binary vector $(\mathbf{l}_x|\mathbf{l}_z)$ and the total complexity is given by $C = i + j$.

To provide a clearer picture of the Quantum GRAND-aided inverse-encoder-based QSC decoder, Fig. 4 portrays the circuit diagram of the quantum encoder \mathcal{V} and of the inverse encoder \mathcal{V}^\dagger for Steane's 7-qubit code based on the PCM given in (15). For the inverse encoder \mathcal{V}^\dagger illustrated in

Fig. 4, the binary matrix representation \mathbf{V}^{-1} is given by

$$\mathbf{V}^{-1} = \left[\begin{array}{c|c} \mathbf{V}_x^{-1} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{V}_z^{-1} \end{array} \right], \quad (23)$$

where \mathbf{V}_x^{-1} and \mathbf{V}_z^{-1} are formulated as

$$\mathbf{V}_x^{-1} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad (24)$$

$$\mathbf{V}_z^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \quad (25)$$

For deeper insights on how to transform the PCM \mathbf{H} of CSS-type QSCs into the quantum encoder \mathcal{V} and the inverse encoder \mathcal{V}^\dagger as well as their associated binary matrices \mathbf{V} and \mathbf{V}^{-1} , we refer enthusiastic readers to [20], [23].

For Steane's 7-qubit code, the first qubit is allocated to the logical qubit, the next three qubits are dedicated to the auxiliary qubits, which are subject to the measurement in the \mathbf{Z} basis and finally, the next three qubits are the auxiliary qubits measured in the \mathbf{X} basis. Therefore, the measurement operator \mathcal{M} can be represented using the binary matrices \mathbf{M}_x and \mathbf{M}_z formulated as follows:

$$\mathbf{M}_x = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad (26)$$

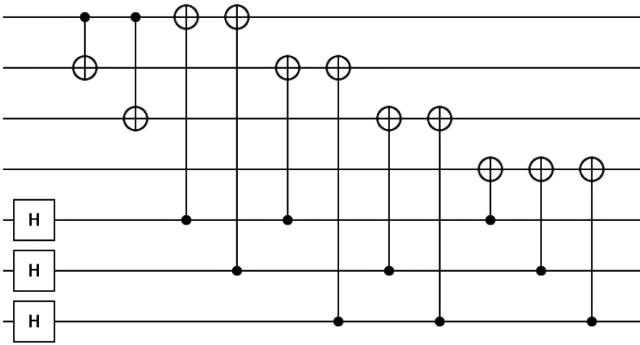
$$\mathbf{M}_z = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (27)$$

Observe that the binary representation of the measurement operator \mathbf{M}_x of (26) is constituted by a specific identity matrix having zero elements for those specific diagonal element $M_{x,ii}$, where the i -th qubit is auxiliary qubit measured in the \mathbf{Z} basis. Similarly, the binary representation of the measurement operator \mathbf{M}_z (27) is represented by a specific identity matrix having the element of $M_{z,jj}$ set to zero, where j -th qubit is auxiliary qubit measured in the \mathbf{X} basis.

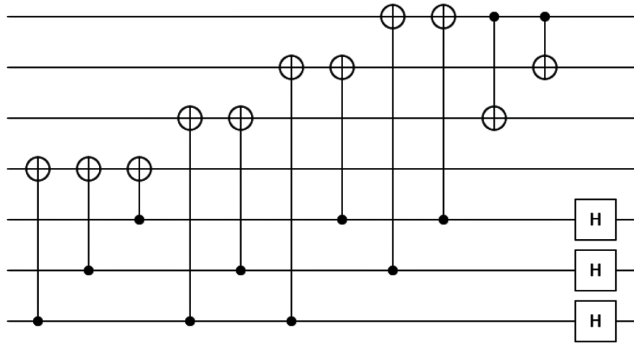
Let us assume that the quantum Pauli channel \mathcal{P} induces

TABLE 2: Syndrome values and the associated error-recovery operator \mathcal{R} .

Error operator P	Syndrome s_x	Error recovery \mathcal{R}	Error operator P	Syndrome s_z	Error recovery \mathcal{R}
$IIIIIII$	(0 0 0)	I	$IIIIIII$	(0 0 0)	I
$XIIIIII$	(1 1 0)	X	$ZIIIIII$	(1 1 0)	Z
$IXIIIII$	(1 0 0)	I	$IZIIIII$	(1 0 1)	Z
$IIXIIII$	(0 1 0)	I	$IIZIIII$	(0 1 1)	Z
$IIIXIII$	(0 0 1)	I	$IIIZIII$	(1 1 1)	I
$IIIXII$	(0 1 1)	X	$IIIZII$	(1 0 0)	I
$IIIIIXI$	(1 0 1)	X	$IIIIZI$	(0 1 0)	I
$IIIIIX$	(1 1 1)	I	$IIIIIZ$	(0 0 1)	I



(a) The quantum encoder \mathcal{V} .



(b) The inverse-encoder \mathcal{V}^\dagger .

FIGURE 4: The quantum encoder and inverse-encoder of Steane's 7-qubit code.

an error pattern of $E = IZIIIXII$. Thus, by using the Pauli-to-binary mapping of (6) and the syndrome calculation of (21), we obtain $s_x = (0 1 1)$ and $s_z = (1 0 1)$. Relying on these syndrome vectors, GRAND will generate the error pattern commencing from the most likely to the least likely and evaluates the syndrome vector. This evaluation process will be terminated when the decoder finally finds the specific error pattern that produces the same syndrome vector as \hat{s}_x and \hat{s}_z . In this example, GRAND will find from Table 2 the Pauli X error pattern after six evaluations ($i = 6$) and the Pauli Z error pattern after three evaluations ($j = 3$). Thus, the total complexity of GRAND in this example is given by $C = i + j = 6 + 3 = 9$.

In contrast to the GRAND simulation used for stabilizer-measurement-based QSC decoding, the observation of errors is carried out for the quantum state $|\psi'\rangle$ after the inverse encoder \mathcal{V}^\dagger and error recovery operator \mathcal{R} are applied, as shown Fig. 3. For the inverse-encoder-based QSC decoder, we declare a quantum block error for every instance, when we find $(\hat{l}_x|\hat{l}_z) \neq (l_x|l_z)$. Furthermore, instead of performing normalization of the QBLER performance using (19), we are able to measure the actual QBLER per logical qubits. More specifically, the number of errors in the logical qubits can be defined as

$$\text{wt}\{(\hat{l}_x \oplus l_x) \vee (\hat{l}_z \oplus l_z)\}, \quad (28)$$

where $\text{wt}\{\cdot\}$ denotes the Hamming weight of a vector, \oplus represents the modulo-2 addition, and \vee denotes the bit-wise logical OR operation. Therefore, the QBLER per logical qubits can be calculated as the ratio between the total number of errors divided by the total number of logical qubits simulated.

V. RESULTS AND DISCUSSIONS

In this section, we present our Monte-Carlo simulation results for Quantum-GRAND-aided QSC decoding relying on both decoding philosophies represented in Section IV. To evaluate the decoding performance, we utilize the quantum depolarizing channel represented by the N -tuple Pauli operator $E \in \mathcal{G}_N$, which is characterized by the depolarizing probability p . To elaborate a little further, each qubit within the N physical qubits may independently experience a Pauli X error, a Pauli Z error, or a Pauli Y error, where the probability of each qubit experiencing one of these errors is given by p_x , p_z , and p_y , respectively. Thus, we have $p_x + p_z + p_y = p$ and $p_x = p_z = p_y = p/3$. To demonstrate the generic nature of our solution, we utilize quantum BCH codes for characterizing the Quantum-GRAND-aided stabilizer-measurement-based decoder and quantum polar codes for the Quantum-GRAND-aided inverse-encoder-based decoder.

A. QUANTUM BCH CODES

In this treatise, we consider the dual-containing CSS-type quantum BCH codes, whose PCM H is taken from the primitive narrow-sense classical BCH codes. More specifically,

the PCM of classical binary BCH codes \mathbf{H} can be expressed in the form of

$$\mathbf{H}_{\text{BCH}} = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \dots & \alpha^{n-1} \\ \alpha^0 & (\alpha^3) & (\alpha^3)^2 & \dots & (\alpha^3)^{n-1} \\ \alpha^0 & (\alpha^5) & (\alpha^5)^2 & \dots & (\alpha^5)^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^0 & (\alpha^{2t-1}) & (\alpha^{2t-1})^2 & \dots & (\alpha^{2t-1})^{n-1} \end{bmatrix}, \quad (29)$$

where the entries α^i of the PCM \mathbf{H} are the elements of $GF(2^m)$ written in binary column vector, $n = 2^m - 1$ is the length of classical codewords and $t = \lfloor (d-1)/2 \rfloor$ is the error correction capability of the classical BCH codes. Finally, the PCM of quantum BCH codes takes the form of (11) with $\mathbf{H}_x = \mathbf{H}_z = \mathbf{H}_{\text{BCH}}$. We summarize the quantum BCH codes used in our Monte-Carlo simulation in Table 3.

B. QUANTUM POLAR CODES

Furthermore, we utilize the quantum polar code constructions presented in [22]. The kernel of the quantum polar encoder can be separated into two types, namely the kernel for the Pauli \mathbf{X} matrix – namely the quantum bit-flip channel and the kernel for the Pauli \mathbf{Z} matrix – namely the quantum phase-flip channel. The Pauli \mathbf{Y} matrix can be readily modeled as the combination of the Pauli \mathbf{X} and \mathbf{Z} channel. The kernel of the quantum polar encoder for the Pauli \mathbf{X} matrix is given by

$$\mathbf{G}_{0,x} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}. \quad (30)$$

Therefore, the binary representation of the quantum polar encoder \mathbf{V}_x having $N = 2^m$ physical qubits is given by

$$\mathbf{V}_x = \mathbf{G}_{0,x}^{\otimes m}. \quad (31)$$

By contrast, the kernel of the quantum polar encoder for the Pauli \mathbf{Z} matrix channel is given by

$$\mathbf{G}_{0,z} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \quad (32)$$

Therefore, the binary representation of the quantum polar encoder \mathbf{V}_z having $N = 2^m$ physical qubits is represented by

$$\mathbf{V}_z = \mathbf{G}_{0,z}^{\otimes m}. \quad (33)$$

Furthermore, the kernels of (30) and (32) are used for determining the frozen qubits of the quantum polar encoder. As detailed further in [22], the channel polarization of quantum bit-flip (\mathbf{X}) channels takes place in the reverse order of the channel polarization of quantum phase-flip (\mathbf{Z}) channels. Therefore, the channel capacity of the qubit's index for the quantum phase-flip error can be inferred from the reverse ordered rank of the quantum bit-flip channel.

We utilize the binary erasure channel (BEC) based approximation for determining the location of the frozen (auxiliary) qubits. Explicitly, we used the erasure probability of $\epsilon = 0.5$. It is important to note that, in the idealistic

implementation of quantum polar codes, the location of the auxiliary qubits may be different for a different depolarizing probability value. This also means that the encoder-decoder pair of the quantum polar codes has the perfect knowledge of the quantum channel's depolarizing probability. In this treatise, we are focusing only on the capability of our Quantum-GRAND-aided inverse-encoder-based decoder to decode quantum polar codes. Thus, optimizing the location of the auxiliary qubits will be left for our future works. The rank-ordered qubit's index spanning from the most reliable qubit to the least reliable are in the presence of a quantum bit-flip (\mathbf{X}) channel is portrayed in Table 4. Thus, the rank-ordered qubit's index for quantum phase-flip (\mathbf{Z}) channels can be determined by reverse-ordering the index presented in Table 4.

C. QBLER AND QBLER PER LOGICAL QUBITS

In this section, we present the QBLER and QBLER per logical qubits performance results of both decoding philosophies represented in Section IV, namely the quantum BCH codes for characterizing the Quantum-GRAND-aided stabilizer-measurement-based decoder and the quantum polar codes for the Quantum-GRAND-aided inverse-encoder-based decoder.

As mentioned in Section IV, the QBLER is determined by the ratio of quantum block errors observed to the total number of quantum blocks simulated. Figure 5a shows the performance of various QSCs codes represented by $\mathcal{C}[[N, K, D]]$, as well as having the quantum coding rates r_Q of Table 3, for quantum BCH codes relying on the Quantum-GRAND-aided stabilizer-measurement-based decoder. As shown in Figure 5a, when a fixed number of N physical qubits is considered such as $N = 63$, as in $[[63, 51, 3]]$, $[[63, 39, 5]]$ and $[[63, 27, 7]]$, the higher the minimum distance D , the better the performance becomes. Hence, as expected $[[63, 27, 7]]$ outperforms the $[[63, 51, 3]]$ and $[[63, 39, 5]]$ schemes.

Additionally, Fig. 5b provides performance of the normalized QBLER per logical qubits for the quantum BCH codes, which is calculated using (19). This normalized metric provides a fairer comparison than the QBLER of Fig. 5a. Interestingly, quantum BCH $[[63, 27, 7]]$ and quantum BCH $[[31, 1, 7]]$ have very similar error correction performances, which have however vastly different quantum coding rates of $r_Q = 0.43$ and $r_Q = 0.03$, respectively. Hence, the former is much preferred for practical systems.

Furthermore, Fig. 6a characterizes the performance of quantum polar codes for the Quantum-GRAND-aided inverse-encoder-based decoder. It is important to highlight that the minimum distance D is unknown for the quantum polar codes. Observe in Fig. 6a when the same number of N physical qubits is considered such as $N = 64$, as in $[[64, 32, D]]$, $[[64, 16, D]]$ and $[[64, 8, D]]$, the quantum polar code having a lower quantum coding rates r_Q attains a better error correction performance. The best overall QBLER performance is achieved by the $[[16, 2, D]]$ having a quantum coding rate of $r_Q = 0.125$. Furthermore, we also quantified the QBLER per logical qubit for the quantum polar

TABLE 3: The list of quantum BCH codes considered in this treatise for evaluating the performance of Quantum-GRAND-aided stabilizer-measurement-based decoding using Monte-Carlo simulations.

Power m	Primitive polynomial $p(X)$	Error correction t	Code parameters $[[N, K, D]]$	Classical codes (n, k, d)	Code rate r_Q
3	$1 + X + X^3$	1	$[[7, 1, 3]]$	$(7, 4, 3)$	0.14
4	$1 + X + X^4$	1	$[[15, 7, 3]]$	$(15, 11, 3)$	0.47
5	$1 + X^2 + X^5$	1	$[[31, 21, 3]]$	$(31, 26, 3)$	0.68
		2	$[[31, 11, 5]]$	$(31, 21, 5)$	0.35
		3	$[[31, 1, 7]]$	$(31, 16, 7)$	0.03
6	$1 + X + X^6$	1	$[[63, 51, 3]]$	$(63, 57, 3)$	0.81
		2	$[[63, 39, 5]]$	$(63, 51, 5)$	0.62
		3	$[[63, 27, 7]]$	$(63, 45, 7)$	0.43
7	$1 + X + X^7$	1	$[[127, 113, 3]]$	$(127, 120, 3)$	0.89
		2	$[[127, 99, 5]]$	$(127, 113, 5)$	0.78
		3	$[[127, 85, 7]]$	$(127, 106, 7)$	0.67

TABLE 4: The rank-ordered qubit index spanning from the most reliable to the least reliable qubit in the presence of quantum bit-flip (X) channels used for determining the location of auxiliary qubits in quantum polar codes. For quantum phase-flip (Z) channel, the rank-ordered index of the qubit is reversed.

Number of physical qubits N	Rank-ordered qubit's index i
8	1, 5, 3, 2, 7, 6, 4, 8
16	1, 9, 5, 3, 2, 13, 11, 7, 10, 6, 4, 15, 14, 12, 8, 16
32	1, 17, 9, 5, 3, 2, 25, 21, 13, 19, 11, 18, 7, 10, 29, 6, 27, 4, 23, 26, 15, 22, 14, 20, 12, 8, 31, 30, 28, 24, 16, 32
64	1, 33, 17, 9, 5, 3, 49, 2, 41, 25, 37, 21, 13, 35, 19, 11, 34, 57, 18, 7, 53, 10, 45, 51, 29, 6, 43, 27, 50, 4, 39, 42, 23, 26, 61, 15, 38, 22, 59, 36, 14, 20, 55, 12, 58, 47, 8, 31, 54, 46, 30, 52, 44, 28, 40, 24, 63, 16, 62, 60, 56, 48, 32, 64

codes using the Quantum-GRAND-aided inverse-encoder-based decoder relying on (28). In this context, the best performance is attained by the $[[64, 8, D]]$ scheme associated with $r_Q = 0.125$.

D. COMPLEXITY

In this section, we present the complexity and complexity per logical qubits of both the quantum BCH codes and of the quantum polar codes. As mentioned in Section IV, in both the Quantum-GRAND-aided stabilizer-measurement-based decoder and the Quantum-GRAND-aided inverse-encoder-based decoder, the complexity estimated in terms of the number of guessing i and j , where the total complexity is given by $C = i + j$.

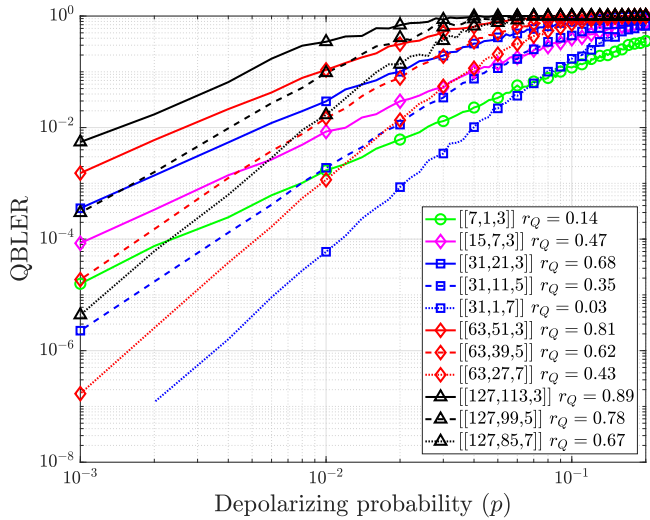
Figure 7a shows the Quantum-GRAND-aided decoder complexity of the quantum BCH codes, which predominantly depends on the N value. More specifically, as shown in the Fig. 7a, a lower N requires fewer number of guesses to find the correct decoded codeword and vice versa. Observe in Fig. 7a, that $[[127, 85, 7]]$ invokes the highest complexity, while $[[7, 1, 3]]$ imposes the lowest complexity. On the other hand, in terms of the complexity per logical qubits, Fig. 7b shows that $[[127, 85, 7]]$ requires the highest complexity per

logical qubits and $[[31, 21, 3]]$ induces the lowest normalized complexity when $p = 10^{-2}$.

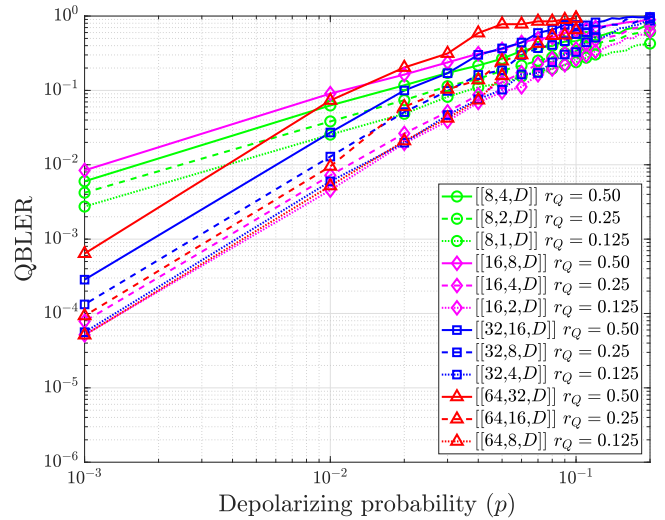
Furthermore, Fig. 8a shows the Quantum-GRAND-aided decoder complexity of the quantum polar codes, which again predominantly depends on the N value. More specifically, as shown in the Fig. 8a, a lower N requires fewer number guesses to find the correct decoded codeword and vice versa. Observe in Fig. 8a, that $[[64, 8, D]]$ requires the highest, while $[[8, 4, D]]$ the lowest complexity. On the other hand, in terms of the complexity per logical qubits, Fig. 8b shows that $[[64, 8, D]]$ requires the highest and $[[8, 4, D]]$ the lowest normalized complexity.

VI. CONCLUSIONS AND FUTURE WORKS

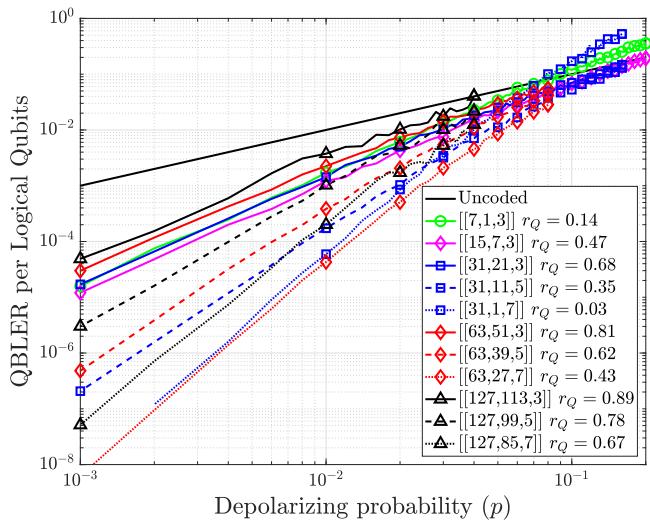
In conclusion, we devised a universal decoding scheme for QSCs by further evolving the GRAND decoding philosophy for employment in the quantum domain. We demonstrated that the decoding scheme conceived may be adopted for two different QSC decoding paradigms, namely for both stabilizer-measurement-based as well as the inverse-encoder-based decoding. We then applied the resultant decoder for both quantum BCH codes and quantum polar codes and quantified their QBLER, QBLER per logical qubits as well as



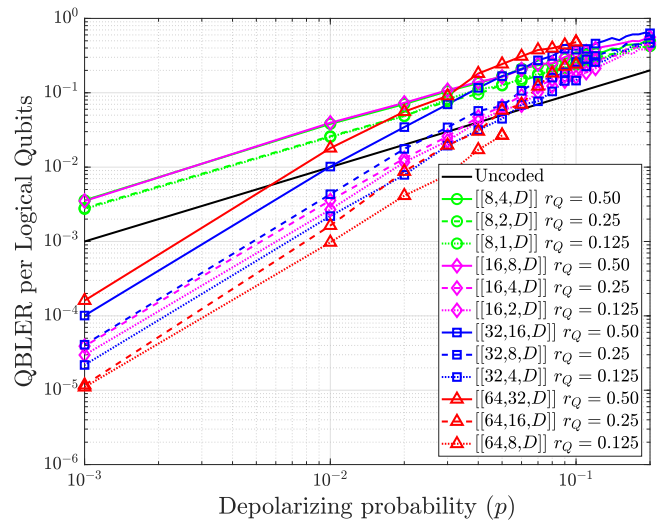
(a) QBLER.



(a) QBLER.



(b) QBLER per logical qubits.



(b) QBLER per logical qubits.

FIGURE 5: The QBLER and QBLER per logical qubits of quantum BCH codes.

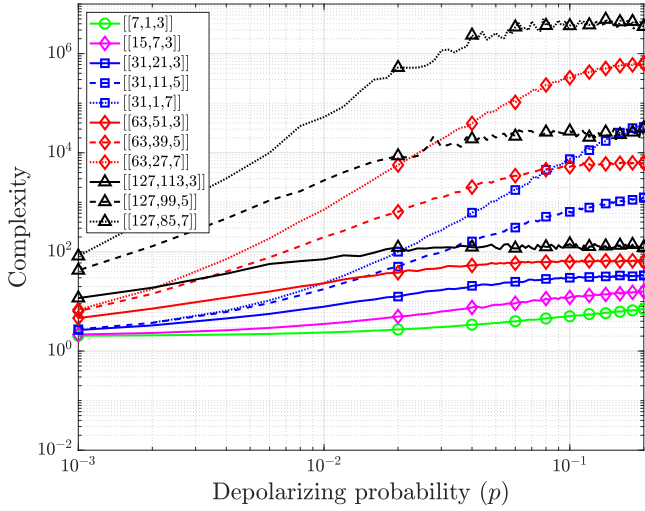
their decoding complexity. We concluded with a parametric study of the associated design trade-offs and provided design guidelines for the implementation of Quantum-GRAND-aided QSC decoders. Based on our QBLER simulations, we demonstrated that when a fixed number of N physical qubits is considered, the higher the minimum distance D , the better the performance becomes. According to the list of quantum BCH codes considered in Table 3, our simulations showed that the quantum BCH $[[63, 27, 7]]$ is much preferred for practical systems upon applying the Quantum-GRAND-aided stabilizer-measurement-based decoder. On the other hand, for quantum polar codes relying on the Quantum-GRAND-aided inverse-encoder-based decoder, the best overall QBLER performance is achieved by the $[[16, 2, D]]$ hav-

FIGURE 6: The QBLER and QBLER per logical qubits of quantum polar codes.

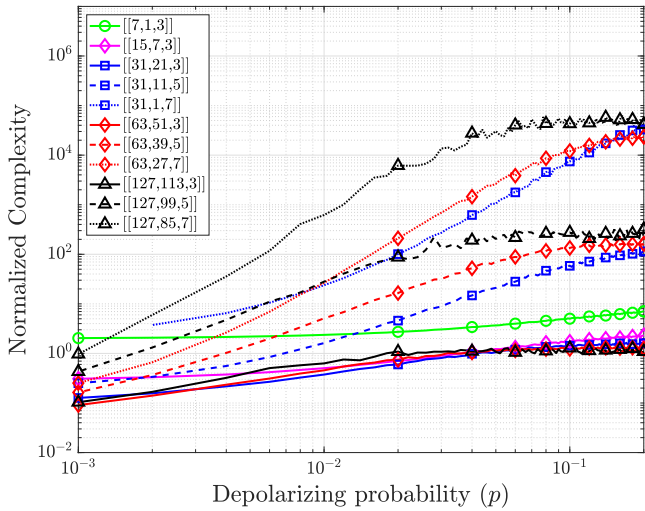
ing quantum coding rate of $r_Q = 0.125$. Furthermore, based on our simulations, the Quantum-GRAND-aided decoder complexity of quantum BCH codes and quantum polar codes is dominated by N , because a lower N requires a lower number of guesses to find the correct decoded codeword. Our future research might also explore the employment of soft-information-aided GRAND [7], [24], [25], which can also be done efficiently from the complexity point of view.

In this treatise, we have concentrated on using Quantum-GRAND-aided QSC decoding for the family of CSS-type QSCs. Our next goal is to expand the proposed decoding method to the family of non-CSS codes, such as the QSCs presented in [15], [26].

Our simulation results confirm the findings presented



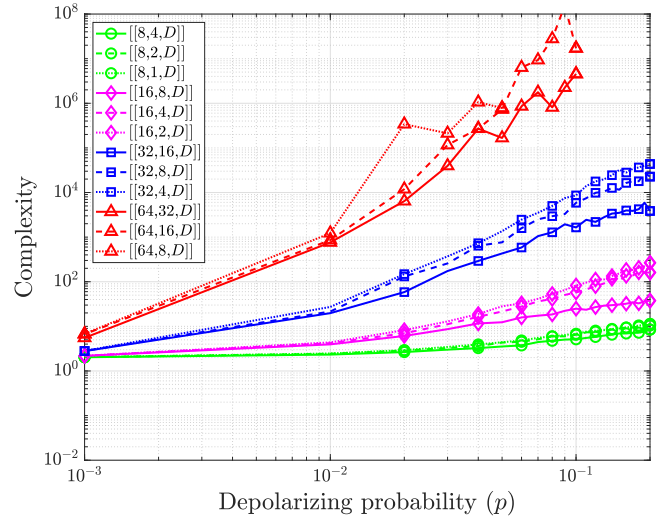
(a) Complexity.



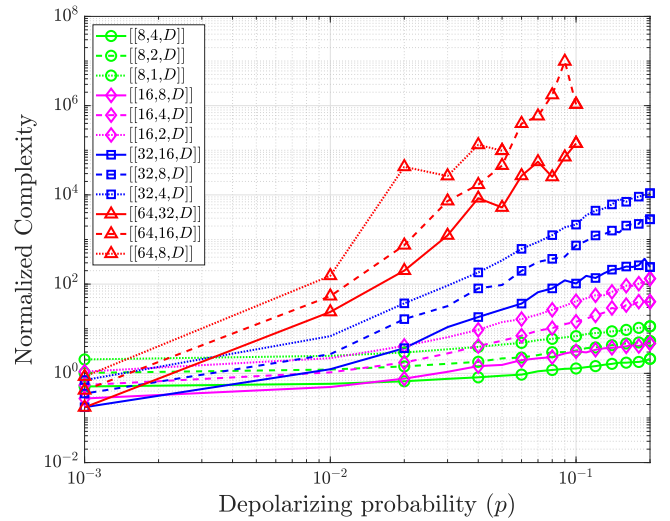
(b) Complexity per logical qubits.

FIGURE 7: The complexity and the normalized complexity of Quantum-GRAND-aided stabilizer-measurement-based decoder for quantum BCH codes.

in [27], namely that quantum polar codes do not offer the best error correction capability in the face of quantum depolarizing channels. This motivates us to explore the use of Quantum-GRAND-aided QSC decoding for more realistic scenarios. Firstly, quantum channels are inherently asymmetric [28]. As a result, the number of frozen qubits in quantum polar codes harnessed for the quantum bit-flip (X) and quantum phase-flip (Z) channels can be made different. Secondly, the encoding and decoding process of QSC is not error-free [29]. Modeling the error proliferation within the quantum error correction circuit is a complex task. Therefore, performing quantum error correction decoding with the knowledge that the quantum encoder and decoder of QSCs are not error-free has been a long-standing challenge



(a) Complexity.



(b) Complexity per logical qubits.

FIGURE 8: The complexity and the normalized complexity of Quantum-GRAND-aided inverse-encoder-based decoder for quantum polar codes.

in fault-tolerant quantum computation. So far, progress has been made mostly for quantum topological error correction codes (QTECCs) [9], because the locality of stabilizer measurements ensures that errors only propagate to a fixed number of qubits, thus minimizing the error proliferation phenomenon. However, quantum polar codes may provide an alternative solution to this problem as a benefit of the systematic structure of the quantum encoder and decoder, making it simpler to model and to predict the error proliferation within the quantum error correction circuit. Therefore, in our future research we will also consider the utilization of Quantum-GRAND-aided QSC decoding for quantum polar codes under realistic fault-tolerance assumptions.

ACKNOWLEDGEMENT

The inspirational comments as well as suggestions of Ken R. Duffy and Muriel Médard are gratefully acknowledged.

REFERENCES

- [1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical review A*, vol. 52, no. 4, 1995.
- [2] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, no. 5, 1996.
- [3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. Sloane, "Quantum error correction and orthogonal geometry," *Physical Review Letters*, vol. 78, no. 3, 1997.
- [4] M. M. Christiansen, K. R. Duffy, F. du Pin Calmon, and M. Médard, "Multi-user guesswork and brute force security," *IEEE Transactions on Information Theory*, vol. 61, no. 12, pp. 6876–6886, 2015.
- [5] M. M. Christiansen and K. R. Duffy, "Guesswork, large deviations, and Shannon entropy," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 796–802, 2012.
- [6] K. R. Duffy, J. Li, and M. Médard, "Capacity-achieving guessing random additive noise decoding," *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4023–4040, 2019.
- [7] K. R. Duffy, M. Médard, and W. An, "Guessing random additive noise decoding with symbol reliability information (SRGRAND)," *IEEE Transactions on Communications*, vol. 70, no. 1, pp. 3–18, 2021.
- [8] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.
- [9] D. Chandra, Z. Babar, H. V. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum coding bounds and a closed-form approximation of the minimum distance versus quantum coding rate," *IEEE Access*, vol. 5, pp. 11557–11581, 2017.
- [10] Z. Babar, D. Chandra, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Duality of quantum and classical error correction codes: Design principles and examples," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 970–1010, 2018.
- [11] J. Roffe, "Quantum error correction: An introductory guide," *Contemporary Physics*, vol. 60, no. 3, pp. 226–245, 2019.
- [12] K. R. Duffy, E. P. Gabhart, and M. Médard, "Quantized guessing random additive noise decoding," arXiv preprint arXiv:2203.13552, 2022.
- [13] A. Rényi, "On measures of entropy and information," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability: Contributions to the Theory of Statistics*, vol. 4, pp. 547–562, University of California Press, 1961.
- [14] A. Riaz, V. Bansal, A. Solomon, W. An, Q. Liu, K. Galligan, K. R. Duffy, M. Médard, and R. T. Yazicigil, "Multi-code multi-rate universal maximum likelihood decoder using GRAND," in *Proceedings of IEEE 47th European Solid-State Circuits Conference (ESSCIRC)*, pp. 239–246, IEEE, 2021.
- [15] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.
- [16] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, 1996.
- [17] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776–2798, 2009.
- [18] A. M. Steane, "Simple quantum error-correcting codes," *Physical Review A*, vol. 54, no. 6, 1996.
- [19] M. Grassl and T. Beth, "Quantum BCH codes," arXiv preprint quant-ph/9910060, 1999.
- [20] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, 2004.
- [21] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Physical Review Letters*, vol. 91, no. 17, 2003.
- [22] Z. Babar, Z. B. K. Egilmez, L. Xiang, D. Chandra, R. G. Maunder, S. X. Ng, and L. Hanzo, "Polar codes and their quantum-domain counterparts," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 123–155, 2019.
- [23] 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, 2019.
- [24] A. Solomon, K. R. Duffy, and M. Médard, "Soft maximum likelihood decoding using GRAND," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2020.
- [25] K. R. Duffy, W. An, and M. Médard, "Ordered reliability bits guessing random additive noise decoding," *IEEE Transactions on Signal Processing*, vol. 70, pp. 4528–4542, 2022.
- [26] D. M. Nguyen and S. Kim, "Quantum stabilizer codes construction from Hermitian self-orthogonal codes over GF(4)," *Journal of Communications and Networks*, vol. 20, no. 3, pp. 309–315, 2018.
- [27] Z. Yi, Z. Liang, and X. Wang, "Quantum polar stabilizer codes based on polarization of pure quantum channel are bad stabilizer codes for quantum computing," arXiv preprint arXiv:2204.11655, 2022.
- [28] 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, 2016.
- [29] D. Chandra, Z. Babar, H. V. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum topological error correction codes are capable of improving the performance of Clifford gates," *IEEE Access*, vol. 7, pp. 121501–121529, 2019.



DARYUS CHANDRA received the B.Eng. and M.Eng. degree in electrical engineering from Universitas Gadjah Mada, Indonesia, in 2013 and 2014, respectively. He obtained his PhD degree with the Next Generation Wireless Group, School of Electronics and Computer Science, University of Southampton, UK, in 2020. He was a postdoctoral research fellow with the Quantum Internet Research Group, University of Naples Federico II, Italy. Currently, he is a postdoctoral research fellow with the Next Generation Wireless Group, School of Electronics and Computer Science, University of Southampton, UK. His research interests include classical and quantum error-correction codes, quantum information, and quantum communications.



ZEYNEP B. KAYKAC EGILMEZ received her dual B.Eng. degrees (Hons.) in Electrical and Electronic Engineering and in Industrial Engineering from the Kırıkkale University, Republic of Turkey, in 2014. She has been awarded an M.Sc degree in wireless communications with distinction from the University of Southampton, Southampton, UK, in November 2017. In June 2022, she received her PhD degree from the University of Southampton in Electronic and Electrical Engineering. Her research interests include channel coding, especially polar coding in wireless communication.



YIFENG XIONG received his B.S. degree in information engineering, and the M.S. degree in information and communication engineering from Beijing Institute of Technology (BIT), Beijing, China, in 2015 and 2018, respectively. He earned his PhD degree with Next-Generation Wireless within the School of Electronics and Computer Science, University of Southampton, UK. Currently he is an Associate Professor at the Beijing University of Post and Telecommunications. His research interests include quantum computation, quantum information theory, graph signal processing, and statistical inference over networks.



PROF SOON XIN NG (S'99-M'03-SM'08) received the B.Eng. degree (First class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow working on collaborative European research projects known as SCOUT, NEWCOM and PHOENIX. Since August 2006, he has been a member of academic staff in the School of Electronics and

Computer Science, University of Southampton. He was involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He was the principal investigator of an EPSRC project on "Cooperative Classical and Quantum Communications Systems". He is currently a Professor of Next Generation Communications at the University of Southampton.

His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes, joint wireless-and-optical-fibre communications, game theory, artificial intelligence and machine learning. He has published over 260 papers and co-authored two John Wiley/IEEE Press books in this field.

He is a Senior Member of the IEEE, a Fellow of the Higher Education Academy in the UK, a Chartered Engineer and a Fellow of the IET. He acted as TPC/track/workshop chairs for various conferences. He serves as an editor of Quantum Engineering. He was a guest editor for the special issues in IEEE Journal on Selected Areas in Communication as well as editors in the IEEE Access and the KSII Transactions on Internet and Information Systems. He is one of the Founders and Officers of the IEEE Quantum Communications & Information Technology Emerging Technical Subcommittee (QCIT-ETC). He was the IEEE ComSoc Representative at the IEEE Nanotechnology Council (NTC) during 2020-2021. He was the programme leader of Electrical and Electronic Engineering (EEE) during 2018 – 2021 and has been the ECS Doctoral Programme Director since 2021, at the University of Southampton.

...



PROF LAJOS HANZO (Life Fellow, IEEE) received the master's and Doctorate degrees from the Technical University (TU) of Budapest in 1976 and 1983, respectively, the Doctor of Science (D.Sc.) degree from the University of Southampton in 2004, and the joint Honorary Doctorate degree from the TU of Budapest in 2009 and the University of Edinburgh in 2015. He is currently a Foreign Member of the Hungarian Academy of Sciences and the Former Editor-in-Chief of the IEEE Press. He has served several terms as a Governor of both IEEE ComSoc and VTS. He has published more than 2000 contributions at IEEE Xplore, 19 Wiley-IEEE Press books, and has helped the fast-track career of 123 Ph.D. students. Over 40 of them are Professors at various stages of their careers in academia and many of them are leading scientists in the wireless industry. He is also a fellow of the Royal Academy of Engineering (FREng), the IET, and EURASIP. He was a recipient of the 2022 Eric Sumner Field Award.



PROF ROBERT G. MAUNDER has studied with the School of Electronics and Computer Science, University of Southampton, UK, since October 2000. He was awarded a first class honours BEng in Electronic Engineering in July 2003, as well as a PhD in Telecommunications in December 2007. He began a lectureship in November 2007 and was promoted to Associate Professor in March 2013 and to Professor in August 2017. He was awarded Senior Member status of the IEEE in

December 2012, Chartered Engineer status of the IET in November 2013 and Fellow status of the IET in January 2017. Rob's research interests include joint source/channel coding and the holistic design of algorithms and hardware implementations for wireless communications. He has published a number of IEEE papers in these areas. He is the founder and CTO of AccelerComm Ltd, which is commercialising his research as soft-IP.