The Road From Classical to Quantum Codes: A Hashing Bound Approaching Design Procedure

ZUNAIRA BABAR, PANAGIOTIS BOTSINIS, DIMITRIOS ALANIS, SOON XIN NG, AND LAJOS HANZO

School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.

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

ABSTRACT Powerful quantum error correction codes (QECCs) are required for stabilizing and protecting fragile qubits against the undesirable effects of quantum decoherence. Similar to classical codes, hashing bound approaching QECCs may be designed by exploiting a concatenated code structure, which invokes iterative decoding. Therefore, in this paper, we provide an extensive step-by-step tutorial for designing extrinsic information transfer (EXIT) chart-aided concatenated quantum codes based on the underlying quantum-to-classical isomorphism. These design lessons are then exemplified in the context of our proposed quantum irregular convolutional code (QIRCC), which constitutes the outer component of a concatenated quantum code. The proposed QIRCC can be dynamically adapted to match any given inner code using EXIT charts, hence achieving a performance close to the hashing bound. It is demonstrated that our QIRCC-based optimized design is capable of operating within 0.4 dB of the noise limit.

INDEX TERMS Quantum error correction, turbo codes, EXIT charts, hashing bound.

NOMENCLATURE

BCH	Bose-Chaudhuri-Hocquenghem
BIBD	Balanced Incomplete Block Designs
BSC	Binary Symmetric Channel
CCC	Classical Convolutional Code
CSS	Calderbank-Shor-Steane
EA	Entanglement-Assisted
EXIT	EXtrinsic Information Transfer
IRCC	IRregular Convolutional Code
LDGM	Low Density Generator Matrix
LDPC	Low Density Parity Check
MAP	Maximum *A Posteriori*
MI	Mutual Information
PCM	Parity Check Matrix
QBER	Qubit Error rate
QC	Quasi-Cyclic
QCC	Quantum Convolutional Code
QECC	Quantum Error Correction Code
QIRCC	Quantum IRregular Convolutional Code
QLDPC	Quantum Low Density Parity Check
QSC	Quantum Stabilizer Code
QTC	Quantum Turbo Code
RX	Receiver
SISO	Soft-In Soft-Out
SNR	Signal-to-Noise Ratio
TX	Transmitter
WER	Word Error Rate

I. INTRODUCTION

The laws of quantum mechanics provide a promising solution to our quest for miniaturization and increased processing power, as implicitly predicted by Moore's law formulated four decades ago [1]. This can be attributed to the inherent parallelism associated with the quantum bits (qubits). More explicitly, in contrast to the classical bits, which can either assume a value of 0 or 1, qubits can exist in a superposition of the two states.[1] Consequently, while an N-bit classical register can store only a single value, an N-qubit quantum register

[1]The superimposed state of a qubit may be represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\ \rangle$ is called Dirac notation or Ket [2], which is a standard notation for states in quantum physics, while α and β are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$. More specifically, a qubit exists in a continuum of states between $|0\rangle$ and $|1\rangle$ until it is 'measured' or 'observed'. Upon 'measurement' it collapses to the state $|0\rangle$ with a probability of $|\alpha|^2$ and $|1\rangle$ with a probability of $|\beta|^2$.
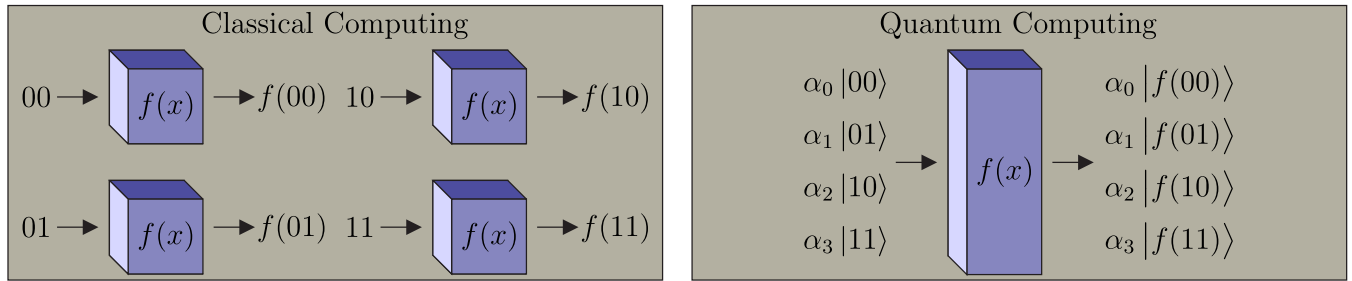
FIGURE 1. Quantum Parallelism: Given a function $f(x)$, which has a regular global structure such that $f(x) : \{0, 1\}^2 \to \{0, 1\}^2$, a classical system requires four evaluations to compute $f(x)$ for all possible $x \in \{00, 01, 10, 11\}$. By contrast, since a 2-qubit quantum register can be in a superposition of all the four states concurrently, i.e. $|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$, quantum computing requires only a single classical evaluation to yield the outcome, which is also in a superposition of all the four possibilities, i.e. $\alpha_0|f(00)\rangle + \alpha_1|f(01)\rangle + \alpha_2|f(10)\rangle + \alpha_3|f(11)\rangle$. However, it is not possible to read all the four states because the quantum register collapses to one of the four superimposed states upon measurement. Nevertheless, we may manipulate the resultant superposition of the four possible states before observing the quantum register for the sake of determining a desired property of the function, as in [5]–[8].

can store all the 2^N states concurrently,[2] allowing parallel evaluations of certain functions with regular global structure at a complexity cost that is equivalent to a single classical evaluation [3], [4], as illustrated in Fig. 1. Therefore, as exemplified by Shor's factorization algorithm [7] and Grover's search algorithm [8], quantum-based computation is capable of solving certain complex problems at a substantially lower complexity, as compared to its classical counterpart. From the perspective of telecommunications, this quantum domain parallel processing seems to be a plausible solution for the massive parallel processing required for achieving joint optimization in large-scale communication systems, e.g. quantum assisted multi-user detection [4], [9], [10] and quantum-assisted routing optimization for self-organizing networks [11]. Furthermore, quantum-based communication is capable of supporting secure data dissemination, where any 'measurement' or 'observation' by an eavesdropper destroys the quantum entanglement,[3] hence intimating the parties concerned [3], [13]. Quantum-based communication has given rise to a new range of security paradigms, which cannot be created using a classical communication system. In this context, quantum key distribution techniques [14], [15], quantum secure direct communication [16], [17] and the recently proposed unconditional quantum location verification [18] are of particular significance.

Unfortunately, a major impediment to the practical realization of quantum computation as well as communication systems is quantum noise, which is conventionally termed as 'decoherence' (loss of the coherent quantum state). More explicitly, decoherence is the undesirable interaction of the qubits with the environment [19], [20]. It may be viewed as the undesirable entanglement of qubits with the environment, which perturbs the fragile superposition of states, thus leading to the detrimental effects of noise. The overall decoherence process may be characterized either by bit-flips or phase-flips or in fact possibly both, inflicted on the qubits [19], as depicted in Fig. 2.[4] The longer a qubit retains its coherent state
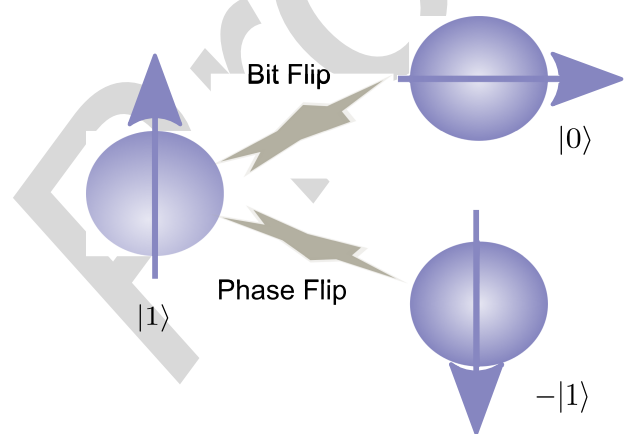
---

[2] A single qubit is essentially a vector in the 2-dimensional Hilbert space. Consequently, an N-qubit composite system, which consists of N qubits, has a 2^N-dimensional Hilbert space, which is the tensor product of the Hilbert space of the individual qubits. The resulting N-qubit state may be generalized as:

$$\alpha_0|00\ldots0\rangle + \alpha_1|00\ldots1\rangle + \ldots + \alpha_{2^N-1}|11\ldots1\rangle,$$

where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1$.

[3] Two qubits are said to be entangled if they cannot be decomposed into the tensor product of the constituent qubits. Let us consider the state $|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$, where both α and β are non-zero. It is not possible to decompose it into two individual qubits because we have:

$$\alpha|00\rangle + \beta|11\rangle \neq (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle),$$

for any choice of α_i and β_i subject to normalization. Consequently, a peculiar link exists between the two qubits such that measuring one qubit also collapses the other, despite their spatial separation. More specifically, if we measure the first qubit of $|\psi\rangle$, we may obtain a $|0\rangle$ with a probability of $|\alpha|^2$ and a $|1\rangle$ with a probability of $|\beta|^2$. If the first qubit is found to be $|0\rangle$, then the measurement of the second qubit will definitely be $|0\rangle$. Similarly, if the first qubit is $|1\rangle$, then the second qubit will also collapse to $|1\rangle$. This mysterious correlation between the two qubits, which doesn't exist in the classical world, is called entanglement. It was termed 'spooky action at a distance' by Einstein [12].

FIGURE 2. Quantum decoherence characterized by bit and phase flips. *The vertical polarization represents the state* $|1\rangle$, *while the horizontal polarization represents the state* $|0\rangle$.

---

[4] A qubit may be realized in different ways, e.g. two different photon polarizations, different alignments of a nuclear spin, two electronic levels of an atom or the charge/current/energy of a Josephson junction.

(this period is known as the coherence time), the better. This may be achieved with the aid of Quantum Error Correction codes (QECCs), which also rely on the peculiar phenomenon of entanglement - hence John Preskill eloquently pointed out that we are ''fighting entanglement with entanglement'' [21]. More explicitly, analogously to the classical channel coding techniques, QECCs rectify the impact of quantum noise (bit and phase flips) for the sake of ensuring that the qubits retain their coherent quantum state with a high fidelity,[5] thus in effect beneficially increasing the coherence time of the unperturbed quantum state. This has been experimentally demonstrated in [23]–[25].

Similar to the family of classical error correction codes [26], [27], which aim for operating close to Shannon's capacity limit, QECCs are designed to approach the quantum capacity [28]–[30], or more specifically the hashing bound, which is a lower bound of the achievable quantum capacity. A significant amount of work has been carried out over the last few decades to achieve this objective. However, the field of quantum error correction codes is still not as mature as that of their classical counterparts. Recently, inspired by the family of classical near-capacity concatenated codes, which rely on iterative decoding schemes, see [31], [32], substantial efforts have been invested in [33]–[35] to construct comparable quantum codes. In the light of this increasing interest in conceiving hashing bound approaching concatenated quantum code design principles, the contributions of this paper are:

1) *We survey the evolution towards constructing hashing bound approaching concatenated quantum codes with the aid of EXtrinsic Information Transfer (EXIT) charts. More specifically, to bridge the gap between the classical and quantum channel coding theory, we provide insights into the transformation from the family of classical codes to the class of quantum codes.*

2) *We propose a generically applicable structure for Quantum Irregular Convolutional Codes (QIRCCs), which can be dynamically adapted to a specific application scenario for the sake of facilitating hashing bound approaching performance. This is achieved with the aid of the EXIT charts of [35].*

3) *More explicitly, we provide a detailed design example by constructing a 10-subcode QIRCC and use it as an outer code in concatenation with the non-catastrophic and recursive inner convolutional code of [34] and [36]. Our QIRCC-based optimized design outperforms both the design of [34], as well as the exhaustive-search based optimized design of [35].*

This paper is organized as follows. We commence by outlining our design objectives in Section II. We then provide a comprehensive historical overview of QECCs in Section III. We detail the underlying stabilizer formalism in Section IV by providing insights into constructing quantum stabilizer codes by cross-pollinating their design with the aid of the

well-known classical codes. We then proceed with the design of concatenated quantum codes in Section V, with a special emphasis on their code construction as well as on their decoding procedure. In Section VI, we will detail the EXIT-chart aided code design principles, providing insights into the application of EXIT charts for the design of quantum codes. We will then present our proposed QIRCC design example in Section VII, followed by our simulation results in Section VIII. Finally, our conclusions and design guidelines are offered in Section IX.

II. DESIGN OBJECTIVES

Meritorious families of quantum error correction codes can be derived from the known classical codes by exploiting the underlying quantum-to-classical isomorphism, while also taking into account the peculiar laws of quantum mechanics. This transition from the classical to the quantum domain must address the following challenges [13]:

- **No-Cloning Theorem:** Most classical codes are based on the transmission of multiple replicas of the same bit, e.g. in a simple rate-1/3 repetition code each information bit is transmitted thrice. This is not possible in the quantum domain according to the no-cloning theorem [37], which states that an arbitrary unknown quantum state cannot be copied/cloned.[6]

- **Continuous Nature of Quantum Errors:** In contrast to the classical errors, which are discrete with bit-flip being the only type of error, a qubit may experience both a bit error as well as a phase error or in fact both, as depicted in Fig. 2. These impairments have a continuous nature and the erroneous qubit may lie anywhere on the surface of the Bloch sphere.[7]

- **Qubits Collapse Upon Measurement:** 'Measurement' of the received bits is a vital step representing a hard-decision operation in the field of classical error correction, but this is not feasible in the quantum domain, since qubits collapse to classical bits upon measurement.

In a nutshell, a classical (n, k) binary code is designed to protect discrete-valued message sequences of length k by encoding them into one of the 2^k discrete codewords of length n. By contrast, since a quantum state of k qubits

---

[5]Fidelity is a measure of closeness of two quantum states [22].

[6]No-cloning theorem is a direct consequence of the linearity of transformations. Let us assume that U is a copying operation, which maps the arbitrary states $|\psi\rangle$ and $|\phi\rangle$ as follows:

$$U|\psi\rangle = |\psi\rangle \otimes |\psi\rangle, \quad U|\phi\rangle = |\phi\rangle \otimes |\phi\rangle.$$

Since the transformation U must be linear, we should have:

$$U(|\psi\rangle + |\phi\rangle) = U|\psi\rangle + U|\phi\rangle = |\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle.$$

However,

$$|\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle \neq (|\psi\rangle + |\phi\rangle) \otimes (|\psi\rangle + |\phi\rangle).$$

[7]A qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, whose orthogonal basis are $|0\rangle$ and $|1\rangle$, can be visualized in $3D$ as a unique point on the surface of a sphere (with unit radius) called Bloch sphere [13].

is specified by 2^k continuous-valued complex coefficients, quantum error correction aims for encoding a k-qubit state into an n-qubit state, so that all the 2^k complex coefficients can be perfectly restored [38]. For example, let $k = 2$, then the 2-qubit information word $|\psi\rangle$ is given by:

$$|\psi\rangle = \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle. \quad (1)$$

Consequently, the error correction algorithm would aim for correctly preserving all the four coefficients, i.e. α_0, α_1, α_2 and α_3. It is interesting to note here that although the coefficients α_0, α_1, α_2 and α_3 are continuous in nature, yet the entire continuum of errors can be corrected, if we can correct a discrete set of errors, i.e. bit (Pauli-**X**),[8] phase (Pauli-**Z**) as well as both (Pauli-**Y**) errors inflicted on either or both qubits [13]. This is because measurement results in collapsing the entire continuum of errors to a discrete set. More explicitly, for $|\psi\rangle$ of Eq. (1), the discrete error set is as follows:

$$\{ \textbf{IX}, \textbf{IZ}, \textbf{IY}, \textbf{XI}, \textbf{XX}, \textbf{XZ}, \textbf{XY}, \textbf{ZI}, \textbf{ZX}, \textbf{ZZ},$$
$$\textbf{ZY}, \textbf{YI}, \textbf{YX}, \textbf{YZ}, \textbf{YY} \}. \quad (2)$$

However, the errors **X**, **Y** and **Z** may occur with varying frequencies. In this paper, we will focus on the specific design of codes conceived for mitigating the deleterious effects of the quantum depolarizing channel, which has been extensively investigated in the context of QECCs [38]–[40]. Briefly, a depolarizing channel, which is characterized by the probability p, inflicts an error $\mathcal{P} \in \mathcal{G}_n$ on n qubits,[9] where each qubit may independently experience either a bit flip (**X**), a phase flip (**Z**) or both (**Y**) with a probability of $p/3$.

An ideal code $\mathcal{C}$ designed for a depolarizing channel may be characterized in terms of the channel's depolarizing probability p and its coding rate R_Q. Here the coding rate R_Q is measured in terms of the number of qubits transmitted per channel use, i.e. we have $R_Q = k/n$, where k and n are the lengths of the information word and codeword, respectively. Analogously to Shannon's classical capacity, the relationship between p and R_Q for the depolarizing channel is defined by the hashing bound, which sets a lower limit on the achievable quantum capacity.[10] The hashing bound is given by [34], [43]:

$$C_Q(p) = 1 - H_2(p) - p \log_2(3), \quad (3)$$

where $H_2(p)$ is the binary entropy function. More explicitly, for a given p, if a random code $\mathcal{C}$ of a sufficiently long codeword-length is chosen such that its coding rate obeys $R_Q \leq C_Q(p)$, then $\mathcal{C}$ may yield an infinitesimally low Qubit Error Rate (QBER) for a depolarizing probability of p. It must be noted here that intuitively a low QBER corresponds to a high fidelity between the transmitted and the decoded quantum state. More explicitly, for a given value of p, $C_Q(p)$ gives the hashing limit on the coding rate. Alternatively, for a given coding rate R_Q, where we have $R_Q = C_Q(p^*)$, p^* gives the hashing limit on the channel's depolarizing probability. In duality to the classical domain, this may also be referred to as the noise limit. An ideal quantum code should be capable of ensuring reliable transmission close to the noise limit p^*. Furthermore, for any arbitrary depolarizing probability p, its discrepancy with respect to the noise limit p^* may be computed in decibels (dB) as follows [34]:

$$\text{Distance from hashing bound} \triangleq 10 \times \log_{10}\left(\frac{p^*}{p}\right). \quad (4)$$

Consequently, our quantum code design objective is to minimize the discrepancy with respect to the hashing bound, thereby yielding a hashing bound approaching code design.

It is pertinent to mention here the Entanglement-Assisted (EA) regime of [44]–[47], where the entanglement-assisted code $\mathcal{C}$ is characterized by an additional parameter c. Here c is the number of entangled qubits pre-shared between the transmitter and the receiver, thus leading to the terminology of being entanglement-assisted.[11] It is assumed furthermore that these pre-shared entangled qubits are transmitted over a noiseless quantum channel. The resultant EA hashing bound is given by [34], [48]:

$$C_Q(p) = 1 - H_2(p) - p \log_2(3) + \text{E}, \quad (5)$$

where the so-called entanglement consumption rate is $\text{E} = \frac{c}{n}$. Furthermore, the value of c may be varied from 0 to a maximum of $(n - k)$. For the family of maximally entangled codes associated with $c = (n - k)$, the EA hashing bound of Eq. (5) is reduced to [34], [48]:

$$C_Q(p) = 1 - \frac{H_2(p) - p \log_2(3)}{2}. \quad (6)$$

---

[8] A qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ may be represented as $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ in vector notation. Consequently, **I**, **X**, **Y** and **Z** Pauli operators (or gates), which act on a single qubit, are defined as follows:

$$\textbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \textbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \textbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \textbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where the **X**, **Y** and **Z** operators anti-commute with each other. The output of a Pauli operator may be computed using matrix multiplication, e.g.:

$$\textbf{X}(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta|0\rangle + \alpha|1\rangle.$$

[9] A single qubit Pauli group $\mathcal{G}_1$ is a group formed by the Pauli matrices **I**, **X**, **Y** and **Z**, which is closed under multiplication. Therefore, it consists of all the Pauli matrices together with the multiplicative factors ± 1 and $\pm i$, i.e. we have:

$$\mathcal{G}_1 \equiv \{\pm\textbf{I}, \pm i\textbf{I}, \pm\textbf{X}, \pm i\textbf{X}, \pm\textbf{Y}, \pm i\textbf{Y}, \pm\textbf{Z}, \pm i\textbf{Z}\}.$$

The general Pauli group $\mathcal{G}_n$ is an n-fold tensor product of $\mathcal{G}_1$.

[10] Quantum codes are inherently degenerate in nature because different errors may have the same impact on the quantum state. For example, let $|\psi\rangle = |00\rangle + |11\rangle$. Both errors **IZ** and **ZI** acting on $|\psi\rangle$ yield the same corrupted state, i.e. $(|00\rangle - |11\rangle)$, and are therefore classified as degenerate errors. Due to this degenerate nature of the channel errors, the ultimate capacity of quantum channel can be higher than that defined by the hashing bound [41], [42]. However, none of the codes known to date outperform the hashing bound at practically feasible frame lengths.

[11] A quantum code without pre-shared entanglement, i.e. $c = 0$, may be termed as an unassisted quantum code. EA quantum codes will be discussed in detail in Section IV-E.
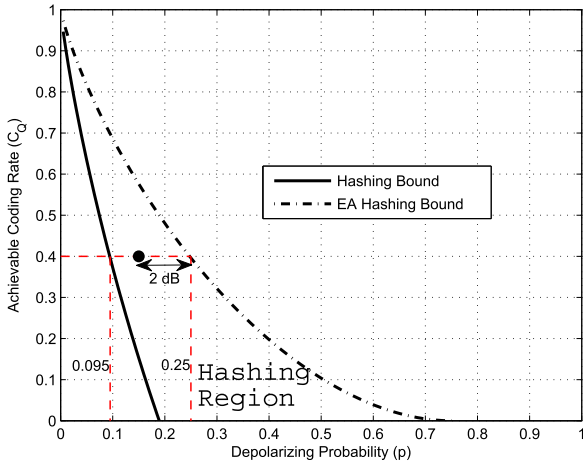
FIGURE 3. Unassisted and EA hashing bounds characterized by Eq. (3) and Eq. (6), respectively, for the quantum depolarizing channel. The region enclosed by these two bounds, which is labeled the hashing region, defines the capacity for varying number of pre-shared entangled qubits (c). At $R_Q = 0.4$, the unassisted hashing bound gives a noise limit of $p^* = 0.095$, while the maximally entangled hashing bound increases the limit to $p^* = 0.25$. The circle represents a maximally entangled code with $R_Q = 0.4$, which ensures reliable transmission for $p \leq 0.15$, thus operating at a distance of 2 dB from the noise limit.

Therefore, the resultant hashing region of the EA communication is bounded by Eq. (3) and Eq. (6), which is also illustrated in Fig. 3. To elaborate a little further, let us assume that the desired coding rate is $R_Q = 0.4$. Then, as gleaned from Fig. 3, the noise limit for the 'unassisted' quantum code is around $p^* = 0.095$, which increases to around $p^* = 0.25$ with the aid of maximum entanglement, i.e. we have $E = 1 - R_Q = 0.6$. Furthermore, $0 < E < 0.6$ will result in bearing noise limits in the range of $0.095 < p^* < 0.25$. Let us assume furthermore that we design a maximally entangled code $\mathcal{C}$ for $R_Q = 0.4$, so that it ensures reliable transmission for $p \leq 0.15$. Based on Eq. (4), the performance of this code (marked with a circle in Fig. 3) is around $[10 \times \log 10(\frac{0.25}{0.15})] = 2$ dB away from the noise limit. We may approach the noise limit more closely by optimizing a range of conflicting design challenges, which are illustrated in the stylized representation of Fig. 4. For example, we may achieve a lower QBER by increasing the code length. However, this in turn incurs longer delays. Alternatively, we may resort to more complex code designs for reducing the QBER, which may also be reduced by employing codes having lower coding rates or higher entanglement consumption rates, thus requiring more transmitted qubits or entangled qubits. Hence striking an appropriate compromise, which meets these conflicting design challenges, is required.

III. HISTORICAL OVERVIEW OF QUANTUM ERROR CORRECTION CODES

A major breakthrough in the field of quantum information processing was marked by Shor's pioneering work on quantum error correction codes, which dispelled the notion that conceiving QECCs was infeasible due to the existence of the no-cloning theorem. Inspired by the classical 3-bit
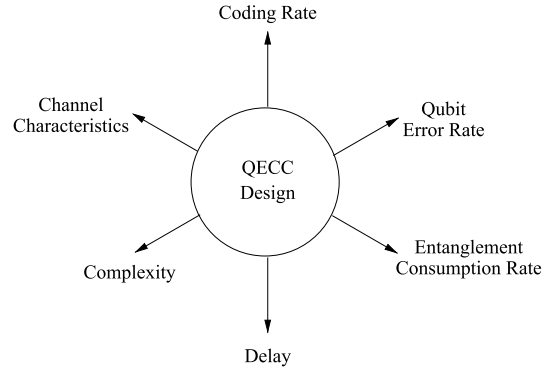

FIGURE 4. Stylized illustration of the conflicting design challenges, which are involved in the design of quantum codes.

repetition codes, Shor conceived the first quantum code in his seminal paper [19], which was published in 1995. The proposed code had a coding rate of 1/9 and was capable of correcting only single qubit errors. This was followed by Calderbank-Shor-Steane (CSS) codes, invented independently by Calderbank and Shor [49] as well as by Steane [50], [51], which facilitated the design of good quantum codes from the known classical binary linear codes. More explicitly, CSS codes may be defined as follows:

An $[n, k_1 - k_2]$ CSS code, which is capable of correcting t bit errors as well as phase errors, can be constructed from classical linear block codes $C_1(n, k_1)$ and $C_2(n, k_2)$, if $C_2 \subset C_1$ and both C_1 as well as the dual[12] of C_2, i.e. $C_2^\perp$, can correct t errors. Here, C_1 is used for correcting bit errors, while $C_2^\perp$ is used for phase-error correction.

Therefore, with the aid of CSS construction, the overall problem of finding good quantum codes was reduced to finding good dual-containing[13] or self-orthogonal classical codes. Following these principles, the classical [7, 4, 3] Hamming code was used to design a 7-qubit Steane code [51] having a coding rate of 1/7, which is capable of correcting single isolated errors inflicted on the transmitted codewords. Finally, Laflamme *et al.* [52] and Bennett *et al.* [43] independently proposed the optimal single error correcting code in 1996, which required only 4 redundant qubits.

Following these developments, Gottesman formalized the notion of constructing quantum codes from the classical binary and quaternary codes by establishing the theory of Quantum Stabilizer Codes (QSCs) [53] in his Ph.D thesis [54]. In contrast to the CSS construction, the stabilizer formalism defines a more general class of quantum codes, which imposes a more relaxed constraint than the CSS codes. Explicitly, the resultant quantum code structure can either assume a CSS or a non-CSS (also called unrestricted) structure, but it has to meet the

---

[12]If G and H are the generator and parity check matrices for any linear block code C, then its dual code $C^\perp$ is a unique code with H^T and G^T as the generator and parity check matrices respectively.

[13]Code C with parity check matrix H is said to be dual-containing if it contains its dual code $C^\perp$, i.e. $C^\perp \subset C$ and $HH^T = 0$.

symplectic product criterion.[14] More specifically, stabilizer codes constitute a broad class of quantum codes, which subsumes CSS codes as a subclass and has undoubtedly provided a firm foundation for a wide variety of quantum codes developed, including for example quantum Bose-Chaudhuri-Hocquenghem (BCH) codes [55]–[58], quantum Reed-Solomon codes [59], [60], Quantum Low Density Parity Check (QLDPC) codes [38], [61]–[63], Quantum Convolutional Codes (QCCs) [64]–[67], Quantum Turbo Codes (QTCs) [33], [39] as well as quantum polar codes [40], [68], [69]. These major milestones achieved in the history of quantum error correction codes are chronologically arranged in Fig. 5. Let us now look deeper into the development of QCCs, QLDPC codes and QTCs, which have been the prime focus of most recent research both in the classical as well as in the quantum domain.
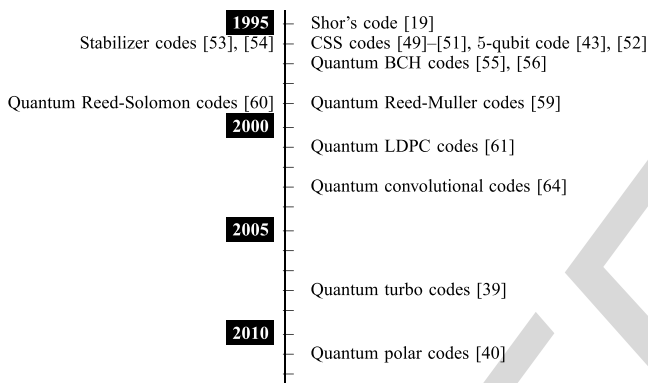

FIGURE 5. Major milestones achieved in the history of quantum error correction codes.

The inception of QCCs dates back to 1998. Inspired by the higher coding efficiencies of Classical Convolutional Codes (CCCs) as compared to the comparable block codes and the low latency associated with the online encoding and decoding of CCCs [70], Chau conceived the first QCC in [71]. He also generalized the classical Viterbi decoding algorithm for the class of quantum codes in [72], but he overlooked some crucial encoding and decoding aspects. Later, Ollivier and J.-P. Tillich [64], [65] revisited the class of stabilizer-based convolutional codes. Similar to the classical Viterbi decoding philosophy, they also conceived a look-up table based quantum Viterbi algorithm for the maximum likelihood decoding of QCCs, whose complexity increases linearly with the number of encoded qubits. Ollivier *et al.* also derived the corresponding online encoding and decoding circuits having complexity which increased linearly with the number of encoded qubits. Unfortunately, their proposed rate-1/5 single-error correcting QCC did not provide any performance or decoding complexity gain over the rate-1/5 single-error correcting block code of [52]. Pursuing this line of research, Almeida *et al.* [73] constructed a rate-1/4 single-error correcting Shor-type concatenated QCC from a

classical CC(2, 1, 2) and invoked the classical syndrome-based trellis decoding for the quantum domain. Hence, the proposed QCC had a higher coding rate than the QCC of [64] and [65]. However, this coding efficiency was achieved at the cost of a relatively high encoding complexity associated with the concatenated trellis structure. It must be pointed out here that the pair of independent trellises used for decoding the bit and phase errors impose a lower complexity than a large joint trellis would. Finally, Forney and Guha [66] and Forney *et al.* [67] designed rate-$(n - 2)/n$ QCCs comparable to their classical counterparts, thus providing higher coding efficiencies than the comparable block codes. Forney and Guha [66] and Forney *et al.* [67] achieved this by invoking arbitrary classical self-orthogonal rate-$1/n$ $\mathbb{F}_4$-linear and $\mathbb{F}_2$-linear convolutional codes for constructing unrestricted and CSS-type QCCs, respectively. Forney and Guha [66] and Forney *et al.* [67] also conceived a simple decoding algorithm for single-error correcting codes. Both the coding efficiency and the decoding complexity of the aforementioned QCC structures are compared in Table 1. Furthermore, in the spirit of finding new constructions for QCCs, Grassl and Rotteler [74], [75] constructed QCCs using the classical self-orthogonal product codes, while Aly *et al.* explored various algebraic constructions in [76] and [77], where QCCs were derived from classical BCH codes and Reed-Solomon and Reed-Muller codes, respectively. Recently, Pelchat and Poulin made a major contribution to the decoding of QCCs by proposing degenerate Viterbi decoding [78], which runs the Maximum *A Posteriori* (MAP) algorithm [27] over the equivalent classes of degenerate errors, thereby improving the attainable performance. The major contributions to the development of QCCs are summarized in Table 2.

TABLE 1. Comparison of the quantum convolutional code (QCC) structures.

AQ:1

Author(s)	Coding Efficiency	Decoding Complexity
Ollivier and Tillich [64], [65]	Low	Moderate
Almeida and Palazzo [73]	Moderate	Moderate
Forney *et al.* [66], [67]	High	Low

Although convolutional codes provide a somewhat better performance than the comparable block codes, yet they are not powerful enough to yield a capacity approaching performance, when used on their own. Consequently, the desire to operate close to the achievable capacity of Fig. 3 at an affordable decoding complexity further motivated researchers to design beneficial quantum counterparts of the classical LDPC codes [79], which achieve information rates close to the Shannonian capacity limit with the aid of iterative decoding schemes. Furthermore, the sparseness of the LDPC matrix is of particular interest in the quantum domain, because it requires only a small number of interactions per qubit during the error correction procedure, thus facilitating fault-tolerant decoding. Moreover, this sparse nature also makes

---

[14]Further details are given in Section IV-C.

TABLE 2. Major contributions to the development of quantum convolutional codes (QCCs).

Year	Author(s)	Contribution
1998	Chau [71]	The first QCCs were developed. Unfortunately, some important encoding/decoding aspects were ignored.
1999	Chau [72]	Classical Viterbi decoding algorithm was generalized to the quantum domain. However, similar to [71], some crucial encoding/decoding aspects were overlooked.
2003	Ollivier and Tillich [64], [65]	Stabilizer-based convolutional codes and their maximum likelihood decoding using the Viterbi algorithm were revisited to overcome the deficiencies of [71], [72]. Failed to provide better performance or decoding complexity than the comparable block codes.
2004	Almeida and Palazzo [73]	Shor-type concatenated QCC was conceived and classical syndrome trellis was invoked for decoding. A high coding efficiency was achieved at the cost of a relatively high encoding complexity.
2005	Forney *et al.* [66], [67]	Unrestricted and CSS-type QCCs were derived from arbitrary classical self-orthogonal $\mathbb{F}_4$ and $\mathbb{F}_2$ CCCs, respectively, yielding a higher coding efficiency as well as a lower decoding complexity than the comparable block codes.
2005	Grassl and Rotteler [74], [75]	Conceived a new construction for QCCs from the classical self-orthogonal product codes.
2007	Aly *et al.* [76]	Algebraic QCCs dervied from BCH codes.
2008	Aly *et al.* [77]	Algebraic QCCs constructed from Reed-Solomon and Reed-Muller Codes.
2013	Pelchat and Poulin [78]	Degenerate Viterbi decoding was conceived, which runs the MAP algorithm over the equivalent classes of degenerate errors, thereby improving the performance.

QLDPC codes highly degenerate. In this context, Postol [61] conceived the first example of a non-dual-containing CSS-based QLDPC code from a finite geometry based classical LDPC in 2001. However, he did not present a generalized formalism for constructing QLDPC codes from the corresponding classical codes. Later, Mackay *et al.* [38] proposed various code structures (e.g. bicycle codes and unicycle codes) for constructing QLDPC codes from the family of classical dual-containing LDPC codes. Among the proposed constructions, the bicycle codes were found to exhibit the best performance. It was observed that unlike good classical LDPC codes, which have at most a single overlap between the rows of the Parity Check Matrix (PCM), dual-containing QLDPC codes must have an even number of overlaps. This in turn results in many unavoidable length-4 cycles, which significantly impair the attainable performance of the message passing decoding algorithm. Furthermore, the minimum distance of the proposed codes was upper bounded by the row weight. Additionally, Mackay *et al.* also proposed the class of Cayley graph-based dual-containing codes in [80], which were further investigated by Couvreur *et al.* in [81] and [82]. Cayley-graph based constructions yield QLDPC codes whose minimum distance has a lower bound, which is a logarithmic function of the code length, thus the minimum distance can be improved by extending the codeword (or block) length, albeit again, only logarithmically. However, this is achieved at the cost of an increased decoding complexity imposed by the row weight, which also increases logarithmically with the code length. Aly *et al.* contributed to these developments by constructing dual-containing QLDPC codes from finite geometries in [83], while Djordjevic exploited the Balanced Incomplete Block Designs (BIBDs) in [84], albeit neither of these provided any gain over Mackay's bicycle codes. Furthermore, Lou and Garcia-Frias [85], [86] invoked the non-dual-containing CSS structure by using both the generator and the PCM of classical Low Density Generator Matrix (LDGM) based codes. Unfortunately, the proposed LDGM based constructions also suffered from length-4 cycles, which in turn required a modified Tanner graph and code doping for decoding, thereby imposing a higher decoding complexity. The only exceptions to

length-4 cycles were constituted by the class of Quasi-Cyclic (QC) QLDPC codes conceived by Hagiwara and Imai [87], whereby the constituent PCMs of non-dual-containing CSS-type QLDPCs were constructed from a pair of QC-LDPC codes found using algebraic combinatorics. The resultant codes had at minimum girth of 6, but they did not outperform MacKay's bicycle codes conceived in [38]. Hagiwara's design of [87] was extended to non-binary QLDPC codes in [88] and [89], which operate closer to the hashing limit than MacKay's bicycle codes. However, having an upper bounded minimum distance remains a deficiency of this construction and the non-binary nature of the code imposes a potentially high decoding complexity. Furthermore, the performance was still not at par with that of the classical LDPC codes. The concept of QC-QLDPC codes was further extended to the class of spatially-coupled QC codes in [90], which outperformed the 'non-coupled' design of [87] at the cost of a small coding rate loss. The spatially-coupled QC-QLDPC was capable of achieving a performance similar to that of the non-binary QC-LDPC code only when its block length was considerably higher. While all the aforementioned QLDPC constructions were CSS-based, Camara *et al.* [63] were the first authors to conceive non-CSS QLDPC codes. They invoked group theory for deriving QLDPC codes from the classical self-orthogonal quaternary LDPC codes. Later, Tan and Li [91] proposed several systematic constructions for non-CSS QLDPC codes, four of which were based on classical binary QC-LDPC codes, while one was derived from classical binary LDPC-convolutional codes. Unfortunately, the non-CSS constructions of [63] and [91] failed to outperform Mackay's bicycle codes. Since most of the above-listed QLDPC constructions exhibit an upper bounded minimum distance, topological QLDPCs[15] were derived from Kitaev's construction in [92]–[94]. Amidst these activities, which focused on the construction of QLDPC codes, Poulin *et al.* were the first scientists to address the decoding issues of QLDPC codes [95]. As mentioned above, most of the QLDPC codes consist of unavoidable

---

[15]Topological code structures are beyond the scope of this paper.

TABLE 3. Major contributions to the development of iterative quantum codes.

		Year	Author(s)	Code Type	Contribution
QLDPC	Code Construction	2001	Postol [61]	Non-dual-containing CSS	The first example of QLDPC code constructed from a finite geometry based classical code. A generalized formalism for constructing QLDPC codes from the corresponding classical codes was not developed.
		2004	Mackay *et al.* [38]	Dual-containing CSS	Various code structures, e.g. bicycle codes and unicycle codes, were conceived for constructing QLDPC codes from classical dual-containing LDPC codes. Performance impairment due to the presence of unavoidable length-4 cycles was first pointed out in this work. Minimum distance of the resulting codes was upper bounded by the row weight.
		2005	Lou *et al.* [85], [86]	Non-dual-containing CSS	The generator and PCM of classical LDGM codes were exploited for constructing CSS codes. An increased decoding complexity was imposed and the codes had an upper bounded minimum distance.
		2007	Mackay [80]	Dual-containing CSS	Cayley graph-based QLDPC codes were proposed, which had numerous length-4 cycles.
			Camara *et al.* [63]	Non-CSS	QLDPC codes derived from classical self-orthogonal quaternary LDPC codes were conceived, which failed to outperform MacKay's bicycle codes.
			Hagiwara *et al.* [87]	Non-dual-containing CSS	Quasi-cyclic QLDPC codes were constructed using a pair of quasi-cyclic LDPC codes, which were found using algebraic combinatorics. The resultant codes had at least a girth of 6, but they failed to outperform MacKay's constructions given in [38].
		2008	Aly *et al.* [83]	Dual-containing CSS	QLDPC codes were constructed from finite geometries, which failed to outperform Mackay's bicycle codes.
			Djordjevic [84]	Dual-containing CSS	BIBDs were exploited to design QLDPC codes, which failed to outperform Mackay's bicycle codes.
		2010	Tan *et al.* [91]	Non-CSS	Several systematic constructions for non-CSS QLDPC codes were proposed, four of which were based on classical binary quasi-cyclic LDPC codes, while one was derived from classical binary LDPC-convolutional codes. These code designs failed to outperform Mackay's bicycle codes.
		2011	Couvreur *et al.* [81], [82]	Dual-containing CSS	Cayley graph-based QLDPC codes of [80] were further investigated. The lower bound on the minimum distance of the resulting QLDPC was logarithmic in the code length, but this was achieved at the cost of an increased decoding complexity.
			Kasai [88], [89]	Non-dual-containing CSS	Quasi-cyclic QLDPC codes of [87] were extended to non-binary constructions, which outperformed Mackay's bicycle codes at the cost of an increased decoding complexity. Performance was still not at par with the classical LDPC codes and minimum distance was upper bounded.
			Hagiwara *et al.* [90]	Non-dual-containing CSS	Spatially-coupled QC-QLDPC codes were developed, which outperformed the 'non-coupled' design of [87] at the cost of a small coding rate loss. Performance was similar to that of [88], [89], but larger block lengths were required.
	Decoding	2008	Poulin *et al.* [95]		Heuristic methods were developed to alleviate the performance degradation caused by unavoidable length-4 cycles and symmetric degeneracy error.
		2012	Wang *et al.* [96]		Feedback mechanism was introduced in the context of the heuristic methods of [95] to further improve the performance.
QTC	Code Construction	2008	Poulin *et al.* [33], [39]	Non-CSS	QTCs were conceived based on the interleaved serial concatenation of QCCs. QTCs are free from the decoding issue associated with the length-4 cycles and they offer a wider range of code parameters. Degenerate iterative decoding algorithm was also proposed. Unfortunately, QTCs have an upper bounded minimum distance.
		2014	Babar *et al.* [35]	Non-CSS	To dispense with the time-consuming Monte Carlo simulations and to facilitate the design of hashing bound approaching QTCs, the application of classical non-binary EXIT charts of [97] was extended to QTCs.
	Decoding	2014	Wilde *et al.* [34]		The iterative decoding algorithm of [33], [39] failed to yield performance similar to the classical turbo codes. The decoding algorithm was improved by iteratively exchanging the *extrinsic* rather than the *a posteriori* information.

length-4 cycles. In fact, when QLDPC codes are viewed in the quaternary formalism, i.e. GF(4), then they must have length-4 cycles, which emerge from the symplectic product criterion. These short cycles erode the performance of the classic message passing decoding algorithm. Furthermore, the classic message passing algorithm does not take into account the degenerate nature of quantum codes, rather it suffers from it. This is known as the 'symmetric degeneracy error'. Hence, Poulin *et al.* proposed heuristic methods in [95] to alleviate the undesired affects of having short cycles and symmetric degeneracy error, which were further improved in [96]. The major contributions made in the context of QLDPC codes are summarized in Table 3, while the most promising QLDPC construction methods are compared in Table 4.[16]

Pursuing further the direction of iterative code structures, Poulin *et al.* conceived QTCs in [33] and [39], based on the interleaved serial concatenation of QCCs. Unlike QLDPC codes, QTCs offer a complete freedom in choosing the code parameters, such as the frame length, coding rate, constraint length and interleaver type. Moreover, their decoding is not impaired by the presence of length-4 cycles associated with the symplectic criterion. Furthermore, in contrast to QLDPC codes, the iterative decoding invoked for QTCs takes into account the inherent degeneracy associated with quantum codes. However, it was found in [33], [39] and [98] that the constituent QCCs cannot be simultaneously both recursive and noncatastrophic. Since the recursive nature of the inner code is essential for ensuring an unbounded minimum distance,[17] whereas the noncatastrophic nature is a necessary condition to be satisfied for achieving

---

[16]The second column indicates 'short cycles' in the binary formalism. Recall that all QLDPC codes must have short cycles in the quaternary formalism.

[17]Unbounded minimum distance of a code implies that its minimum distance increases almost linearly with the interleaver length.

TABLE 4. Comparison of the quantum low density parity check (QLDPC) code structures.

Code Construction	Short Cycles	Minimum Distance	Delay	Decoding Complexity
Bicycle codes [38]	Yes	Upper Bounded	Standard	Standard
Cayley-graph based codes [80]–[82]	Yes	Increases with the code length	Standard	Increases with the code length
LDGM-based codes [85], [86]	Yes	Upper Bounded	Standard	High
Non-binary quasi-cyclic codes [88], [89]	No	Upper Bounded	Standard	High
Spatially-coupled quasi-cyclic codes [90]	No	Upper Bounded	High	High

decoding convergence to a vanishingly low error rate, the QTCs designed in [33] and [39] had a bounded minimum distance. The QBER performance curves of the QTCs conceived in [33] and [39] also failed to match the classical turbo codes. This issue was dealt with in [34], where the quantum turbo decoding algorithm of [33] was improved by iteratively exchanging the *extrinsic* rather than the *a posteriori* information. Furthermore, in [33], [34], and [39], the optimal components of QTCs were found by analyzing their distance spectra, followed by extensive Monte Carlo simulations for the sake of determining the convergence threshold of the resultant QTC. In order to circumvent this time-consuming approach and to facilitate the design of hashing bound approaching QTCs, the application of classical non-binary EXIT charts [97] was extended to QTCs in [35]. An EXIT-chart aided exhaustive-search based optimized QTC was also presented in [35]. The major contributions made in the domain of quantum turbo codes are summarized in Table 3.

Some of the well-known classical codes cannot be imported into the quantum domain by invoking the aforementioned stabilizer-based code constructions because the stabilizer codes have to satisfy the stringent symplectic product criterion. This limitation was overcome in [44]–[47] with the notion of EA quantum codes, which exploit pre-shared entanglement between the transmitter and receiver. Later, this concept was extended to numerous other code structures, e.g. EA-QLDPC code [99], EA-QCC [100], EA-QTC [34], [36] and EA-polar codes [101]. In [34] and [36], it was also found that entanglement-assisted convolutional codes may be simultaneously both recursive as well as non-catastrophic. Therefore, the issue of bounded minimum distance of QTCs was resolved with the notion of entanglement. Furthermore, EA-QLDPC codes are free from length-4 cycles in the binary formalism, which in turn results in an impressive performance similar to that of the corresponding classical LDPC codes. Hence, the concept of the entanglement-assisted regime resulted in a major breakthrough in terms of constructing quantum codes, whose behaviour is similar to that of the corresponding classical codes. The major milestones achieved in the history of entanglement-assisted quantum error correction codes are chronologically arranged in Fig. 5.

In this contribution, we design a novel QIRCC, which may be used as an outer component in a QTC, or in fact any arbitrary concatenated quantum code structure.

Explicitly, the proposed QIRCC may be invoked in conjunction with any arbitrary inner code (both unassisted as well as entanglement-assisted) for the sake of attaining a hashing bound approaching performance with the aid of the EXIT charts of [35]. More specifically, we construct a 10-subcode QIRCC and use it as the outer code in concatenation with the non-catastrophic and recursive inner convolutional code of [34]. In contrast to the concatenated code of [34], which exhibited a performance within 0.9 dB of the hashing bound, our QIRCC-based optimized design operates within 0.4 dB of the noise limit. Furthermore, at a Word Error Rate (WER) of 10^{-3}, our design outperforms the benchmark designed in [34] by about 0.5 dB. Our proposed design also yields a lower error rate than the exhaustive-search based optimized design of [35].

IV. STABILIZER FORMALISM

Most of the quantum codes developed to date owe their existence to the theory of stabilizer codes, which allows us to import any arbitrary classical binary as well as quaternary code to the quantum domain. Unfortunately, this is achieved at the cost of imposing restrictions on the code structure, which may adversely impact the performance of the code, e.g. as in QLDPC codes and QTCs, which was discussed in Section III. In this section, we will delve deeper into the stabilizer formalism for the sake of ensuring a smooth transition from the classical to the quantum domain.

A. CLASSICAL LINEAR BLOCK CODES

The stabilizer formalism derives its existence from the theory of classical linear block codes. A classical linear block code $C(n, k)$ maps k-bit information blocks onto n-bit codewords. For small values of k and n, this can be readily achieved using a look-up table, which maps the input information blocks onto the encoded message blocks. However, for large values of k and n, the process may be simplified using an $k \times n$ generator matrix G as follows:

$$\bar{x} = xG, \qquad (7)$$

where x and $\bar{x}$ are row vectors for information and encoded messages, respectively. Furthermore, G may be decomposed as:

$$G = (I_k | P), \qquad (8)$$

where I_k is a $(k \times k)$-element identity matrix and P is a $k \times (n-k)$-element matrix. This in turn implies that the first
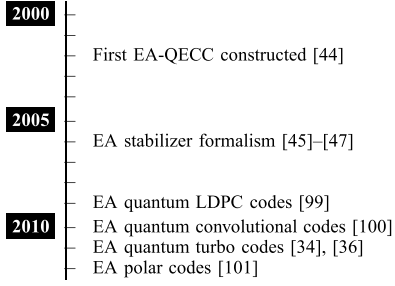
FIGURE 6. Major milestones achieved in the history of entanglement-assisted quantum error correction codes.

AQ:2

588 k bits of the encoded message are information bits, followed
589 by $(n - k)$ parity bits.

590 At the decoder, syndrome-based decoding is invoked,
591 which determines the position of the channel-induced error
592 using the observed syndromes rather than directly acting
593 on the received codewords. More precisely, each generator
594 matrix is associated with an $(n - k) \times n$-element PCM H
595 which is given by:

596 $$H = \left(P^T | I_{n-k} \right), \qquad (9)$$

597 and is defined such that $\bar{x}$ is a valid codeword only if,

598 $$\bar{x} H^T = 0. \qquad (10)$$

599 For a received vector $y = \bar{x} + e$, where e is the error incurred
600 during transmission, the error syndrome of length $(n - k)$ is
601 computed as:

602 $$s = y H^T = (\bar{x} + e) H^T = \bar{x} H^T + e H^T = e H^T, \quad (11)$$

603 which is then used for identifying the erroneous parity bit.

604 Let us consider a simple 3-bit repetition code, which makes
605 three copies of the intended information bit. More precisely,
606 $k = 1$ and $n = 3$. It is specified by the following generator
607 matrix:

608 $$G = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \qquad (12)$$

609 which yields two possible codewords [111] and [000]. At the
610 receiver, a decision may be made on the basis of the majority
611 voting. For example, if $y = [011]$ is received, then we may
612 conclude that the transmitted bit was 1. Alternatively, we
613 may invoke the PCM-based syndrome decoding. According
614 to Eq. (9), the corresponding PCM is given by:

615 $$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \qquad (13)$$

616 It can be worked out that $y H^T = 0$ only for the two valid
617 codewords [111] and [000]. For all other received codewords,
618 at least one of the two syndrome elements is set to 1, e.g. when
619 the first bit is corrupted, i.e. $y = [011]$ or $[100]$, $s = [11]$.
620 Table 5 enlists all the 1-bit errors, which may be identified
621 using this syndrome decoding procedure.

622 This process of error correction using generator and parity
623 check matrices is usually preferred due to its compact nature.

TABLE 5. Single-bit errors along with the corresponding syndromes for the PCM of Eq. (13).

Syndrome (s)	Index of Error
[11]	1
[10]	2
[01]	3

624 Generally, $C(n, k)$ code, which encodes a k-bit information
625 message into an n-bit codeword, would require 2^k n-bit
626 codewords. Thus, it would required a total of $n2^k$ bits to
627 completely specify the code space. By contrast, the aforemen-
628 tioned approach only requires kn bits of the generator matrix.
629 Hence, memory resources are saved exponentially and encod-
630 ing and decoding operations are efficiently implemented.
631 These attractive features of classical block linear codes and
632 the associated PCM-based syndrome decoding [102] have led
633 to the development of quantum stabilizer codes.

B. QUANTUM STABILIZER CODES (QSCs)

635 Let us recall from Section II that qubits collapse to clas-
636 sical bits upon measurement [13]. This prevents us from
637 directly applying the classical error correction techniques for
638 reliable quantum transmission. Inspired by the PCM-based
639 syndrome decoding of classical codes, Gottesman [53], [54]
640 introduced the notion of stabilizer formalism, which facili-
641 tates the design of quantum codes from the classical ones.
642 Analogous to Shor's pioneering 9-qubit code [19], stabilizer
643 formalism overcomes the measurement issue by observing
644 the error syndromes without reading the actual quantum
645 information. More specifically, QSCs invoke the
646 PCM-based syndrome decoding approach of classical linear
647 block codes for estimating the errors incurred during
648 transmission.

649 Fig. 7 shows the general schematic of a quantum com-
650 munication system relying on a quantum stabilizer code for
651 reliable transmission. An $[n, k]$ QSC encodes the information
652 qubits $|\psi\rangle$ into the coded sequence $|\bar{\psi}\rangle$ with the aid of $(n - k)$
653 auxiliary (also called ancilla) qubits, which are initialized to
654 the state $|0\rangle$. The noisy sequence $|\hat{\psi}\rangle = \mathcal{P}|\bar{\psi}\rangle$, where $\mathcal{P}$ is
655 the n-qubit channel error, is received at the receiver (RX),
656 which engages in a 3-step process for the sake of recov-
657 ering the intended transmitted information. More explicitly,
658 RX computes the syndrome of the received sequence $|\hat{\psi}\rangle$
659 and uses it to estimate the channel error $\tilde{\mathcal{P}}$. The recovery
660 operator $\mathcal{R}$ then uses the estimated error $\tilde{\mathcal{P}}$ to restore the
661 transmitted coded stream. Finally, the decoder, or more
662 specifically the inverse encoder, processes the recovered
663 coded sequence $|\tilde{\bar{\psi}}\rangle$, yielding the estimated transmitted
664 information qubits $|\tilde{\psi}\rangle$.

665 *An $[n, k]$ quantum stabilizer code, constructed over a code*
666 *space $\mathcal{C}$, which maps the information word (logical qubits)*
667 *$|\psi\rangle \in \mathbb{C}^{2^k}$ onto the codeword (physical qubits) $|\bar{\psi}\rangle \in \mathbb{C}^{2^n}$,*
668 *where $\mathbb{C}^d$ denotes the d-dimensional Hilbert space, is defined*
669 *by a set of $(n - k)$ independent commuting n-tuple Pauli*
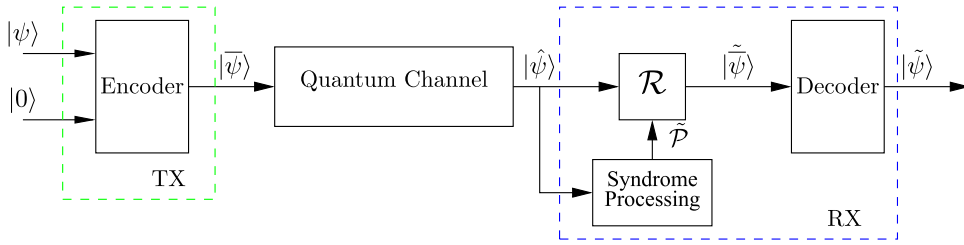670 *operators g_i, for $1 \leq i \leq (n - k)$. The corresponding*

FIGURE 7. System Model: Quantum communication system relying on a quantum stabilizer code.

stabilizer group $\mathcal{H}$ contains both g_i and all the products of g_i for $1 \leq i \leq (n-k)$ and forms an abelian subgroup of $\mathcal{G}_n$. *A unique feature of these operators is that they do not change the state of valid codewords, while yielding an eigenvalue of -1 for corrupted states.*

Let us now elaborate on this definition of the stabilizer code by considering a simple 3-qubit bit-flip repetition code, which is capable of correcting single-qubit bit-flip errors. Since the laws of quantum mechanics do not permit cloning of the information qubit, we cannot encode $|\psi\rangle$ to $(\psi \otimes \psi \otimes \psi)$. Instead, the 3-qubit bit-flip repetition code entangles two auxiliary qubits with the information qubit such that the basis states $|0\rangle$ and $|1\rangle$ are copied thrice in the superposition of basis states of the resulting 3-qubit codeword, i.e. $|0\rangle$ and $|1\rangle$ are mapped as follows:

$$|0\rangle \rightarrow |000\rangle,$$
$$|1\rangle \rightarrow |111\rangle. \tag{14}$$

Consequently, the information word $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is encoded as:

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle. \tag{15}$$

The resultant codeword is stabilized by the operators $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$. Here the term 'stabilize' implies that the valid codewords are not affected by the generators g_1 and g_2 and yield an eigenvalue of $+1$, as shown below:

$$g_1\left[|\overline{\psi}\rangle\right] = \alpha|000\rangle + \beta|111\rangle \equiv |\overline{\psi}\rangle,$$
$$g_2\left[|\overline{\psi}\rangle\right] = \alpha|000\rangle + \beta|111\rangle \equiv |\overline{\psi}\rangle. \tag{16}$$

On the other hand, if a corrupted state $|\hat{\psi}\rangle$ is received, then the stabilizer generators yield an eigenvalue of -1, e.g. let $|\hat{\psi}\rangle = |100\rangle + \beta|011\rangle$ where $\mathcal{P} = \mathbf{XII}$, then we have:

$$g_1\left[|\hat{\psi}\rangle\right] = -\alpha|100\rangle - \beta|011\rangle \equiv -|\hat{\psi}\rangle,$$
$$g_2\left[|\hat{\psi}\rangle\right] = -\alpha|100\rangle - \beta|011\rangle \equiv -|\hat{\psi}\rangle. \tag{17}$$

More specifically, the eigenvalue is -1 if the *n*-tuple Pauli error $\mathcal{P}$ acting on the transmitted codeword $|\overline{\psi}\rangle$ anti-commutes with the stabilizer g_i and it is $+1$ if $\mathcal{P}$ commutes with g_i. Therefore, we have:

$$g_i|\hat{\psi}\rangle = \begin{cases} |\overline{\psi}\rangle, & g_i\mathcal{P} = \mathcal{P}g_i \\ -|\overline{\psi}\rangle, & g_i\mathcal{P} = -\mathcal{P}g_i, \end{cases} \tag{18}$$

where $|\hat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle$. Table 6 enlists the eigenvalues for all possible single-qubit bit-flip errors. The resultant ± 1 eigenvalue gives the corresponding error syndrome *s*, which is 0 for an eigenvalue of $+1$ and 1 for an eigenvalue of -1, as depicted in Table 6.

TABLE 6. Single-qubit bit-flip errors along with the corresponding eigenvalues for 3-qubit bit-flip repetition code.

$|\hat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle$	$g_1|\hat{\psi}\rangle$	$g_2|\hat{\psi}\rangle$	Syndrome (*s*)	Index of Error
$\alpha|100\rangle + \beta|011\rangle$	-1	-1	[11]	1
$\alpha|010\rangle + \beta|101\rangle$	-1	$+1$	[10]	2
$\alpha|001\rangle + \beta|110\rangle$	$+1$	-1	[01]	3

A 3-qubit phase-flip repetition code may be constructed using a similar approach. This is because phase errors in the Hadamard basis $\{|+\rangle, |-\rangle\}$ are similar to the bit errors in the computational basis $\{|0\rangle, |1\rangle\}$. More explicitly, the states $|+\rangle$ and $|-\rangle$ are defined as:

$$|+\rangle \equiv \mathbf{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$
$$|-\rangle \equiv \mathbf{H}|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{19}$$

where $\mathbf{H}$ is a single-qubit Hadamard gate, which is given by [13]:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{20}$$

Therefore, Pauli-$\mathbf{Z}$ acting on the states $|+\rangle$ and $|-\rangle$ yields:

$$\mathbf{Z}|+\rangle = |-\rangle,$$
$$\mathbf{Z}|-\rangle = |+\rangle, \tag{21}$$

which is similar to the operation of Pauli-$\mathbf{X}$ on the states $|0\rangle$ and $|1\rangle$, i.e. we have:

$$\mathbf{X}|0\rangle = |1\rangle,$$
$$\mathbf{X}|1\rangle = |0\rangle. \tag{22}$$

Consequently, analogous to Eq. (14), a 3-qubit phase-flip repetition code encodes $|0\rangle$ and $|1\rangle$ as follows:

$$|0\rangle \rightarrow |+++\rangle,$$
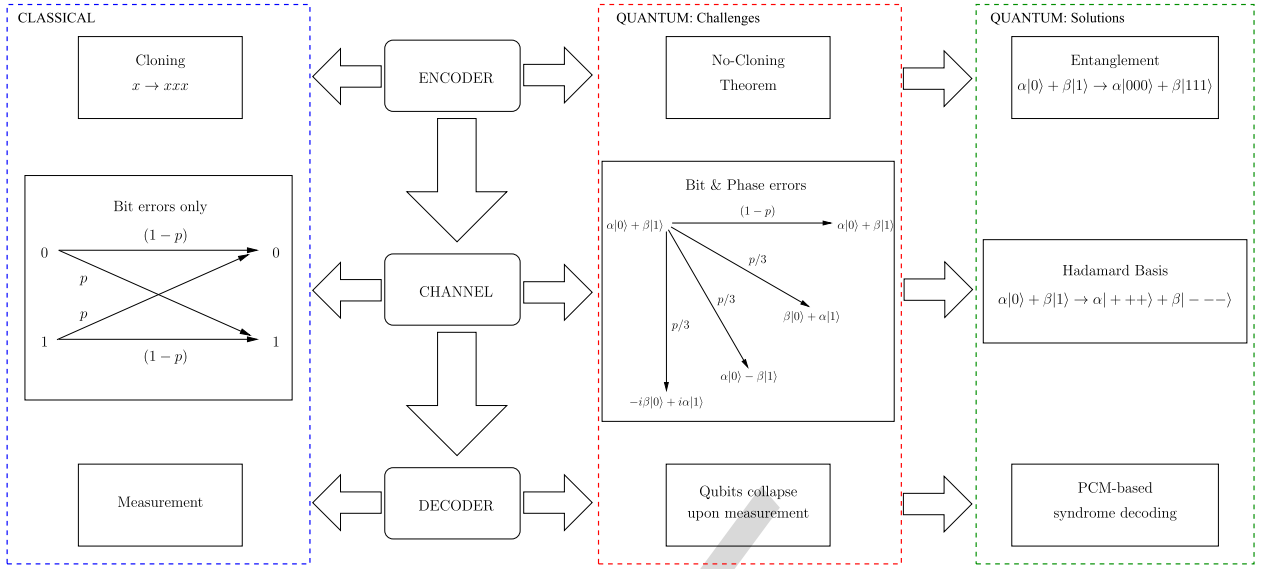$$|1\rangle \rightarrow |---\rangle. \tag{23}$$

FIGURE 8. Transition from the classical to quantum codes. **Encoder:** In classical codes, the information bit may be copied during the encoding process, e.g. in a 3-bit repetition code. This is not permissible in the quantum domain (no-cloning theorem). Alternatively, in quantum codes, the information qubit is entangled to the auxiliary qubits, e.g. in a 3-qubit bit-flip repetition code. **Channel:** Only bit errors occur over a classical channel, e.g. a binary symmetric channel with the channel crossover probability p. By contrast, qubits may experience a bit or phase error as well as both, e.g. depolarizing channel with a probability p. Since phase errors in the Hadamard basis $\{|+\rangle, |-\rangle\}$ are similar to the bit errors in the computational basis $\{|0\rangle, |1\rangle\}$, phase errors may be corrected in the same way as the bit errors by exploiting the Hadamard basis. **Decoder:** In classical codes, the received bits are measured during the decoding process, e.g. in a 3-bit repetition code a decision may be made on the basis of majority voting. Unfortunately, qubits collapse upon measurement. Consequently, quantum codes invoke the PCM-based syndrome decoding.

Based on Eq. (23), $|\psi\rangle$ is encoded to:

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|+++\rangle + \beta|---\rangle, \qquad (24)$$

which is stabilized by the generators $g_1 = \mathbf{XXI}$ and $g_2 = \mathbf{XIX}$. Hence, the Hadamard and Pauli-$\mathbf{X}$ operators enable a quantum code to correct phase errors. This overall transition from the classical 3-bit repetition code of Section IV-A to the quantum repetition code is summarized in Fig. 8.

Furthermore, the stabilizer generators g_i constituting the stabilizer group $\mathcal{H}$ must exhibit the following two characteristics:

1) **Any two operators in the stabilizer set must commute** so that the stabilizer operators can be applied simultaneously, i.e. we have:

$$g_1 g_2 |\overline{\psi}\rangle = g_2 g_1 |\overline{\psi}\rangle. \qquad (25)$$

This is because the stabilizer leaves the codeword unchanged as encapsulated below:

$$g_i |\overline{\psi}\rangle = |\overline{\psi}\rangle. \qquad (26)$$

Hence, evaluating the left-hand and right-hand sides of Eq. (25) gives:

$$g_1 g_2 |\overline{\psi}\rangle = g_1 |\overline{\psi}\rangle = |\overline{\psi}\rangle, \qquad (27)$$

and

$$g_2 g_1 |\overline{\psi}\rangle = g_2 |\overline{\psi}\rangle = |\overline{\psi}\rangle, \qquad (28)$$

respectively. This further imposes the constraint that the stabilizers should have an even number of places with different non-Identity (i.e. $\mathbf{X}$, $\mathbf{Y}$, or $\mathbf{Z}$) operations. This is derived from the fact that the $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ operations anti-commute with one another as shown below:

$$\mathbf{XY} = i\mathbf{Z}, \quad \mathbf{YX} = -i\mathbf{Z} \rightarrow \mathbf{XY} = -\mathbf{YX}$$
$$\mathbf{YZ} = i\mathbf{X}, \quad \mathbf{ZY} = -i\mathbf{X} \rightarrow \mathbf{YZ} = -\mathbf{ZY}$$
$$\mathbf{ZX} = i\mathbf{Y}, \quad \mathbf{XZ} = -i\mathbf{Y} \rightarrow \mathbf{ZX} = -\mathbf{XZ} \quad (29)$$

Thus, for example the operators $\mathbf{ZZI}$ and $\mathbf{XYZ}$ commute, whereas $\mathbf{ZZI}$ and $\mathbf{YZI}$ anti-commute.

2) **Generators constituting the stabilizer group $\mathcal{H}$ are closed under multiplication**, i.e. multiplication of the constituent generators g_i yields another generator, which is also part of the stabilizer group $\mathcal{H}$. For example, the full stabilizer group $\mathcal{H}$ of the 3-qubit bit-flip repetition code will also include the operator $\mathbf{IZZ}$, which is the product of g_1 and g_2.

It must be mentioned here that the Pauli errors which differ only by the stabilizer group have the same impact on all the codewords and therefore can be corrected by the same recovery operations. This gives quantum codes the intrinsic property of degeneracy [78]. More explicitly, the errors $\mathcal{P}$ and $\mathcal{P}' = g_i \mathcal{P}$ have the same impact on the transmitted codeword and therefore can be corrected by the same recovery operation. Getting back to our example of the 3-qubit bit-flip repetition code, let $\mathcal{P} = \mathbf{IIX}$ and $\mathcal{P}' = g_1 \mathcal{P} = \mathbf{ZZX}$. Both $\mathcal{P}$ as well as $\mathcal{P}'$ corrupt the transmitted codeword of Eq. (15) to $\alpha|001\rangle + \beta|110\rangle$. Consequently, $\mathcal{P}$ and $\mathcal{P}'$ need not be differentiated and are therefore classified as degenerate errors.

C. PAULI-TO-BINARY ISOMORPHISM

QSCs may be characterized in terms of an equivalent classical parity check matrix notation satisfying the commutativity constraint of stabilizers [38], [103] given in Eq. (25). This is achieved by mapping the **I**, **X**, **Y** and **Z** Pauli operators onto $(\mathbb{F}_2)^2$ as follows:

$$\mathbf{I} \to (0, 0),$$
$$\mathbf{X} \to (0, 1),$$
$$\mathbf{Y} \to (1, 1),$$
$$\mathbf{Z} \to (1, 0). \tag{30}$$

More explicitly, the $(n - k)$ stabilizers of an $[n, k]$ stabilizer code constitute the rows of the binary PCM H, which can be represented as a concatenation of a pair of $(n - k) \times n$ binary matrices H_z and H_x based on Eq. (30), as given below:

$$H = (H_z | H_x). \tag{31}$$

Each row of H corresponds to a stabilizer of $\mathcal{H}$, so that the ith column of H_z and H_x corresponds to the ith qubit and a binary 1 at these locations represents a **Z** and **X** Pauli operator, respectively, in the corresponding stabilizer. For the 3-qubit bit-flip repetition code, which can only correct bit-flip errors, the PCM H is given by:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}. \tag{32}$$

It must be pointed out here that H_z of Eq. (32) is same as the H of the classical repetition code of Eq. (13), yielding the same syndrome patterns in Table 5 and Table 6.

TABLE 7. Stabilizers for 9-qubit Shor's code.

	Stabilizer
g_1	ZZIIIIIII
g_2	IZZIIIIII
g_3	IIIZZIIII
g_4	IIIIZZIII
g_5	IIIIIIZZI
g_6	IIIIIIIZZ
g_7	XXXXXXIII
g_8	IIIXXXXXX

Let us further elaborate the process by considering the $[9, 1]$ Shor's code, which consists of the Pauli-**Z** as well as the Pauli-**X** operators. The corresponding stabilizer generators are given in Table 7. They can be mapped onto the binary matrix H as follows:

$$H = \begin{pmatrix} H_z' & \mathbf{0} \\ \mathbf{0} & H_x' \end{pmatrix}, \tag{33}$$

where we have $H_z = \begin{pmatrix} H_z' \\ \mathbf{0} \end{pmatrix}$, $H_x = \begin{pmatrix} \mathbf{0} \\ H_x' \end{pmatrix}$ and:

$$H_z' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}, \tag{34}$$

$$H_x' = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{35}$$

With the matrix notation of Eq. (31), the commutative property of stabilizers given in Eq. (25) is transformed into the orthogonality of rows with respect to the symplectic product (also called twisted product). If row m is $r_m = (z_m, x_m)$, where z_m and x_m are the binary strings for Z and X respectively, then the symplectic product of rows m and m' is given by,

$$r_m \star r_{m'} = (z_m \cdot x_{m'} + z_{m'} \cdot x_m) \bmod 2. \tag{36}$$

This symplectic product is zero if there are even number of places where the operators (X or Z) in row m and m' are different; thus meeting the commutativity requirement. In other words, if H is written as $H = (H_z | H_x)$, then the symplectic product is satisfied for all the rows only if,

$$H_z H_x^T + H_x H_z^T = 0, \tag{37}$$

which may be readily verified for the H of Eq. (33). Consequently, any classical binary codes satisfying Eq. (37) may be used to construct QSCs. A special class of these stabilizer codes are CSS codes, which are defined as follows:

An $[n, k_1 - k_2]$ CSS code, which is capable of correcting t bit as well as phase errors, can be constructed from classical linear block codes $C_1(n, k_1)$ and $C_2(n, k_2)$, if $C_2 \subset C_1$ and both C_1 as well as the dual of C_2, i.e. $C_2^\perp$, can correct t errors.

In CSS construction, the PCM H_z' of C_1 is used for correcting bit errors, while the PCM H_x' of $C_2^\perp$ is used for phase-error correction. Consequently, the PCM of the resultant CSS code takes the form of Eq. (33). H_z' and H_x' are now the $(n - k_1) \times n$ and $k_2 \times n$ binary matrices, respectively. Furthermore, since $C_2 \subset C_1$, the symplectic condition of Eq. (37) is reduced to $H_z' H_x'^T = 0$. In this scenario, $(n - k_1 + k_2)$ stabilizers are applied to n qubits. Therefore, the resultant quantum code encodes $(k_1 - k_2)$ information qubits into n qubits. Furthermore, if $H_z' = H_x'$, the resultant structure is called dual-containing (or self-orthogonal) code because $H_z' H_z'^T = 0$, which is equivalent to $C_1^\perp \subset C_1$. Hence, stabilizer codes may be sub-divided into various code structures, which are summarized in Fig. 9.
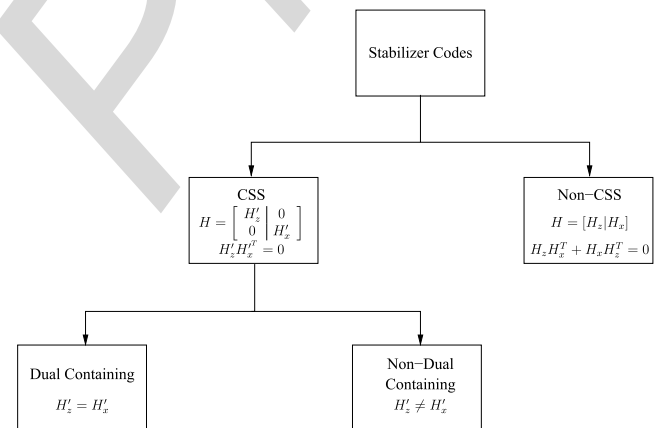

FIGURE 9. Family of stabilizer codes.

Let us consider the classical $(7, 4)$ Hamming code, whose PCM is given by:

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \qquad (38)$$

Since the H of Eq. (38) yields $HH^T = 0$, it is used for constructing the dual-containing rate-1/7 Steane code [51].
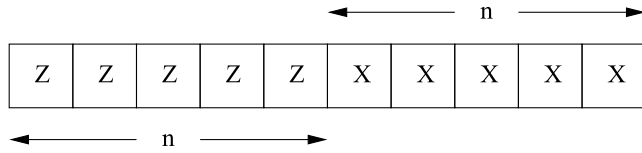

FIGURE 10. Effective classical error P corresponding to the error $\mathcal{P}$ imposed on an *n*-qubit frame.

Based on the aforementioned Pauli-to-binary isomorphism, a quantum-based Pauli error operator $\mathcal{P}$ can be represented by the effective classical error pattern P, which is a binary vector of length $2n$. More specifically, P is a concatenation of n bits for **Z** errors, followed by another n bits for **X** errors, as depicted in Fig. 10. An **X** error imposed on the 1st qubit will yield a 0 and a 1 at the 1st and $(n + 1)$th index of P, respectively. Similarly, a **Z** error imposed on the 1st qubit will give a 1 and a 0 at the 1st and $(n + 1)$th index of P, respectively, while a Y error on the 1st qubit will result in a 1 at both the 1st as well as $(n + 1)$th index of P.[18] The resultant syndrome is given by the symplectic product of $\mathbf{H}$ and P, which is equivalent to $\mathbf{H}(P_x : P_z)^T$. Here colon (:) denotes the concatenation operation. In other words, the Pauli-**X** operator is used for correcting **Z** errors, while the Pauli-**Z** operator is used for correcting **X** errors [13]. Thus, the quantum-domain syndrome is equivalent to the classical-domain binary syndrome and a basic quantum-domain decoding procedure is similar to syndrome based decoding of the equivalent classical code [38]. However, due to the degenerate nature of quantum codes, quantum decoding aims for finding the most likely error coset, while the classical syndrome decoding [102] finds the most likely error.

Hence, an $[n, k]$ quantum stabilizer code associated with $(n{-}k)$ stabilizers can be effectively modeled using an $(n{-}k) \times 2n$-element classical PCM satisfying Eq. (37). The coding rate of the equivalent classical code R_c can be determined as follows:

$$\begin{aligned} R_c &= \frac{2n - (n - k)}{2n} \\ &= \frac{n + k}{2n} \\ &= \frac{1}{2}\left(1 + \frac{k}{n}\right) \\ &= \frac{1}{2}\left(1 + R_Q\right), \end{aligned} \qquad (39)$$

[18]Since a depolarizing channel characterized by the probability p incurs **X**, **Y** and **Z** errors with an equal probability of $p/3$, the effective error-vector P reduces to two Binary Symmetric Channels (BSCs), one channel for the **Z** errors and the other for the **X** errors. The crossover probability of each BSC is given by $2p/3$.

where R_Q is its quantum coding rate. Using Eq. (39), the coding rate of the classical equivalent of Shor's rate-1/9 quantum code is 5/9.

D. STABILIZER FORMALISM OF QUANTUM CONVOLUTIONAL CODES

Quantum convolutional codes are derived from the corresponding classical convolutional codes using stabilizer formalism. This is based on the equivalence between the classical convolutional codes and the classical linear block codes with semi-infinite length, which is derived below [26].

Consider a $(2, 1, m)$ classical convolutional code with generators,

$$\begin{aligned} g^{(0)} &= (g_0^{(0)}, g_1^{(0)}, \dots, g_m^{(0)}), \\ g^{(1)} &= (g_0^{(1)}, g_1^{(1)}, \dots, g_m^{(1)}). \end{aligned} \qquad (40)$$

For an input sequence $[u = (u_0, u_1, u_2, \dots)]$, the output sequences $[v^{(0)} = (v_0^{(0)}, v_1^{(0)}, v_2^{(0)}, \dots)]$ and $[v^{(1)} = (v_0^{(1)}, v_1^{(1)}, v_2^{(1)}, \dots)]$ are given as follows:

$$\begin{aligned} v^{(0)} &= u \circledast g^{(0)}, \\ v^{(1)} &= u \circledast g^{(1)}, \end{aligned} \qquad (41)$$

where $\circledast$ denotes discrete convolution (modulo 2), which implies that for all $l \geq 0$ we have:

$$v_l^{(j)} = \sum_{i=0}^{m} u_{l-i} g_i^{(j)} = u_l g_0^{(j)} + u_{l-1} g_1^{(j)} + \dots + u_{l-m} g_m^{(j)}, \qquad (42)$$

where $j = 0, 1$ and $u_{l-i} \triangleq 0$ for all $l < i$. The two encoded sequences are multiplexed into a single codeword sequence v given by:

$$v = (v_0^{(0)}, v_0^{(1)}, v_1^{(0)}, v_1^{(1)}, v_2^{(0)}, v_2^{(1)}, \dots) \qquad (43)$$

This encoding process can also be represented in matrix notation by interlacing the generators $g^{(0)}$ and $g^{(1)}$ and arranging them in matrix form as follows,[19]

$$G = \begin{pmatrix} g_0^{(0)(1)} & g_1^{(0)(1)} & \cdots & g_m^{(0)(1)} & & \\ & g_0^{(0)(1)} & g_1^{(0)(1)} & \cdots & g_m^{(0)(1)} & \\ & & g_0^{(0)(1)} & g_1^{(0)(1)} & \cdots & g_m^{(0)(1)} \\ & \ddots & & \cdots & & \ddots \end{pmatrix}, \qquad (44)$$

where $g_i^{(0)(1)} \triangleq \left(g_i^{(0)} g_i^{(1)}\right)$. The encoding operation of Eq. (42) is therefore equivalent to,

$$v = uG. \qquad (45)$$

Since the information sequence u is of arbitrary length, G is semi-infinite. Furthermore, each row of G is identical to the previous row, but is shifted to the right by two places (since $n = 2$). In practice, u has a finite length N. Therefore, G has N rows and $2(m + N)$ columns

[19]Blank spaces in the matrix indicate zeros.

for CC(2, 1, m). For CC(n, k, m), G can be generalized as follows:

$$G = \begin{pmatrix} G_0 & G_1 & \ldots & G_m & & & \\ & G_0 & G_1 & \ldots & G_m & & \\ & & G_0 & G_1 & \ldots & G_m & \\ & & & \ddots & & \ldots & \ddots \end{pmatrix}, \quad (46)$$

where G_l is a ($k \times n$) submatrix with entries,

$$G_l = \begin{pmatrix} g_{1,l}^{(0)} & g_{1,l}^{(1)} & \cdots & g_{1,l}^{(n-1)} \\ g_{2,l}^{(0)} & g_{2,l}^{(1)} & \cdots & g_{2,l}^{(n-1)} \\ \vdots & \vdots & & \vdots \\ g_{k,l}^{(0)} & g_{k,l}^{(1)} & \cdots & g_{k,l}^{(n-1)} \end{pmatrix}. \quad (47)$$

The corresponding PCM H can be represented as a semi-infinite matrix consisting of submatrices H_l with dimensions of $(n - k) \times n$. For a convolutional code with constraint length[20] ($m + 1$), H is given by:

$$H = \begin{pmatrix} H_0 & & & & & \\ H_1 & H_0 & & & & \\ H_2 & H_1 & H_0 & & & \\ \vdots & \vdots & \vdots & & & \\ H_m & H_{m-1} & H_{m-2} & \ldots & H_0 & \\ & H_m & H_{m-1} & H_{m-2} & \ldots & H_0 \\ & & \vdots & \vdots & & \vdots \end{pmatrix}. \quad (48)$$

Therefore, a CCC can be represented as a linear block code with semi-infinite block length. Furthermore, if each row of the submatrices H_l is considered as a single block and $h_{j,i}$ is the ith row of the jth block, then H has a block-band structure after the first m blocks, whereby the successive blocks are time-shifted versions of the first block ($j = 0$) and the adjacent blocks have an overlap of m submatrices. This has been depicted in Fig. 11 and can be mathematically represented as follows:

$$h_{j,i} = [\mathbf{0}^{j \times n}, h_{0,i}], \quad 1 \le i \le (n - k), \ 0 \le j, \quad (49)$$

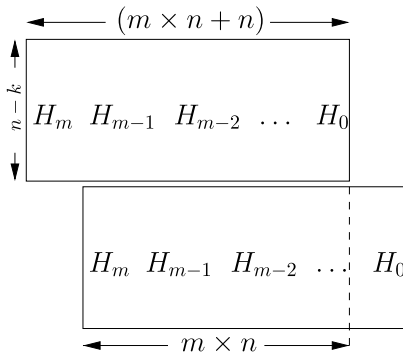where $\mathbf{0}^{j \times n}$ is a row-vector with ($j \times n$) zeros.

FIGURE 11. Block-band structure of the semi-infinite classical PCM *H*.

[20]Constraint length is the number of memory units (shift registers) plus 1.

As discussed in Section IV-C, the rows of a classical PCM correspond to the stabilizers of a quantum code. Hence, the quantum stabilizer group $\mathcal{H}$ of an [n, k, m] stabilizer convolutional code is given by [65]:

$$\mathcal{H} = sp\{g_{j,i} = I^{\otimes jn} \otimes g_{0,i}\}, \quad 1 \le i \le (n - k), \ 0 \le j, \quad (50)$$

where $g_{j,i}$ is the ith stabilizer of the jth block of the stabilizer group $\mathcal{H}$. Furthermore, sp represents a symplectic group, thus implying that all the stabilizers $g_{j,i}$ must be independent and must commute with each other.

As proposed by Forney and Guha in [66] and Forney *et al.* in [67], CSS-type QCCs can be derived from the classical self-orthogonal binary convolution codes. Let us consider the rate 1/3 QCC of [66] and [67], which is constructed from a binary rate-1/3 CCC with generators:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & \ldots \\ & & & & & \ldots & & & & & & & \end{pmatrix}. \quad (51)$$

In D-transform notation, these generators are represented as $(1 + D + D^2, 1 + D^2, 1)$. Each generator is orthogonal to all other generators under the binary inner product, making it a self-orthogonal code. Moreover, the dual $C^\perp$ has the capability of correcting 1 bit. Therefore, based on the CSS construction, the basic stabilizers of the corresponding single-error correcting [3, 1] QCC are as follows:

$$g_{0,1} = [\mathbf{XXX}, \mathbf{XII}, \mathbf{XXI}], \quad (52)$$
$$g_{0,2} = [\mathbf{ZZZ}, \mathbf{ZII}, \mathbf{ZZI}]. \quad (53)$$

Other stabilizers of $\mathcal{H}$ are the time-shifted versions of these basic stabilizers as depicted in Eq. (50).

Let us further consider a non-CSS QCC construction given by Forney and Guha in [66] and Forney *et al.* in [67]. It is derived from the classical self-orthogonal rate-1/3 quaternary ($\mathbb{F}_4$) convolutional code C having generators $(1 + D, 1 + wD, 1 + \bar{w}D)$, where $\mathbb{F}_4 = \{0, 1, w, \bar{w}\}$. These generators can also be represented as follows:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & w & \bar{w} & 0 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & w & \bar{w} & \ldots \\ & & & & \ldots & & & & & \end{pmatrix}. \quad (54)$$

Since all these generators are orthogonal under the Hermitian inner product, C is self-orthogonal. Therefore, a [3, 1] QCC can be derived from this classical code. The basic generators $g_{0,i}$, for $1 \le i \le 2$, of the corresponding stabilizer group, $\mathcal{H}$, are generated by multiplying the generators of Eq. (54) with w and $\bar{w}$, and mapping 0, w, 1, $\bar{w}$ onto $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ respectively. The resultant basic stabilizers are as follows:

$$g_{0,1} = (\mathbf{XXX}, \mathbf{XZY}), \quad (55)$$
$$g_{0,2} = (\mathbf{ZZZ}, \mathbf{ZYX}), \quad (56)$$

and all other constituent stabilizers of $\mathcal{H}$ can be derived using Eq. (50).
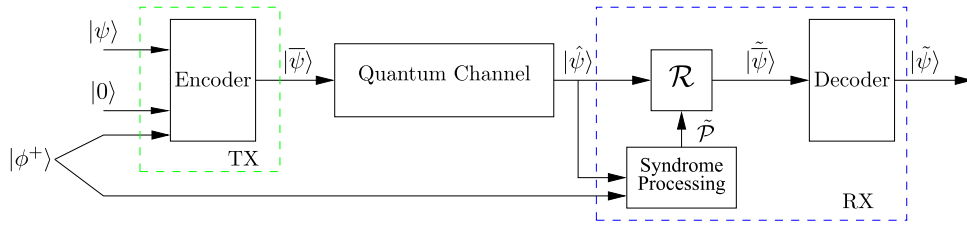
FIGURE 12. System Model: Quantum communication system relying on an entanglement-assisted quantum stabilizer code.

E. ENTANGLEMENT-ASSISTED STABILIZER FORMALISM

Let us recall that the classical binary and quaternary codes may be used for constructing stabilizer codes only if they satisfy the symplectic criterion of Eq. (37). Consequently, some of the well-known classical codes cannot be explored in the quantum domain. This limitation can be readily overcome by using the entanglement-assisted stabilizer formalism, which exploits pre-shared entanglement between the transmitter and receiver to embed a set of non-commuting stabilizer generators into a larger set of commuting generators.

Fig. 12 shows the general schematic of a quantum communication system, which incorporates an Entanglement-Assisted Quantum Stabilizer Code (EA-QSC). An $[n, k, c]$ EA-QSC encodes the information qubits $|\psi\rangle$ into the coded sequence $|\overline{\psi}\rangle$ with the aid of $(n-k-c)$ auxiliary qubits, which are initialized to the state $|0\rangle$. Furthermore, the transmitter and receiver share c entangled qubits (ebits) before actual transmission takes place. This may be carried out during the off-peak hours, when the channel is under-utilized, thus efficiently distributing the transmission requirements in time. More specifically, the state $|\phi^+\rangle$ of an ebit is given by the following Bell state:

$$|\phi^+\rangle = \frac{|00\rangle^{T_X R_X} + |11\rangle^{T_X R_X}}{\sqrt{2}}, \tag{57}$$

where T_X and R_X denotes the transmitter's and receiver's half of the ebit, respectively. Similar to the superdense coding protocol of [104], it is assumed that the receiver's half of the c ebits are transmitted over a noiseless quantum channel, while the transmitter's half of the c ebits together with the $(n-k-c)$ auxiliary qubits are used to encode the intended k information qubits into n coded qubits. The resultant n-qubit codewords $|\overline{\psi}\rangle$ are transmitted over a noisy quantum channel. The receiver then combines his half of the c noiseless ebits with the received n-qubit noisy codewords $|\hat{\psi}\rangle$ to compute the syndrome, which is used for estimating the error $\tilde{\mathcal{P}}$ incurred on the n-qubit codewords. The rest of the processing at the receiver is the same as that in Fig. 7.

The entangled state of Eq. (57) has unique commutativity properties, which aid in transforming a set of non-abelian generators into an abelian set. The state $|\phi^+\rangle$ is stabilized by the operators $\mathbf{X}^{T_X}\mathbf{X}^{R_X}$ and $\mathbf{Z}^{T_X}\mathbf{Z}^{R_X}$, which commute with each other. Therefore, we have[21]:

$$[\mathbf{X}^{T_X}\mathbf{X}^{R_X}, \mathbf{Z}^{T_X}\mathbf{Z}^{R_X}] = 0. \tag{58}$$

However, local operators acting on either of the qubits anti-commute, i.e. we have:

$$\{\mathbf{X}^{T_X}, \mathbf{Z}^{T_X}\} = \{\mathbf{X}^{R_X}, \mathbf{Z}^{R_X}\} = 0. \tag{59}$$

Therefore, if we have two single qubit operators $\mathbf{X}^{T_X}$ and $\mathbf{Z}^{T_X}$, which anti-commute with each other, then we can resolve the anti-commutativity by entangling another qubit and choosing the local operators on this additional qubit such that the resultant two-qubit generators ($\mathbf{X}^{T_X}\mathbf{X}^{R_X}$ and $\mathbf{Z}^{T_X}\mathbf{Z}^{R_X}$ for this case) commute. This additional qubit constitutes the receiver half of the ebit. In other words, we entangle an additional qubit for the sake of ensuring that the resultant two-qubit operators have an even number of places with different non-identity operators, which in turn ensures commutativity.

Let us consider a pair of classical binary codes associated with the following PCMs:

$$H_z = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \tag{60}$$

and

$$H_x = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \tag{61}$$

which are used to construct a non-CSS quantum code having $H = (H_z|H_x)$. The PCM H does not satisfy the symplectic criterion. The resultant non-abelian set of Pauli generators are as follows:

$$H_Q = \begin{pmatrix} \mathbf{X} & \mathbf{Z} & \mathbf{X} & \mathbf{I} \\ \mathbf{X} & \mathbf{X} & \mathbf{I} & \mathbf{X} \\ \mathbf{Y} & \mathbf{Z} & \mathbf{Z} & \mathbf{X} \\ \mathbf{X} & \mathbf{Y} & \mathbf{Y} & \mathbf{Z} \end{pmatrix}. \tag{62}$$

In Eq. (62), the first two generators (i.e. the first and second row) anti-commute, while all other generators commute with each other. This is because the local operators acting on the second qubit in the first two generators anti-commute, while the local operators acting on all other qubits in these two generators commute. In other words, there is a

---

[21][a, b] represents the commutative relation between *a* and *b*, while {a, b} denotes the anti-commutative relation.

single index (i.e. 2) with different non-Identity operators. To transform this non-abelian set into an abelian set, we may extend the generators of Eq. (62) with a single additional qubit, whose local operators also anti-commute for the sake of ensuring that the resultant extended generators commute. Therefore, we get:

$$H_Q = \begin{pmatrix} \mathbf{X} & \mathbf{Z} & \mathbf{X} & \mathbf{I} & \mathbf{Z} \\ \mathbf{X} & \mathbf{X} & \mathbf{I} & \mathbf{X} & \mathbf{X} \\ \mathbf{Y} & \mathbf{Z} & \mathbf{Z} & \mathbf{X} & \mathbf{I} \\ \mathbf{X} & \mathbf{Y} & \mathbf{Y} & \mathbf{Z} & \mathbf{I} \end{pmatrix}, \quad (63)$$

where the operators to the left of the vertical bar (|) act on the transmitted n-qubit codewords, while those on the right of the vertical bar act on the receiver's half of the ebits.

V. CONCATENATED QUANTUM CODES

In this section, we will lay out the structure of a concatenated quantum code, with a special emphasis on the encoder structure and the decoding algorithm. We commence with the circuit-based representation of quantum stabilizer codes, followed by the system model and then the decoding algorithm.

A. CIRCUIT-BASED REPRESENTATION OF STABILIZER CODES

Circuit-based representation of quantum codes facilitates the design of concatenated code structures. More specifically, for decoding concatenated quantum codes it is more convenient to exploit the circuit-based representation of the constituent codes, rather than the conventional PCM-based syndrome decoding. Therefore, in this section, we will review the circuit-based representation of quantum codes. This discussion is based on [33].

Let us recall from Section IV-A that an (n, k) classical linear block code constructed over the code space C maps the information word $x \in \mathbb{F}_2^k$ onto the corresponding codeword $\bar{x} \in \mathbb{F}_2^n$. In the circuit-based representation, this encoding procedure can be encapsulated as follows:

$$C = \{\bar{x} = (x : 0_{n-k}) V\}, \quad (64)$$

where V is an $(n \times n)$-element invertible encoding matrix over $\mathbb{F}_2$ and 0_{n-k} is an $(n - k)$-bit vector initialized to 0. Furthermore, given the generator matrix G and the PCM H, the encoding matrix V may be specified as:

$$V = \begin{pmatrix} G \\ (H^{-1})^T \end{pmatrix}, \quad (65)$$

and its inverse is given by:

$$V^{-1} = (G^{-1} \ H^T). \quad (66)$$

The encoding matrix V specifies both the code space as well as the encoding operation, while its inverse V^{-1} specifies the error syndrome. More specifically, let $y = \bar{x} + e$ be the received codeword, where e is the n-bit error incurred during transmission. Then, passing the received codeword y through the inverse encoder V^{-1} yields:

$$yV^{-1} = (\tilde{x} : s), \quad (67)$$

where $\tilde{x} = x + l$ for the logical error $l \in \mathbb{F}_2^k$ inflicted on the information word x and $s \in \mathbb{F}_2^{n-k}$ is the syndrome, which is equivalent to yH^T. Eq. (67) may be further decomposed to:

$$(\bar{x} + e) V^{-1} = (x + l : s),$$
$$\bar{x}V^{-1} + eV^{-1} = (x : 0_{n-k}) + (l : s), \quad (68)$$

which is a linear superposition of the inverse of Eq. (64) and $eV^{-1} = (l : s)$. Hence, the inverse encoder V^{-1} decomposes the channel error e into the logical error l and error syndrome s, which is also depicted in Fig. 13.
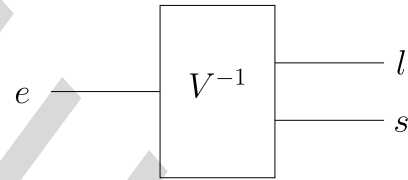

FIGURE 13. Circuit representation of the inverse encoder $eV^{-1} = (l : s)$.

Analogously to Eq. (64), the unitary encoding operation $\mathcal{V}$ of an $[n, k]$ QSC, constructed over a code space $\mathcal{C}$, which maps the information word (logical qubits) $|\psi\rangle \in \mathbb{C}^{2^k}$ onto the codeword (physical qubits) $|\bar{\psi}\rangle \in \mathbb{C}^{2^n}$, may be mathematically encapsulated as follows:

$$\mathcal{C} = \{|\bar{\psi}\rangle = \mathcal{V}(|\psi\rangle \otimes |0_{n-k}\rangle)\}, \quad (69)$$

where $|0_{n-k}\rangle$ are $(n - k)$ auxiliary qubits initialized to the state $|0\rangle$. The unitary encoder $\mathcal{V}$ of Eq. (69) carries out an n-qubit Clifford transformation, which maps an n-qubit Pauli group $\mathcal{G}_n$ onto itself under conjugation [105], i.e. we have:

$$\mathcal{V}\mathcal{G}_n\mathcal{V}^\dagger = \mathcal{G}_n. \quad (70)$$

In other word, a Clifford operation preserves the elements of the Pauli group under conjugation such that for $\mathcal{P} \in \mathcal{G}_n$, $\mathcal{V}\mathcal{P}\mathcal{V}^\dagger \in \mathcal{G}_n$. Furthermore, any Clifford unitary matrix is completely specified by a combination of Hadamard (**H**) gates, phase (**S**) gates and controlled-NOT (C-NOT) gates, which are defined as follows [13]:

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (71)$$

Hadamard gate preserves the elements of a single-qubit Pauli group $\mathcal{G}_1$ as follows:

$$\mathbf{X} \rightarrow \mathbf{H}\mathbf{X}\mathbf{H}^\dagger = \mathbf{Z},$$
$$\mathbf{Z} \rightarrow \mathbf{H}\mathbf{Z}\mathbf{H}^\dagger = \mathbf{X},$$
$$\mathbf{Y} \rightarrow \mathbf{H}\mathbf{Y}\mathbf{H}^\dagger = -\mathbf{Y}, \quad (72)$$

while phase gate preserves them as:

$$\mathbf{X} \rightarrow \mathbf{SXS}^{\dagger} = \mathbf{Y},$$

$$\mathbf{Z} \rightarrow \mathbf{SZS}^{\dagger} = \mathbf{Z},$$

$$\mathbf{Y} \rightarrow \mathbf{SYS}^{\dagger} = -\mathbf{X}, \qquad (73)$$

Since C-NOT is a 2-qubit gate, it acts on the elements of $\mathcal{G}_2$, transforming the standard basis of $\mathcal{G}_2$ as given below:

$$\mathbf{X} \otimes \mathbf{I} \rightarrow \mathbf{X} \otimes \mathbf{X},$$

$$\mathbf{I} \otimes \mathbf{X} \rightarrow \mathbf{I} \otimes \mathbf{X},$$

$$\mathbf{Z} \otimes \mathbf{I} \rightarrow \mathbf{Z} \otimes \mathbf{I},$$

$$\mathbf{I} \otimes \mathbf{Z} \rightarrow \mathbf{Z} \otimes \mathbf{Z}. \qquad (74)$$

Let us further emphasize on the significance of Clifford encoding operation. *Since $\mathcal{V}$ belongs to the Clifford group, it preserves the elements of the stabilizer group $\mathcal{H}$ under conjugation.* If g_i' is the ith stabilizer of the unencoded state $|\psi\rangle$, then this may be proved as follows:

$$|\psi\rangle \otimes |0_{n-k}\rangle = g_i' (|\psi\rangle \otimes |0_{n-k}\rangle). \qquad (75)$$

Encoding $|\psi\rangle$ with $\mathcal{V}$ yields:

$$\mathcal{V} (|\psi\rangle \otimes |0_{n-k}\rangle) = \mathcal{V} \left(g_i' (|\psi\rangle \otimes |0_{n-k}\rangle) \right), \qquad (76)$$

which is equivalent to:

$$\mathcal{V} (|\psi\rangle \otimes |0_{n-k}\rangle) = \mathcal{V} \left(g_i' \mathcal{V}^{\dagger} \mathcal{V} (|\psi\rangle \otimes |0_{n-k}\rangle) \right), \qquad (77)$$

since $\mathcal{V}^{\dagger}\mathcal{V} = \mathbb{I}_n$. Substituting Eq. (69) into Eq. (77) gives:

$$|\overline{\psi}\rangle = \left(\mathcal{V} g_i' \mathcal{V}^{\dagger} \right) |\overline{\psi}\rangle. \qquad (78)$$

Hence, the encoded state $|\overline{\psi}\rangle$ is stabilized by $g_i = \mathcal{V} g_i' \mathcal{V}^{\dagger}$. From this it appears as if any arbitrary $\mathcal{V}$ (not necessarily Clifford) can be used to preserve the stabilizer subspace, which is not true. Since we assume that the stabilizer group $\mathcal{H}$ is a subgroup of the Pauli group, we impose the additional constraint that $\mathcal{V}$ must yield the elements of Pauli group under conjugation as in Eq. (70), which is only true for Clifford operations.

Furthermore, *the Clifford encoding operation also preserves the commutativity relation of stabilizers.* Let g_i' and g_j' be a pair of unencoded stabilizers. Then the above statement can be proved as follows:

$$g_i g_j = \left(\mathcal{V} g_i' \mathcal{V}^{\dagger} \right) \left(\mathcal{V} g_j' \mathcal{V}^{\dagger} \right) = \mathcal{V} g_i' g_j' \mathcal{V}^{\dagger}. \qquad (79)$$

Since g_i' and g_j' commute, we have:

$$\mathcal{V} g_i' g_j' \mathcal{V}^{\dagger} = \mathcal{V} g_j' g_i' \mathcal{V}^{\dagger}. \qquad (80)$$

Using $\mathcal{V}^{\dagger}\mathcal{V} = \mathbb{I}_n$, gives:

$$\mathcal{V} g_j' \mathcal{V}^{\dagger} \mathcal{V} g_i' \mathcal{V}^{\dagger}. = g_j g_i. \qquad (81)$$

Since the n-qubit Pauli group forms a basis for the $(2^n \times 2^n)$-element matrices of Eq. (71), the Clifford encoder $\mathcal{V}$, which acts on the 2^n-dimensional Hilbert space, can be completely defined by specifying its action under conjugation on the Pauli-$\mathbf{X}$ and $\mathbf{Z}$ operators acting on each of the n qubits, as seen in Eq. (72) to (74). However, $\mathcal{V}$ and $\mathcal{V}'$, which differ only through a global phase such that $\mathcal{V}' = e^{j\theta}\mathcal{V}$, have the same impact under conjugation. Therefore, global phase has no physical significance in the context of Eq. (70) and the n-qubit encoder $\mathcal{V}$ can be completely specified by its action on the binary equivalent of the Pauli operators. More specifically, for an n-qubit Clifford transformation, there is an equivalent $2n \times 2n$ binary symplectic matrix V, which is given by:

$$[\mathcal{V}\mathcal{P}\mathcal{V}^{\dagger}] = [\mathcal{P}]V = PV, \qquad (82)$$

where $[.]$ denotes the effective Pauli group G_n such that $P = [\mathcal{P}]$ differs from $\mathcal{P}$ by a multiplicative constant, i.e. we have $P = \mathcal{P}/\{\pm 1 \pm i\}$, and the elements of G_n are represented by $2n$-tuple binary vectors based on the mapping given in Eq. (30). As a consequence of this equivalence, any Clifford unitary can be efficiently simulated on a classical system as stated in the Gottesman-Knill theorem [106].

We next define $\mathcal{V}$ by specifying its action on the elements of the Pauli group $\mathcal{G}_n$. More precisely, we consider $2n$ n-qubit unencoded operators $Z_i, X_i, \ldots, Z_n, X_n$, where Z_i and X_i represents the Pauli $\mathbf{Z}$ and $\mathbf{X}$ operator, respectively, acting on the ith qubit and the identity $\mathbf{I}$ on all other qubits. The unencoded operators $Z_{k+1}, \ldots, Z_n$ stabilizes the unencoded state of Eq. (69), i.e. $(|\psi\rangle \otimes |0_{n-k}\rangle)$, and are therefore called the unencoded stabilizer generators. On the other hand, $X_{k+1}, \ldots, X_n$ are the unencoded pure errors since X_i anti-commutes with the corresponding unencoded stabilizer generator Z_i, yielding an error syndrome of 1. Furthermore, the unencoded logical operators acting on the information qubits are $Z_i, X_i, \ldots, Z_k, X_k$, which commute with the unencoded stabilizers $Z_{k+1}, \ldots, Z_n$. The encoder $\mathcal{V}$ maps the unencoded operators $Z_i, X_i, \ldots, Z_n, X_n$ onto the encoded operators $\overline{Z}_i, \overline{X}_i, \ldots, \overline{Z}_n, \overline{X}_n$, which may be represented as follows:

$$\overline{X}_i = \left[\mathcal{V} X_i \mathcal{V}^{\dagger} \right] = [X_i] V, \quad \overline{Z}_i = \left[\mathcal{V} Z_i \mathcal{V}^{\dagger} \right] = [Z_i] V. \qquad (83)$$

Since Clifford transformations do not perturb the commutativity relation of the operators, the resultant encoded stabilizers $\overline{Z}_{k+1}, \ldots, \overline{Z}_n$ are equivalent to the stabilizers g_i of Eq. (18), while $\overline{X}_{k+1}, \ldots, \overline{X}_n$ are the pure errors t_i of the resultant stabilizer code, which trigger a non-trivial syndrome. Moreover, $\overline{Z}_i, \overline{X}_i, \ldots, \overline{Z}_k, \overline{X}_k$ are the encoded logical operators, which commute with the stabilizers g_i. Logical operators merely map one codeword onto the other, without affecting the codespace $\mathcal{C}$ of the stabilizer code. It also has to be mentioned here that the stabilizer generators g_i together with the encoded logical operations constitute the normalizer of the stabilizer code. The $(2n \times 2n)$-element binary

symplectic encoding matrix V is therefore given by:

$$V = \begin{pmatrix} \overline{Z}_1 \\ \vdots \\ \overline{Z}_k \\ \overline{Z}_{k+1} \\ \vdots \\ \overline{Z}_n \\ \overline{X}_1 \\ \vdots \\ \overline{X}_k \\ \overline{X}_{k+1} \\ \vdots \\ \overline{X}_n \end{pmatrix} = \begin{pmatrix} \overline{Z}_1 \\ \vdots \\ \overline{Z}_k \\ g_1 \\ \vdots \\ g_{n-k} \\ \overline{X}_1 \\ \vdots \\ \overline{X}_k \\ t_1 \\ \vdots \\ t_{n-k} \end{pmatrix}, \qquad (84)$$

where the Pauli $\mathbf{Z}$ and $\mathbf{X}$ operators are mapped onto the classical bits using the Pauli-to-binary isomorphism of Section IV-C.

Analogously to the classical inverse encoder of Eq. (67), the inverse encoder of a quantum code is the Hermitian conjugate $\mathcal{V}^\dagger$. Let $|\hat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle$ be the received codeword such that $\mathcal{P}$ is the n-qubit channel error. Then, passing the received codeword $|\hat{\psi}\rangle$ through the inverse encoder $\mathcal{V}^\dagger$ yields:

$$\mathcal{V}^\dagger \mathcal{P}|\overline{\psi}\rangle = \mathcal{V}^\dagger \mathcal{P}\mathcal{V}(|\psi\rangle \otimes |0_{(n-k)}\rangle)$$
$$= (\mathcal{L}|\psi\rangle) \otimes (\mathcal{S}|0_{(n-k)}\rangle), \qquad (85)$$

where $\mathcal{V}^\dagger \mathcal{P}\mathcal{V} \equiv (\mathcal{L} \otimes \mathcal{S})$ and $\mathcal{L} \in \mathcal{G}_k$ denotes the error imposed on the information word, while $\mathcal{S} \in \mathcal{G}_{n-k}$ represents the error inflicted on the remaining $(n-k)$ auxiliary qubits. In the equivalent binary representation, Eq. (85) may be modeled as follows:

$$PV^{-1} = (L : S), \qquad (86)$$

where we have $P = [\mathcal{P}]$, $L = [\mathcal{L}]$ and $S = [\mathcal{S}]$.

Let us now derive the encoding matrix V for the 3-qubit bit-flip repetition code, which has a binary PCM H given by:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}. \qquad (87)$$

The corresponding encoding circuit is depicted in Fig. 14. Its unencoded operators are as follows:

$$\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \\ X_1 \\ X_2 \\ X_3 \end{pmatrix} = \begin{pmatrix} \mathbf{ZII} \\ \mathbf{IZI} \\ \mathbf{IIZ} \\ \mathbf{XII} \\ \mathbf{IXI} \\ \mathbf{IIX} \end{pmatrix} \equiv \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right). \qquad (88)$$

A C-NOT gate is then applied to the second qubit, which is controlled by the first. As seen in Eq. (74), the C-NOT gate copies Pauli $\mathbf{X}$ operator forward from the control qubit to the target qubit, while $\mathbf{Z}$ is copied in the opposite direction.
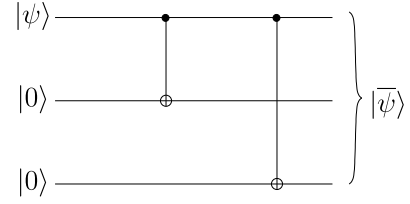

FIGURE 14. Encoding Circuit for 3-qubit bit-flip repetition code.

Therefore, we get:

$$\begin{pmatrix} \mathbf{ZII} \\ \mathbf{IZI} \\ \mathbf{IIZ} \\ \mathbf{XII} \\ \mathbf{IXI} \\ \mathbf{IIX} \end{pmatrix} \xrightarrow{\text{C-NOT}(1,2)} \begin{pmatrix} \mathbf{ZII} \\ \mathbf{ZZI} \\ \mathbf{IIZ} \\ \mathbf{XXI} \\ \mathbf{IXI} \\ \mathbf{IIX} \end{pmatrix} \equiv \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right). \qquad (89)$$

Another C-NOT gate is then applied to the third qubit, which is also controlled by the first, yielding:

$$\begin{pmatrix} \mathbf{ZII} \\ \mathbf{ZZI} \\ \mathbf{IIZ} \\ \mathbf{XXI} \\ \mathbf{IXI} \\ \mathbf{IIX} \end{pmatrix} \xrightarrow{\text{C-NOT}(1,3)} \begin{pmatrix} \mathbf{ZII} \\ \mathbf{ZZI} \\ \mathbf{ZIZ} \\ \mathbf{XXX} \\ \mathbf{IXI} \\ \mathbf{IIX} \end{pmatrix} \equiv \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array} \right)$$
$$= V. \qquad (90)$$

As gleaned from Eq. (90), the stabilizer generators of the 3-qubit bit-flip repetition code are $g_1 = \mathbf{ZZI}$ and $g_2 = \mathbf{ZIZ}$. More explicitly, rows 2 and 3 of V constitute the PCM H of Eq. (87). The encoded logical operators are $\overline{Z}_1 = \mathbf{ZII}$ and $\overline{X}_1 = \mathbf{XXX}$, which commute with the stabilizers g_1 and g_2. Finally, the pure errors are $t_1 = \mathbf{IXI}$ and $t_2 = \mathbf{IIX}$, which anticommute with g_1 and g_2, respectively, yielding a non-trivial syndrome.

Based on the above discussion, we now proceed to lay out the circuit-based model for a convolutional code, which is given in [33]. As discussed in Section IV-D, convolutional codes are equivalent to linear block codes associated with semi-infinite block lengths. More specifically, as illustrated in Fig. 11, the PCM H of an (n, k, m) convolutional code has a block-band structure, where the adjacent blocks have an overlap of m submatrices. Similarly, the encoder V of a classical convolutional code can be built from repeated applications of a linear invertible seed transformation U, which is an $(n+m) \times (n+m)$-element encoding matrix, as shown in Fig. 15. The inverse encoder V^{-1} can be easily obtained by moving backwards in time, i.e. by reading Fig. 15 from right to left. Let us further elaborate by stating that at time instant j, the seed transformation matrix U takes as its input the memory bits $m_{j-1} \in \mathbb{F}_2^m$, the logical bits $l_j \in \mathbb{F}_2^k$ and the syndrome bits $s_j \in \mathbb{F}_2^{n-k}$ to generate the output bits $e_j \in \mathbb{F}_2^n$ and the memory state m_j. More explicitly, we have:

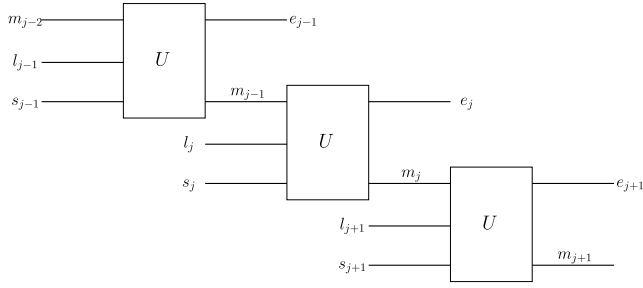$$(m_j : e_j) = (m_{j-1} : l_j : s_j)\,U, \qquad (91)$$

FIGURE 15. Circuit representation of the encoder *V* of a convolutional code [33].

and the overall encoder is formulated as [33]:

$$V = U_{[1,...,n+m]}U_{[n+1,...,2n+m]}\ldots U_{[(N-1)n+1,...,Nn+m]},$$

$$= \prod_{j=1}^{N} U_{[(j-1)n+1,...,jn+m]}, \quad (92)$$

where N denotes the length of the convolutional code and $U_{[(j-1)n+1,...,jn+m]}$ acts on $(n+m)$ bits, i.e. $\left(m_{j-2} : l_{j-1} : s_{j-1}\right)$. For an $[n, k, m]$ quantum convolutional code, the seed transformation U is a $2(n + m) \times 2(n + m)$-element symplectic matrix and Eq. (91) may be re-written as:

$$\left(M_j : P_j\right) = \left(M_{j-1} : L_j : S_j\right) U, \quad (93)$$

where M represents the memory state with an m-qubit Pauli operator.

The aforementioned methodology conceived for constructing the circuit-based model of unassisted quantum codes may be readily extended to the class of entanglement-assisted codes [34]. The unitary encoding operation $\mathcal{V}$ of an $[n, k, c]$ EA-QSC, which acts only on the n transmitter qubits, may be mathematically modeled as follows:

$$\mathcal{C} = \{|\overline{\psi}\rangle = \mathcal{V}(|\psi\rangle^{T_X} \otimes |0_a\rangle^{T_X} \otimes |\phi_c^+\rangle^{T_X R_X})\}, \quad (94)$$

where the superscripts T_X and R_X denote the transmitter's and receiver's qubits, respectively. Furthermore, $|0_a\rangle^{T_X}$ are a auxiliary qubits initialized to the state $|0\rangle$, where $a = (n - k - c)$, and $|\phi_c^+\rangle^{T_X R_X}$ are the c entangled qubits. Analogously to Eq. (85), the inverse encoder of an entanglement-assisted quantum code $\mathcal{V}^\dagger$ gives:

$$\mathcal{V}^\dagger \mathcal{P}|\overline{\psi}\rangle = \mathcal{V}^\dagger \mathcal{P}\mathcal{V}(|\psi\rangle^{T_X} \otimes |0_a\rangle^{T_X} \otimes |\phi_c^+\rangle^{T_X R_X})$$

$$= (\mathcal{L}^{T_X}|\psi\rangle^{T_X}) \otimes (\mathcal{S}^{T_X}|0_a\rangle^{T_X}) \otimes (\mathcal{E}^{T_X}|\phi_c^+\rangle^{T_X R_X}), \quad (95)$$

where $\mathcal{L}^{T_X} \in \mathcal{G}_k$ denotes the error imposed on the information word, while $\mathcal{S}^{T_X} \in \mathcal{G}_a$ represents the error inflicted on the transmitter's a auxiliary qubits and $\mathcal{E}^{T_X} \in \mathcal{G}_c$ is the error corrupting the transmitter's half of c ebits. The equivalent binary representation of Eq. (95) is given by:

$$PV^{-1} = (L : S : E), \quad (96)$$

where we have $P = [\mathcal{P}^{T_X}]$, $L = [\mathcal{L}^{T_X}]$, $S = [\mathcal{S}^{T_X}]$ and $E = [\mathcal{E}^{T_X}]$. Similarly, Eq. (93) can be re-modeled as follows:

$$\left(M_j : P_j\right) = \left(M_{j-1} : L_j : S_j : E_j\right) U. \quad (97)$$

B. SYSTEM MODEL: CONCATENATED QUANTUM CODES

Fig. 16 shows the general schematic of a quantum communication system relying on a pair of concatenated quantum stabilizer codes. In this contribution, both the inner as well as the outer codes are assumed to be convolutional codes. Furthermore, analogously to the classical concatenated codes, the inner code must be recursive, while both the inner as well the outer code must be non-catastrophic. Having a recursive nature of the inner code is essential for the sake of ensuring that the resultant families of codes have an unbounded minimum distance. On the other hand, the non-catastrophic nature of both the inner and the outer codes guarantees that a decoding convergence to
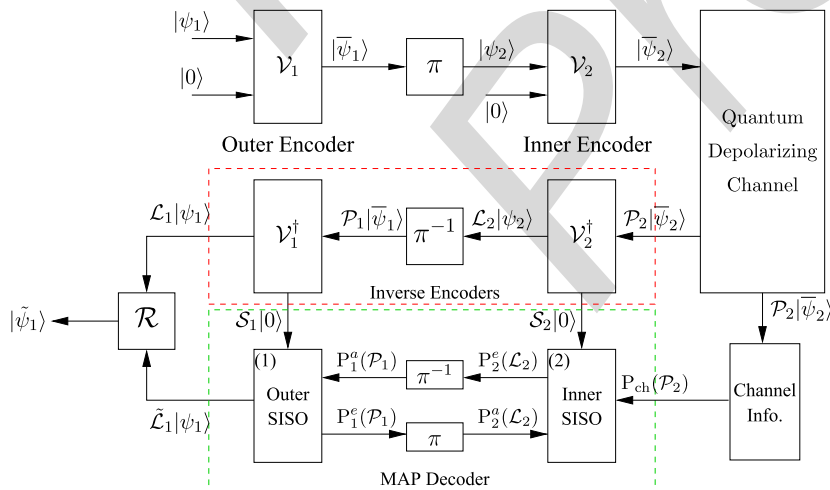

FIGURE 16. System Model: Quantum communication system relying on concatenated quantum stabilizer codes. $P_i^a(.)$, $P_i^e(.)$ and $P_i^o(.)$ *denote the a-priori, extrinsic and a-posteriori probabilities related to the ith decoder.*

an infinitesimally low error rate is achieved. It was found in [39] and [98] that QCCs cannot be simultaneously recursive and non-catastrophic. In order to overcome this problem, Wilde *et al.* [34] and Wilde and Hsieh [36] proposed to employ entanglement-assisted inner codes, which are recursive as well as non-catastrophic. Therefore, the inner code should be an entanglement-assisted recursive and non-catastrophic code, while the outer code can be either an unassisted or an entanglement-assisted non-catastrophic code.

At the transmitter, the intended quantum information $|\psi_1\rangle$ is encoded by an $[n_1, k_1]$ outer encoder $\mathcal{V}_1$ using $(n_1 - k_1)$ auxiliary qubits, which are initialized to the state $|0\rangle$, as depicted in Eq. (69). The encoded qubits $|\overline{\psi}_1\rangle$ are passed through a quantum interleaver (π). The resultant permuted qubits $|\psi_2\rangle$ are fed to an $[n_2, k_2]$ inner encoder $\mathcal{V}_2$, which encodes them into the codewords $|\overline{\psi}_2\rangle$ using $(n_2 - k_2)$ auxiliary qubits initialized to the state $|0\rangle$.[22] The n-qubit codewords $|\overline{\psi}_2\rangle$, where we have $n = n_1 n_2$, are then serially transmitted over a quantum depolarizing channel, which imposes an n-tuple error $\mathcal{P}_2 \in \mathcal{G}_n$ on the transmitted codewords.

At the receiver, the received codeword $|\hat{\psi}_2\rangle = \mathcal{P}_2|\overline{\psi}_2\rangle$ is passed through the inverse encoder $\mathcal{V}_2^\dagger$, which yields the corrupted information word of the inner encoder $\mathcal{L}_2|\psi_2\rangle$ and the associated $(n_2 - k_2)$-qubit syndrome $\mathcal{S}_2|0_{(n_2-k_2)}\rangle$ as depicted previously in Eq. (85), where $\mathcal{L}_2$ denotes the error imposed on the logical qubits of the inner encoder, while $\mathcal{S}_2$ represents the error inflicted on the remaining $(n_2 - k_2)$ qubits. The corrupted logical qubits of the inner encoder are de-interleaved, resulting in $\mathcal{P}_1|\overline{\psi}_1\rangle$, which is then passed through the inverse outer encoder $\mathcal{V}_1^\dagger$. This gives the corrupted information word of the outer encoder $\mathcal{L}_1|\psi_1\rangle$ and the associated $(n_1 - k_1)$-qubit syndrome $\mathcal{S}_1|0_{(n_1-k_1)}\rangle$.

The next step is to estimate the error $\mathcal{L}_1$ for the sake of ensuring that the original logical qubit $|\psi_1\rangle$ can be restored by applying the recovery operation $\mathcal{R}$. For estimating $\mathcal{L}_1$, both the syndromes $\mathcal{S}_2|0_{(n_2-k_2)}\rangle$ and $\mathcal{S}_1|0_{(n_1-k_1)}\rangle$ are fed to the inner and outer Soft-In Soft-Out (SISO) decoders [27], respectively, which engage in iterative decoding [33], [34] in order to yield the estimated error $\tilde{\mathcal{L}}_1$. The corresponding block is marked as 'MAP Decoder' in Fig. 16. Here, $\mathrm{P}_i^a(.)$, $\mathrm{P}_i^e(.)$ and $\mathrm{P}_i^o(.)$ denote the *a-priori*, *extrinsic* and *a-posteriori* probabilities [27] related to the ith decoder. Based on this notation, the turbo decoding process can be summarized as follows:

- The inner SISO decoder of Fig. 16 uses the channel information $\mathrm{P}_{ch}(\mathcal{P}_2)$, the *a-priori* information gleaned from the outer decoder $\mathrm{P}_2^a(\mathcal{L}_2)$ (initialized to be equiprobable for the first iteration) and the syndrome $\mathcal{S}_2$ to compute the *extrinsic* information $\mathrm{P}_2^e(\mathcal{L}_2)$. For a coded sequence of length N, we have $\mathcal{P}_2 = [\mathcal{P}_{2,1}, \mathcal{P}_{2,2}, \ldots, \mathcal{P}_{2,t}, \ldots, \mathcal{P}_{2,N}]$, where

$\mathcal{P}_{2,t} = [\mathcal{P}_{2,t}^1, \mathcal{P}_{2,t}^2, \ldots, \mathcal{P}_{2,t}^n]$. The channel information $\mathbf{P}_{ch}(\mathcal{P}_{2,t})$ is computed assuming that each qubit is independently transmitted over a quantum depolarizing channel having a depolarizing probability of p, whose channel transition probabilities are given by [33]:

$$\mathbf{P}_{ch}(P_{2,t}^i) = \begin{cases} 1-p, & \text{if } \mathcal{P}_{2,t}^i = \mathbf{I} \\ p/3, & \text{if } \mathcal{P}_{2,t}^i \in \{\mathbf{X}, \mathbf{Z}, \mathbf{Y}\}. \end{cases} \quad (98)$$

- $\mathrm{P}_2^e(\mathcal{L}_2)$ is passed through the quantum de-interleaver (π^{-1}) of Fig. 16 to generate the *a-priori* information for the outer decoder $\mathrm{P}_1^a(\mathcal{P}_1)$.
- Based on both the *a-priori* information $\mathrm{P}_1^a(\mathcal{P}_1)$ and on the syndrome $\mathcal{S}_1$, the outer SISO decoder of Fig. 16 computes both the *a-posteriori* information $\mathrm{P}_1^o(\mathcal{L}_1)$ and the *extrinsic* information $\mathrm{P}_1^e(\mathcal{P}_1)$.
- $\mathrm{P}_1^e(\mathcal{P}_1)$ is then interleaved to obtain $\mathrm{P}_2^a(\mathcal{L}_2)$, which is fed back to the inner SISO decoder of Fig. 16. This iterative procedure continues, until either convergence is achieved or the maximum affordable number of iterations is reached.
- Finally, a qubit-based MAP decision is made for determining the most likely error coset $\mathcal{L}_1$. It must be mentioned here that both the inner and outer SISO decoders employ the degenerate decoding approach of [33], which aims for finding the 'most likely error coset' rather than the 'most likely error' acting on the logical qubits $\mathcal{L}_i$, as we will discuss in the next section.

C. DEGENERATE ITERATIVE DECODING

As discussed in Section IV-B, quantum codes exhibit the intrinsic property of degeneracy, which is also obvious from Eq. (85). More explicitly, we have:

$$\mathcal{S}|0_{n-k}\rangle = \mathcal{S}_1|0\rangle \otimes \cdots \otimes \mathcal{S}_{n-k}|0\rangle. \quad (99)$$

Since, we have $\mathcal{S}_i \in \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}$, we can re-write Eq. (99) as follows [33]:

$$\mathcal{S}|0_{n-k}\rangle \equiv \epsilon|s_1\rangle \otimes \cdots \otimes |s_{n-k}\rangle, \quad (100)$$

where $\epsilon \in \{\pm 1, \pm i\}$, and:

$$s_i = 0 \quad \text{if } \mathcal{S}_i = \mathbf{I} \text{ or } \mathcal{S}_i = \mathbf{Z},$$
$$s_i = 1 \quad \text{otherwise}. \quad (101)$$

For example, if $\mathcal{S}_1 = \mathbf{Y}$ and $\mathcal{S}_i = \mathbf{I}$ for $i \neq 1$, since $\mathbf{Y} = i\mathbf{XZ}$, we get $\mathcal{S}|0_{n-k}\rangle = i|1\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$.

Observing the $(n - k)$ syndrome qubits of Eq. (100) collapses them to the classical syndrome $s = \{s_1, \ldots, s_{n-k}\}$, which is equivalent to the symplectic product of P and H, i.e. $s = (P \star H_i)_{1 \leq i \leq n-k}$. More precisely, the syndrome sequence $|0_{n-k}\rangle$ is invariant to the $\mathbf{Z}$-component of $\mathcal{S}$ since $\mathbf{Z}|0\rangle = |0\rangle$. Let S be the effective $2(n - k)$-bit error on the syndrome, which may be decomposed as $S = S^x + S^z$, where S^x and S^z are the $\mathbf{X}$ and $\mathbf{Z}$ components of S, respectively. Then s only reveals S^x. Hence, two distinct error sequences $P = (L : S^x + S^z)V$ and $P' = (L : S^x + S'^z)V$, which only differ in the $\mathbf{Z}$-component of $\mathcal{S}$, yield the same syndrome s.

---

[22] Please note that this is a general schematic. The inner code can be either an un-assisted or an entanglement-assisted code. However, it is advisable to use an entanglement-assisted inner code for the sake of ensuring an unbounded minimum distance of the resultant concatenated code.

Furthermore, it must be noted that both P and P' have the same logical error L. Therefore, P and P' differ only by the stabilizer group and are known as degenerate errors, which do not have to be distinguished, since they can be corrected by the same recovery operation L^{-1}.

Recall that a classical syndrome-based MAP decoder aims for finding the most likely error for a given syndrome, which may be modeled as:

$$L(S) = \text{argmax}_L P(L|S), \tag{102}$$

where $P(L|S)$ denotes the probability of experiencing the logical error L imposed on the transmitted qubits, given that the syndrome of the received qubits is S. By contrast, quantum codes employ degenerate decoding, which aims for finding the most likely error coset $C(L, S^x)$ associated with the observed syndrome S^x. The coset $C(L, S^x)$ is defined as [33]:

$$C(L, S^x) = \{P = (L : S^x + S^z)V\} \quad \forall S^z \in \{\mathbf{I}, \mathbf{Z}\}^{n-k}. \tag{103}$$

Therefore, a degenerate MAP decoder yields:

$$L(S^x) = \text{argmax}_L P(L|S^x), \tag{104}$$

where we have:

$$P(L|S^x) \equiv \sum_{S^z \in \{\mathbf{I}, \mathbf{Z}\}^{n-k}} P(L|(S^x + S^z)). \tag{105}$$

The MAP decoder of Fig. 16 consists of two serially concatenated SISO decoders, which employ the aforementioned degenerate decoding approach. Fig. 17 shows the general schematic of a SISO decoder, where the Pauli operators $\mathcal{P}$, $\mathcal{L}$ and $\mathcal{S}$ are replaced by the effective operators P, L and S^x, respectively. The SISO decoder of Fig. 17 yields the *a-posteriori* information pertaining to L and P based on the classic forward-backward recursive coefficients α and β, as follows [33]:

- For a coded sequence of duration N, let $P = [P_1, P_2, \ldots, P_t, \ldots, P_N]$ and $L = [L_1, L_2, \ldots, L_t, \ldots, L_N]$, where $P_t \in G_n$ and $L_t \in G_k$. More explicitly, $P_t = [P_t^1, P_t^2, \ldots, P_t^n]$ and $L_t = [L_t^1, L_t^2, \ldots, L_t^k]$.
- Let us decompose the seed transformation as $U = (U_M : U_P)$, where U_M is the binary matrix formed
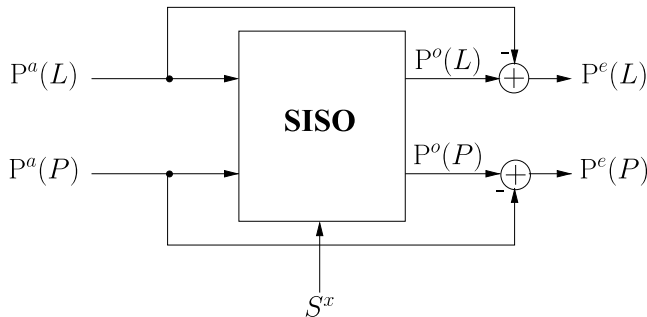
by the first $2m$ columns of U, while U_P is the binary matrix formed by the last $2n$ columns of U. Therefore, we have:

$$M_t = (M_{t-1} : L_t : S_t) U_M, \tag{106}$$
$$P_t = (M_{t-1} : L_t : S_t) U_P. \tag{107}$$

- Let $\alpha_t(M_t)$ be the forward recursive coefficient, which is defined as follows:

$$\alpha_t(M_t) \triangleq P\left(M_t | S_{\leq t}^x\right),$$
$$\propto \sum_{\mu, \lambda, \sigma} P^a(L_t = \lambda) P^a(P_t) \alpha_{t-1}(\mu), \tag{108}$$

where $S_{\leq t}^x \triangleq \left(S_j^x\right)_{0 \leq j \leq t}$, $\mu \in G_m$, $\lambda \in G_k$ and $\sigma \in G_{n-k}$, while $\sigma = \sigma_x + \sigma_z$, having $\sigma_x = S_t^x$. Furthermore, we have $P_t = (\mu : \lambda : \sigma)U_P$ and $M_t = (\mu : \lambda : \sigma)U_M$.

- Let $\beta_t(M_t)$ be the backward recursive coefficient, which is defined as:

$$\beta_t(M_t) \triangleq P\left(M_t | S_{>t}^x\right),$$
$$\propto \sum_{\lambda, \sigma} P^a(L_t = \lambda) P^a(P_{t+1}) \beta_{t+1}(M_{t+1}), \tag{109}$$

where $S_{>t}^x \triangleq \left(S_j^x\right)_{t < j \leq N}$, $P_{t+1} = (M_t : \lambda : \sigma)U_P$ and $M_{t+1} = (M_t : \lambda : \sigma)U_M$.

- Finally, we have the *a-posteriori* probabilities $P^o(L_t)$ and $P^o(P_t)$, which are given by:

$$P^o(L_t) \triangleq P(L_t | S^x),$$
$$\propto \sum_{\mu, \sigma} P^a(L_t) P^a(P_t) \alpha_{t-1}(\mu) \beta_t(M_t), \tag{110}$$

$$P^o(P_t) \triangleq P(P_t | S^x),$$
$$\propto \sum_{\mu, \lambda, \sigma} P^a(P_t) P^a(L_t = \lambda) \alpha_{t-1}(\mu) \beta_t(M_t), \tag{111}$$

where $S^x \triangleq \left(S_t^x\right)_{0 \leq t \leq N}$, $P_t = (\mu : L_t : \sigma)U_P$ and $M_t = (\mu : L_t : \sigma)U_M$.

- The marginalized probabilities $P^o(L_t^j)$, for $j \in \{0, k-1\}$, and $P^o(P_t^j)$, for $j \in \{0, n-1\}$, are then computed from $P^o(L_t^j)$ and $P^o(P_t^j)$, respectively. The *a-priori* information is then removed in order to yield the *extrinsic* probabilities [34], i.e we have:

$$\ln[P^e(L_t^j)] = \ln[P^o(L_t^j)] - \ln[P^a(L_t^j)], \tag{112}$$
$$\ln[P^e(P_t^j)] = \ln[P^o(P_t^j)] - \ln[P^a(P_t^j)]. \tag{113}$$

It has to be mentioned here that the property of degeneracy is only an attribute of auxiliary qubits and the ebits of an entanglement-assisted code do not contribute to it. This is because both $\mathbf{X}$ as well as $\mathbf{Z}$ errors acting on the transmitter's half of ebits give distinct results when measured in the Bell basis, i.e. $\mathcal{E}^{T_X} | \phi_c^+ \rangle^{T_X R_X}$ gives four distinct Bell states for $\mathcal{E}_j^{T_X} \in \{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{Y}\}$. Consequently, the degeneracy is a function of a and reduces to zero for $a = 0$.

FIGURE 17. General schematic of a SISO decoder. $P^a(.)$, $P^e(.)$ and $P^o(.)$ denote the a-priori, extrinsic and a-posteriori probabilities.

VI. EXIT-CHART AIDED CODE DESIGN

EXIT charts [27], [32], [107] are capable of visualizing the convergence behaviour of iterative decoding schemes by exploiting the input/output relations of the constituent decoders in terms of their average Mutual Information (MI) characteristics. The EXIT chart analysis not only allows us to dispense with the time-consuming Monte-Carlo simulations, but also facilitates the design of capacity approaching codes without resorting to the tedious analysis of their distance spectra. Therefore, they have been extensively employed for designing near-capacity classical codes [108]–[111]. Let us recall that the EXIT chart of a serially concatenated scheme visualizes the exchange of four MI terms, i.e. average *a-priori* MI of the outer decoder I_A^1, average *a-priori* MI of the inner decoder I_A^2, average *extrinsic* MI of the outer decoder I_E^1, and average *extrinsic* MI of the inner decoder I_E^2. More specifically, I_A^1 and I_E^1 constitute the EXIT curve of the outer decoder, while I_A^2 and I_E^2 yield the EXIT curve of the inner decoder. The MI transfer characteristics of both the decoders are plotted in the same graph, with the *x* and *y* axes of the outer decoder swapped. The resultant EXIT chart quantifies the improvement in the mutual information as the iterations proceed, which can be viewed as a stair-case-shaped decoding trajectory. An open tunnel between the two EXIT curves ensures that the decoding trajectory reaches the $(1, y)$ point of perfect convergence.

In our prior work [35], we extended the application of EXIT charts to the quantum domain by appropriately adapting the conventional non-binary EXIT chart generation technique for the quantum syndrome decoding approach. Recall from Section IV-C that a quantum code is equivalent to a classical code. More specifically, the decoding of a quantum code is essentially carried out with the aid of the equivalent classical code by exploiting the additional property of degeneracy, as discussed in Section V-C. Quantum codes employ syndrome decoding, which yields information about the error-sequence rather than about the information-sequence or coded qubits, hence avoiding the observation of the latter sequences, which would collapse them back to the classical domain. Since a quantum code has an equivalent classical representation and the depolarizing channel is analogous to a Binary Symmetric Channel (BSC), we employ the EXIT chart technique to design hashing bound approaching concatenated quantum codes. The major difference between the EXIT charts conceived for the classical and quantum domains is that while the former models the *a-priori* information concerning the input bits of the inner encoder (and similarly the output bits of the outer encoder), the latter models the *a-priori* information concerning the corresponding error-sequence, i.e. the error-sequence related to the input qubits of the inner encoder L_2 (and similarly the error-sequence related to the output qubits of the outer encoder P_1).

Similar to the classical EXIT charts, it is assumed that the interleaver length is sufficiently high to ensure that [27], [32]:

- the *a-priori* values are fairly uncorrelated; and
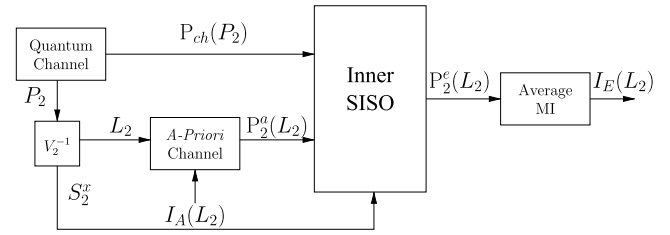- the *a-priori* information has a Gaussian distribution.

FIGURE 18. System model for generating the EXIT chart of the inner decoder [35].

Fig. 18 shows the system model used for generating the EXIT chart of the inner decoder. Here, a quantum depolarizing channel having a depolarizing probability of *p* generates the error sequence P_2, which is passed through the inverse inner encoder V_2^{-1}. This yields both the error imposed on the logical qubits L_2 and the syndrome S_2^x. The *a-priori* channel block then models the *a-priori* information $P_1^a(L_2)$ such that the average MI between the actual error L_2 and the *a-priori* probabilities $P_2^a(L_2)$ is given by $I_A(L_2)$ [27], [32], [107]. More explicitly, we have $I_A(L_2) = I[L_2, P_2^a(L_2)]$, where I denotes the average MI function. Moreover, the *i*th and $(N + i)$th bits of the effective error vector L_2 can be visualized as 4-ary symbols. Consequently, similar to classical non-binary EXIT charts [97], [112], the *a-priori* information is modeled using an independent Gaussian distribution with a mean of zero and variance of σ_A^2, assuming that the **X** and **Z** errors constituting the 4-ary symbols are independent.[23] Based on the channel information $P_{ch}(P_2)$, on the syndrome S_2^x and on the *a-priori* information, the inner SISO decoder generates the *extrinsic* information $P_2^e(L_2)$ by using the degenerate decoding approach of Section V-C. Finally, the *extrinsic* average MI $I_E(L_2) = I[L_2, P_2^e(L_2)]$ between L_2 and $P_2^e(L_2)$ is computed. Since the equivalent classical capacity of a quantum channel is given by the capacity achievable over each half of the 4-ary symmetric channel, $I_E(L_2)$ is the normalized MI of the 4-ary symbols, which can be computed based on [97] and [113] as:

$$I_E(L_2) = \frac{1}{2}\left(2 + E\left[\sum_{m=0}^{3} P_2^e(L_2^{j(m)}) \log_2 P_2^e(L_2^{j(m)})\right]\right), \quad (114)$$

where E is the expectation (or time average) operator and $L_2^{j(m)}$ is the m$^{\text{th}}$ hypothetical error imposed on the logical qubits. More explicitly, since the error on each qubit is represented by an equivalent pair of classical bits, $L_2^{j(m)}$ is a 4-ary classical symbol associated with m $\in \{0, 3\}$. The process is repeated for a range of $I_A(L_2) \in [0, 1]$ values for the sake of obtaining the *extrinsic* information transfer characteristics at the depolarizing probability *p*. The resultant inner EXIT transfer function T_2 of the specific inner decoder may be

---

[23]Under the idealized asymptotic conditions of having an infinite-length interleaver, $I_A(L_2)$ may be accurately modeled by the Gaussian distribution. As and when shorter interleavers are used, the Gaussian assumption becomes less accurate, hence in practice a histogram-based approximation may be relied upon.

defined as follows:

$$I_E(L_2) = T_2[I_A(L_2), p], \qquad (115)$$

which is a function of the channel's depolarizing probability p.

The system model used for generating the EXIT chart of the outer decoder is depicted in Fig. 19. As inferred from Fig. 19, the EXIT curve of the outer decoder is independent of the channel's output information. The *a-priori* information is generated by the *a-priori* channel based on P_1 (error on the physical qubits of the second decoder) and $I_A(P_1)$, which is the average MI between P_1 and $P_1^a(P_1)$. Furthermore, as for the inner decoder, P_1 is passed through the inverse outer encoder V_1^{-1} to compute S_1^x, which is fed to the outer SISO decoder to yield the *extrinsic* information $P_1^e(P_1)$. The average MI between P_1 and $P_1^e(P_1)$ is then calculated using Eq. (114). The resultant EXIT chart is characterized by the following MI transfer function:

$$I_E(P_1) = T_1[I_A(P_1)], \qquad (116)$$

where T_1 is the outer EXIT transfer function, which is dependent on the specific outer decoder, but it is independent of the depolarizing probability p.
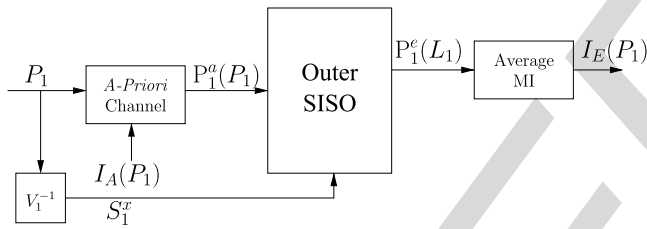
FIGURE 19. System model for generating the EXIT chart of the outer decoder [35].

Finally, the MI transfer characteristics of both decoders characterized by Eq. (115) and Eq. (116) are plotted in the same graph, with the x and y axes of the outer decoder swapped. For the sake of approaching the achievable capacity of Fig. 3, *our EXIT-chart aided design aims for creating a narrow, but marginally open tunnel between the EXIT curves of the inner and outer decoders at the highest possible depolarizing probability (analogous to the lowest possible SNR for a classical channel)*. For a given noise limit p^* and the desired code parameters, this may be achieved in two steps. We first find that specific inner code, which yields the largest area under its EXIT-curve at the noise limit p^*. Once the optimal inner code is selected, we find the optimal outer code, whose EXIT-curve gives the best match with the chosen inner code. The narrower the tunnel-area between the inner and outer decoder's EXIT curve, the lower is the deviation from achievable capacity, which may be quantified using Eq. (4).

VII. A KEY TO HASHING BOUND: QUANTUM IRREGULAR CONVOLUTIONAL CODES

In this section, we exploit the EXIT-chart aided design criterion of Section VI to design concatenated codes, which

operate arbitrarily close to the hashing bound. Here, we assume that we already have the optimal inner code. *More explicitly, our design objective is to find the optimal outer code C having a coding rate R_Q, which gives the best match with the given inner code, i.e. whose EXIT curve yields a marginally open tunnel with the given inner decoder's EXIT curve at a depolarizing probability close to the hashing bound.* For the sake of achieving this objective, a feasible design option could be to create the outer EXIT curves of all the possible convolutional codes to find the optimal code C, which gives the best match, as we did in our prior work [35]. To circumvent this exhaustive code search, in this contribution we propose to invoke Quantum Irregular Convolutional Codes (QIRCCs) for achieving EXIT-curve matching.

Similar to the classical Irregular Convolutional Code (IRCC) of [114], our proposed QIRCC employs a family of Q subcodes C_q, $q \in \{1, 2, \ldots, Q\}$, for constructing the target code C. Due to its inherent flexibility, the resultant QIRCC provides a better EXIT-curve match than any single code, when used as the outer component in the concatenated structure of Fig. 16. The qth subcode has a coding rate of r_q and it encodes a specifically designed fraction of the original information qubits to $\varrho_q N$ encoded qubits. Here, N is the total length of the coded frame. More specifically, for a Q-subcode IRCC, ϱ_q is the qth IRCC weighting coefficient satisfying the following constraints [114], [115]:

$$\sum_{q=1}^{Q} \varrho_q = 1, \quad R_Q = \sum_{q=1}^{Q} \varrho_q r_q, \quad \varrho_q \in [0, 1], \quad \forall q, \qquad (117)$$

which can be conveniently represented in the following matrix form:

$$\begin{pmatrix} 1 & 1 & \ldots & 1 \\ r_1 & r_2 & \ldots & r_Q \end{pmatrix} \begin{pmatrix} \varrho_1 & \varrho_2 \ldots & \varrho_Q \end{pmatrix}^T = \begin{pmatrix} 1 \\ R_Q \end{pmatrix}$$

$$\mathbf{r}\,\boldsymbol{\varrho} = \mathbf{R}. \qquad (118)$$

Hence, as shown in Fig. 20, the input stream is partitioned into Q sub-frames,[24] which are assembled back into a single N-qubit stream after encoding.
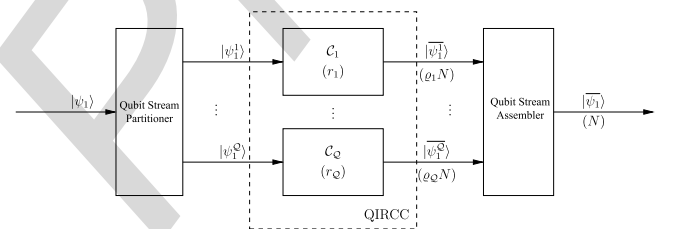

FIGURE 20. Structure of a Q-subcode QIRCC encoder.

In the context of classical IRCCs, the subcodes C_q are constructed from a mother code [114], [115]. More specifically, high-rate subcodes are obtained by puncturing the

---

[24]This is only true if all subcodes are active. If $\varrho_q = 0$ for the qth subcode, then C_q is not activated. Therefore, the input stream is only divided among the active subcodes.

mother code, while the lower rates are obtained by adding more generators. However, unlike classical codes, puncturing is not easy to implement for quantum codes, since the resultant punctured code must satisfy the symplectic criterion, as in [116]. In this context, in order to design the constituent subcodes of our proposed QIRCC, we selected 5 strong randomly-constructed memory-3 quantum convolutional codes with quantum code rates {1/4, 1/3, 1/2, 2/3, 3/4}, which met the non-catastrophic criterion of [33]. More explicitly, for the sake of achieving a random construction for the Clifford encoder specifying the quantum convolutional code, we used the classical random walk algorithm over the $(n + m)$-qubit Clifford group as in [117]. The seed transformations of the resultant subcodes having rates {1/4, 1/3, 1/2, 2/3, 3/4} are given below:

$$U_1 = \{9600, 691, 11713, 4863, 1013, 6907, 1125, 828,$$
$$10372, 6337, 5590, 11024, 12339, 3439\},$$

$$U_2 = \{3968, 1463, 2596, 3451, 1134, 3474, 657, 686,$$
$$3113, 1866, 2608, 2570\},$$

$$U_3 = \{848, 1000, 930, 278, 611, 263, 744, 260, 356, 880\},$$

$$U_4 = \{529, 807, 253, 1950, 3979, 2794, 956, 1892, 3359,$$
$$2127, 3812, 1580\},$$

$$U_5 = \{62, 6173, 4409, 12688, 7654, 10804, 1763, 15590,$$
$$6304, 3120, 2349, 1470, 9063, 4020\}. \qquad (119)$$

The EXIT curves of these QIRCC subcodes are shown in Fig. 21, whereby the memory-3 subcodes of Eq. (119) are indicated by solid lines. Furthermore, in order to facilitate

accurate EXIT curve matching with a sufficiently versatile and diverse set of inner EXIT functions, we also selected 5 weak randomly-constructed memory-1 subcodes for the same range of coding rates, i.e. {1/4, 1/3, 1/2, 2/3, 3/4}. The corresponding seed transformations are as follows:

$$U_6 = \{475, 194, 526, 422, 417, 988, 426, 611, 831, 84\},$$

$$U_7 = \{26, 147, 149, 99, 112, 184, 64, 139\},$$

$$U_8 = \{37, 55, 58, 35, 57, 54\},$$

$$U_9 = \{57, 248, 99, 226, 37, 93, 244, 54\},$$

$$U_{10} = \{469, 634, 146, 70, 186, 969, 387, 398, 807, 452\},$$
$$(120)$$

and their EXIT curves are plotted in Fig. 21 with the aid of dotted lines. It must be mentioned here that the range of coding rates chosen for the QIRCC subcodes can be expanded such that the EXIT curves cover a larger portion of the EXIT plot, which further improves curve matching. However, this increases the encoding and decoding complexity.

Based on our proposed QIRCC, relying on the 10 subcodes specified by Eq. (119) and (120), the input bit stream is divided into 10 fractions corresponding to the 10 different-rate subcodes. The specific optimum fractions to be encoded by these codes are found by dynamic programming. More specifically, since the QCCs belong to the class of linear codes, the EXIT curves of the 10 subcodes, given in Fig. 21, are superimposed onto each other after weighting by the appropriate fraction-based weighting coefficients, which are determined by minimizing the area of the open EXIT-tunnel. To elaborate a little further, the transfer function of the QIRCC is given by the weighted sum of each subcode's transfer function as shown below:

$$I_E(P_1) = T_1[I_A(P_1)] = \sum_{q=1}^{Q} \varrho_q \, T_1^q[I_A(P_1)], \qquad (121)$$

where $T_1^q[I_A(P_1)]$ is the transfer function of the qth subcode. For a given inner EXIT curve and outer code rate R_Q, we employ the curve matching algorithm of [114] and [115] for optimizing the weighting coefficients ϱ of our proposed QIRCC such that the square of the error between the inner and inverted outer EXIT curves is minimized subject to Eq. (117). More explicitly, the error function may be modeled as:

$$e(i) = T_2[i, p] - T_1^{-1}[i], \qquad (122)$$

where $p = (p^* - \epsilon)$ given that p^* is the noise limit defined by the hashing bound and ϵ is an arbitrarily small number. The corresponding matrix-based notation may be formulated as [114], [115]:

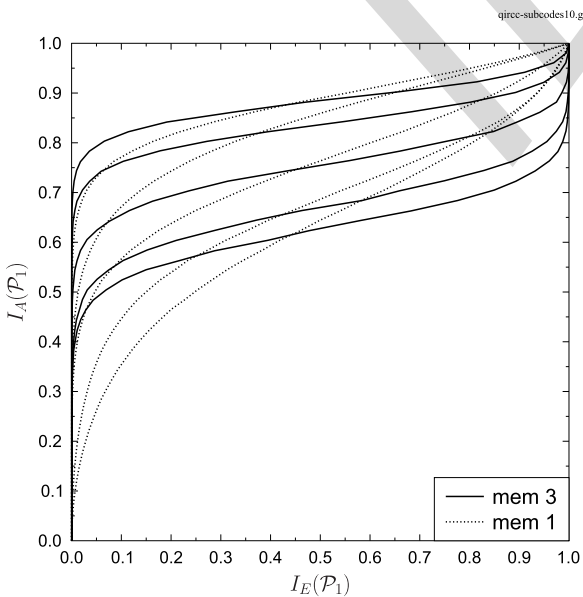$$\mathbf{e} = \mathbf{b} - \mathbf{A}\varrho, \qquad (123)$$

qircc-subcodes10.gle

FIGURE 21. Outer EXIT curves (inverted) of our QIRCC subcodes having code rates {1/4, 1/3, 1/2, 2/3, 3/4} for both memory-3 as well as memory-1.

where we have:

$$\mathbf{b} = \begin{pmatrix} T_2[i_1, p] \\ T_2[i_2, p] \\ \vdots \\ T_2[i_N, p] \end{pmatrix}, \quad \text{and}$$

$$\mathbf{A} = \begin{pmatrix} T_1^{1^{-1}}[i_1] & T_1^{2^{-1}}[i_1] & \dots & T_1^{Q^{-1}}[i_1] \\ T_1^{1^{-1}}[i_2] & T_1^{2^{-1}}[i_2] & \dots & T_1^{Q^{-1}}[i_2] \\ \vdots & \vdots & \vdots & \vdots \\ T_1^{1^{-1}}[i_N] & T_1^{2^{-1}}[i_N] & \dots & T_1^{Q^{-1}}[i_N] \end{pmatrix}. \quad (124)$$

Here, N denotes the number of sample points such that $i \in \{i_1, i_2, \dots, i_N\}$ and it is assumed that $N > Q$. Furthermore, the error should be greater than zero for the sake of ensuring an open tunnel, i.e. we have:

$$e(i) > 0, \quad \forall i \in [0, 1]. \quad (125)$$

The resultant cost function, i.e. sum of the square of the errors, is given by [115]:

$$\mathcal{J}(\varrho_1, \dots, \varrho_Q) = \int_0^1 e(i)^2 di, \quad (126)$$

which may also be written as:

$$\mathcal{J}(\boldsymbol{\varrho}) = \mathbf{e}^T \mathbf{e}. \quad (127)$$

The overall process may be encapsulated as follows:

$$\boldsymbol{\varrho}_{opt} = \arg \min_{\boldsymbol{\varrho}} \mathcal{J}(\boldsymbol{\varrho}), \quad (128)$$

subject to Eq. (117) and (125), which is a convex optimization problem. The unconstrained optimal solution for Eq. (128) is found iteratively using steepest descent approach with a gradient of $\partial \mathcal{J}(\boldsymbol{\varrho})/\partial \boldsymbol{\varrho} = 2\mathbf{e}$, which is then projected onto the constraints defined in Eq. (117) and (125). Further details of this optimization algorithm can be found in [114] and [115].

VIII. RESULTS AND DISCUSSIONS

For the sake of demonstrating the curve matching capability of our proposed QIRCC, we designed a rate-1/9 concatenated code relying on the rate-1/3 entanglement-assisted inner code of [34] and [36], namely "PTO1REA", with our proposed QIRCC as the outer code. Since the entanglement consumption rate of "PTO1REA" is 2/3, the resultant code has an entanglement consumption rate of 6/9, for which the corresponding noise limit is $p^* = 0.3779$ according to Eq. (5) [34]. Furthermore, since we intend to design a rate-1/9 system with a rate-1/3 inner code, we have $R_Q = 1/3$. Hence, for a target coding rate of 1/3, we used the optimization algorithm discussed in Section VII for the sake of finding the optimum weighting coefficients of Eq. (128) at the highest possible depolarizing probability $p = p^* - \epsilon$. It was found that we only need to invoke two subcodes out of the 10 possible subcodes, based on $\boldsymbol{\varrho} = [0\ 0\ 0\ 0\ 0.168\ 0.832\ 0\ 0\ 0\ 0]^T$, for attaining a marginally open tunnel, which occurs at $p = 0.345$, as shown in Fig. 22. Hence, the resultant code
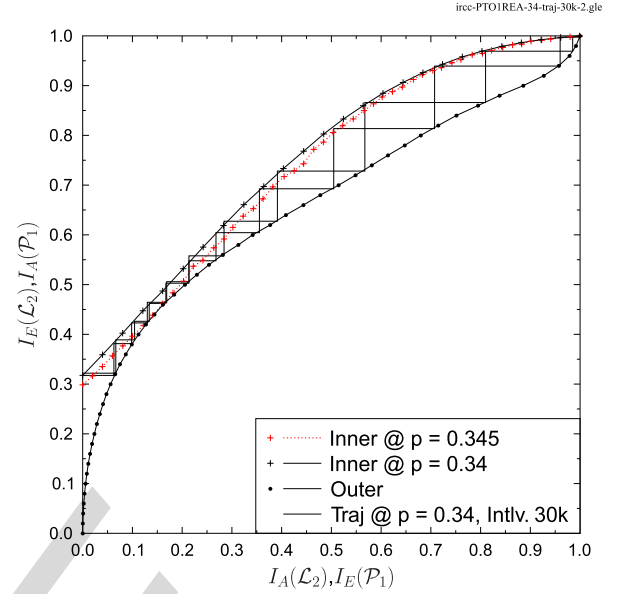

FIGURE 22. EXIT curves of the concatenated rate-1/9 system, with PTO1REA as the inner code and QIRCC as the outer, at $p = 0.345$ and $p = 0.34$.

has a convergence threshold of $p = 0.345$, which is only $\left[10 \times \log_{10}(\frac{0.345}{0.3779})\right] = 0.4$ dB from the noise limit of 0.3779. Fig. 22 also shows two decoding trajectories at $p = 0.34$ for a 30,000 qubit long interleaver. As gleaned from the figure, the decoding trajectories closely follow the EXIT curves reaching the (1, 1) point of perfect convergence.

The corresponding Word Error Rate (WER) performance curves recorded for our QIRCC-based optimized design using a 3,000 qubit long interleaver are seen in Fig. 23, where the WER is reduced upon increasing the number of iterations. More explicitly, our code converges to a low WER for $p \leq 0.345$. Thus, this convergence threshold matches the one predicted using EXIT charts in Fig. 22. More explicitly, since the EXIT chart tunnel closes for $p > 0.345$, the system
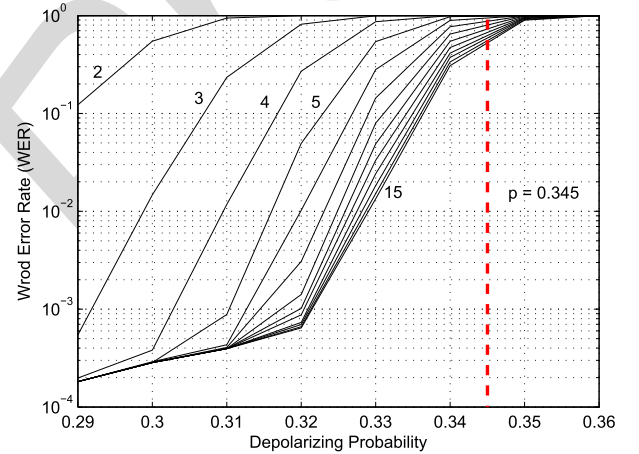

FIGURE 23. WER performance curves with increasing iteration number for an interleaver length of 3,000 qubits. *Rate-1/9 concatenated code, relying on PTO1REA as the inner code and the proposed QIRCC as the outer code, was used.*

fails to converge, if the depolarizing probability is increased beyond 0.345. Hence, the performance does not improve upon increasing the number of iterations if the depolarizing probability exceeds the threshold. By contrast, when the depolarizing probability is below the threshold, the WER improves at each successive iteration. It should also be noted that the performance improves with diminishing returns at a higher number of iterations.
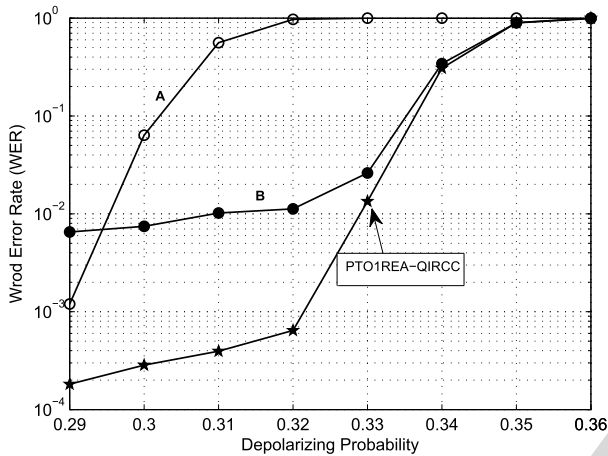

FIGURE 24. Comparison of WER performance of our QIRCC-based optimized rate-1/9 QTC with the PTO1REA-PTO1R configuration of [34] (labeled "A") and the exhaustive-search based optimized QTC of [35] (labeled "B") for an interleaver length of 3,000 qubits and a maximum of 15 iterations.

Fig. 24 compares our QIRCC-based optimized design with the rate-1/9 "PTO1REA-PTO1R" configuration of [34], which is labeled "A" in the figure. An interleaver length of 3000 qubits was used. For the "PTO1REA-PTO1R" configuration, the turbo cliff region emerges around 0.31, which is within 0.9 dB of the noise limit. Therefore, our QIRCC-based design outperforms the "PTO1REA-PTO1R" configuration of [34]. More specifically, the "PTO1REA-PTO1R" configuration yields a WER of 10^{-3} at $p = 0.29$, while our design gives a WER of 10^{-3} at $p = 0.322$. Hence, our optimized design outperforms the "PTO1REA-PTO1R" configuration by about $\left[10 \times \log_{10}(\frac{0.29}{0.322}) \right] = 0.5$ dB at a WER of 10^{-3}. It must be mentioned here that the "PTO1REA-PTO1R" configuration may have a lower error floor than our design, yet our design exhibits a better performance in the turbo cliff region. We further compare our QIRCC-based optimized design with the exhaustive-search based optimized turbo code of [35], which is labeled "B" in Fig. 24. Both code designs have similar convergence threshold. However, our QIRCC-based design has a much lower error rate, resulting in a lower error floor as gleaned from Fig. 24.

IX. CONCLUSIONS AND DESIGN GUIDELINES
Powerful QECCs are required for stabilizing and protecting the fragile constituent qubits of quantum computation as well as communication systems against the undesirable decoherence. In line with the developments in the field of classical channel coding theory, this may be achieved by exploiting concatenated codes designs, which invoke iterative decoding. Therefore, in this paper we have laid out a slow-paced tutorial for designing hashing bound approaching concatenated quantum codes using EXIT charts. To bridge the gap between the quantum and classical channel coding theory, we have provided insights into the transition from the classical to the quantum code design. More specifically, with the help of toy examples, we have illustrated that quantum block codes as well as convolutional codes may be constructed from arbitrary classical linear codes. We then move onto the construction of concatenated quantum codes, focusing specifically on the circuit-based structure of the constituent encoders and their equivalent classical representation as well as the degenerate iterative decoding. Finally, we have detailed the procedure for generating EXIT charts for quantum codes and the principles of EXIT-chart aided design. Our design guidelines may be summarized as follows:

- As discussed in the context of our design objectives in Section II, we commence our design by determining the noise limit p^* for the desired code parameters, i.e the coding rate and the entanglement consumption rate of the resultant concatenated quantum code, which was introduced in Section II.
- We then proceed with the selection of the inner stabilizer code of Fig. 16, which has to be both recursive as well as non-catastrophic, as argued in Section V-B. Since the unassisted quantum codes cannot be simultaneously both recursive as well as non-catastrophic, we employ an entanglement-assisted code. Furthermore, the EA inner code of Fig. 16 may be either derived from the family of known classical codes, as discussed in Section IV or it may be constructed using random Clifford operations, which were discussed in Section V-A. At this point, the EXIT curves of Section VI may be invoked for the sake of finding that specific inner code, which yields the largest area under its EXIT-curve at the noise limit p^*.
- Finally, we find the optimal non-catastrophic outer code of Fig. 16, which gives the best EXIT-curve match with that of the chosen inner code. In this context, our EXIT-chart aided design of Section VI aims for creating a narrow, but marginally open tunnel between the EXIT curves of the inner and outer decoders at the highest possible depolarizing probability. The narrower the tunnel-area, the lower is the deviation from the hashing bound, which may be quantified using Eq. (4).

Recall that the desired code structure may also be optimized on the basis of a range of conflicting design challenges, which were illustrated in Fig. 4.

Furthermore, for the sake of facilitating the hashing bound approaching code design, we have proposed the structure of QIRCC, which constitutes the outer component of a concatenated quantum code. The proposed QIRCC allows us to dispense with the exhaustive code-search methods,

since it can be dynamically adapted to match any given inner code using EXIT charts. We have constructed a 10-subcode QIRCC and used it as an outer code in concatenation with a non-catastrophic and recursive inner convolutional code of [34] and [36]. In contrast to the concatenated codes of [34], whose performance is within 0.9 dB of the hashing bound, our QIRCC-based optimized design operates within 0.4 dB of the noise limit. Furthermore, at a WER of 10^{-3}, our design outperforms the design of [34] by around 0.5 dB. Our proposed design also yields lower error rate as compared to the exhaustive-search based optimized design of [35].

ACKNOWLEDGEMENT

REFERENCES

[1] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[2] P. A. M. Dirac, *The Principles of Quantum Mechanics*. London, U.K.: Oxford Univ. Press, 1982.

[3] S. Imre and F. Balazs, *Quantum Computing and Communications: An Engineering Approach*. New York, NY, USA: Wiley, 2005.

[4] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6515077

[5] D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 400, no. 1818, pp. 97–117, 1985.

[6] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 439, no. 1907, pp. 553–558, 1992.

[7] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134. [Online]. Available: http://portal.acm.org/citation.cfm?id=1398518.1399018

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, 1996, pp. 212–219. [Online]. Available: http://doi.acm.org/10.1145/237814.237866

[9] P. Botsinis, S. X. Ng, and L. Hanzo, "Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 990–1000, Mar. 2014.

[10] P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Low-complexity soft-output quantum-assisted multiuser detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems," *IEEE Access*, vol. 2, pp. 451–472, 2014.

[11] D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum-assisted routing optimization for self-organizing networks," *IEEE Access*, vol. 2, pp. 614–632, 2014.

[12] M. Born, *The Born–Einstein Letters*. London, U.K.: Walker, 1971.

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[14] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983. [Online]. Available: http://doi.acm.org/10.1145/1008908.1008920

[15] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179.

[16] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with single-photon two-qubit states," *J. Phys. A, Math. General*, vol. 35, no. 28, p. L407, 2002. [Online]. Available: http://stacks.iop.org/0305-4470/35/i=28/a=103

[17] K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," *Phys. Rev. Lett.*, vol. 89, p. 187902, Oct. 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.89.187902

[18] R. A. Malaney, "Location-dependent communications using quantum entanglement," *Phys. Rev. A*, vol. 81, p. 042319, Apr. 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.81.042319

[19] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.52.R2493

[20] J. Preskill, "Battling decoherence: The fault-tolerant quantum computer," *Phys. Today*, vol. 52, pp. 24–32, Jun. 1999.

[21] J. Preskill, "Reliable quantum computers," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 454, no. 1969, pp. 385–410, 1998.

[22] M. M. Wilde, *Quantum Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, May 2013. [Online]. Available: http://arxiv.org/abs/1106.1445

[23] D. G. Cory *et al.*, "Experimental quantum error correction," *Phys. Rev. Lett.*, vol. 81, pp. 2152–2155, Sep. 1998. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.81.2152

[24] M. D. Reed *et al.*, "Realization of three-qubit quantum error correction with superconducting circuits," *Nature*, vol. 482, no. 7385, pp. 382–385, Feb. 2012. [Online]. Available: http://dx.doi.org/10.1038/nature10786

[25] G. Arrad, Y. Vinkler, D. Aharonov, and A. Retzker, "Increasing sensing resolution with error correction," *Phys. Rev. Lett.*, vol. 112, p. 150801, Apr. 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.112.150801

[26] S. Lin and D. J. Costello, *Error Control Coding*. Pearson Education India. [Online]. Available: http://books.google.co.uk/books?id=BG08Zylo_7gC

[27] L. L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee, and S. X. Ng, *Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart-Aided Near-Capacity Designs for Wireless Channels*, 2nd ed. New York, NY, USA: Wiley, Mar. 2011.

[28] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, pp. 1613–1622, Mar. 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.55.1613

[29] P. W. Shor, "The quantum channel capacity and coherent information," in *Proc. MSRI Workshop Quantum Comput.*, 2002.

[30] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.

[31] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Proc. Tech. Program IEEE Int. Conf. Commun. (ICC)*, vol. 2. Geneva, Switzerland, May 1993, pp. 1064–1070.

[32] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Commun.*, vol. 49, no. 10, pp. 1727–1737, Oct. 2001.

[33] D. Poulin, J. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2776–2798, Jun. 2009.

[34] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1203–1222, Feb. 2014.

[35] Z. Babar, S. X. Ng, and L. Hanzo, "EXIT-chart aided near-capacity quantum turbo code design," *IEEE Trans. Veh. Technol.*, to be published.

[36] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 2011, pp. 445–449.

[37] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982. [Online]. Available: http://dx.doi.org/10.1038/299802a0

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

[39] D. Poulin, J. Tillich, and H. Ollivier, "Quantum serial turbo codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 310–314.

[40] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Phys. Rev. Lett.*, vol. 109, p. 050504, Aug. 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.109.050504

[41] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A*, vol. 57, pp. 830–839, Feb. 1998. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.57.830

[42] G. Smith and J. A. Smolin, "Degenerate quantum codes for pauli channels," *Phys. Rev. Lett.*, vol. 98, p. 030501, Jan. 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.98.030501

[43] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824–3851, Nov. 1996. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.54.3824

[44] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A*, vol. 66, p. 052313, Nov. 2002. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.66.052313

[45] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[46] T. Brun, I. Devetak, and M.-H. Hsieh, "General entanglement-assisted quantum error-correcting codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2101–2105.

[47] M.-H. Hsieh, I. Devetak, and T. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A*, vol. 76, p. 062313, Dec. 2007. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.76.062313

[48] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quantum Inf. Process.*, vol. 13, no. 4, pp. 957–990, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11128-013-0704-8

[49] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, Aug. 1996.

[50] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 452, pp. 2551–2577, Nov. 1995.

[51] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, 1996.

[52] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, pp. 198–201, Jul. 1996. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.77.198

[53] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, no. 3, pp. 1862–1868, Sep. 1996.

[54] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Inst. Technol., Pasadena, CA, USA, 1997.

[55] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A*, vol. 56, pp. 33–38, Jul. 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.56.33

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

[57] M. Grassl and T. Beth, "Quantum BCH codes," in *Proc. Int. Symp. Theoretical Elect. Eng.*, Magdeburg, Germany, Oct. 1999, pp. 207–212. [Online]. Available: http://arxiv.org/abs/quant-ph/9910060

[58] A. M. Steane, "Enlargement of Calderbank–Shor–Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492–2495, Nov. 1999.

[59] A. M. Steane, "Quantum Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1701–1703, Jul. 1999.

[60] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed–Solomon codes," in *Proc. Appl. Algebra, Algebraic Algorithms Error-Correcting Codes (AAECC)*, 1999, pp. 231–244.

[61] M. S. Postol. (2001). "A proposed quantum low density parity check code." [Online]. Available: http://arxiv.org/abs/quant-ph/0108131

[62] T. Camara, H. Ollivier, and J.-P. Tillich. (2005). "Constructions and performance of classes of quantum LDPC codes." [Online]. Available: http://arxiv.org/abs/quant-ph/0502086

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

[64] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, p. 177902, Oct. 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.91.177902

[65] H. Ollivier and J.-P. Tillich. (2004). "Quantum convolutional codes: Fundamentals." [Online]. Available: http://arxiv.org/abs/quant-ph/0401134

[66] G. D. Forney, Jr., and S. Guha, "Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2005, pp. 1028–1032.

[67] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 865–880, Mar. 2007.

[68] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4718–4729, Jul. 2013.

[69] J. M. Renes and M. M. Wilde, "Polar codes for private and quantum communication over arbitrary channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3090–3103, Jun. 2014.

[70] P. Piret, *Convolutional Codes: An Algebraic Approach*. Cambridge, MA, USA: MIT Press, 1988.

[71] H. F. Chau, "Quantum convolutional error-correcting codes," *Phys. Rev. A*, vol. 58, no. 2, pp. 905–909, Aug. 1998. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.58.905

[72] H. F. Chau, "Good quantum-convolutional error-correction codes and their decoding algorithm exist," *Phys. Rev. A*, vol. 60, no. 3, pp. 1966–1974, Sep. 1999. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.60.1966

[73] A. C. Aido De Almeida and R. Palazzo, Jr., "A concatenated [(4, 1, 3)] quantum convolutional code," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2004, pp. 28–33.

[74] M. Grassl and M. Rotteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Sep. 2005, pp. 1018–1022.

[75] M. Grassl and M. Rotteler, "Constructions of quantum convolutional codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 816–820.

[76] S. A. Aly, M. Grassl, A. Klappenecker, M. Rotteler, and P. K. Sarvepalli, "Quantum convolutional BCH codes," in *Proc. 10th Can. Workshop Inf. Theory*, Jun. 2007, pp. 180–183.

[77] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "Quantum convolutional codes derived from generalized Reed–Solomon codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 821–825.

[78] E. Pelchat and D. Poulin, "Degenerate Viterbi decoding," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3915–3921, Jun. 2013.

[79] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[80] D. C. MacKay, G. Mitchison, and A. Shokrollahi. (2007). *More Sparse-Graph Codes for Quantum Error-Correction*. [Online]. Available: http://www.inference.phy.cam.ac.uk/mackay/cayley.pdf

[81] A. Couvreur, N. Delfosse, and G. Zemor, "A construction of quantum LDPC codes from Cayley graphs," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 2011, pp. 643–647.

[82] A. Couvreur, N. Delfosse, and G. Zemor, "A construction of quantum LDPC codes from Cayley graphs," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 6087–6098, Sep. 2013.

[83] S. A. Aly, "A class of quantum LDPC codes constructed from finite geometries," in *Proc. IEEE Global Telecommun. Conf.*, Nov./Dec. 2008, pp. 1–5.

[84] I. B. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.

[85] H. Lou and J. Garcia-Frias, "Quantum error-correction using codes with low-density generator matrix," in *Proc. IEEE 6th Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2005, pp. 1043–1047.

[86] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low-density generator matrix over different quantum channels," in *Proc. Int. ITG-Conf. Sour. Channel Coding*, Apr. 2006, pp. 1–6.

[87] M. Hagiwara and H. Imai, "Quantum quasi-cyclic LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 806–810.

[88] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Non-binary quasi-cyclic quantum LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul./Aug. 2011, pp. 653–657.

[89] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1223–1230, Feb. 2012.

[90] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, "Spatially coupled quasi-cyclic quantum LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul./Aug. 2011, pp. 638–642.

[91] P. Tan and J. Li, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 476–491, Jan. 2010.

[92] N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 917–921.

[93] A. A. Kovalev and L. P. Pryadko, "Quantum Kronecker sum-product low-density parity-check codes with finite rate," *Phys. Rev. A*, vol. 88, no. 1, p. 012311, Jul. 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.88.012311

[94] J.-P. Tillich and G. Zemor, "Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1193–1202, Feb. 2014.

[95] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," *Quantum Inf. Comput.*, vol. 8, no. 10, pp. 987–1000, Nov. 2008. [Online]. Available: http://dl.acm.org/citation.cfm?id=2016985.2016993

[96] Y.-J. Wang, B. C. Sanders, B.-M. Bai, and X.-M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1231–1241, Feb. 2012.

[97] J. Kliewer, S. X. Ng, and L. Hanzo, "Efficient computation of EXIT functions for nonbinary iterative decoding," *IEEE Trans. Commun.*, vol. 54, no. 12, pp. 2133–2136, Dec. 2006.

[98] M. Houshmand and M. M. Wilde, "Recursive quantum convolutional encoders are catastrophic: A simple proof," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6724–6731, Oct. 2013.

[99] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A*, vol. 79, no. 3, p. 032340, Mar. 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.79.032340

[100] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A*, vol. 81, no. 4, p. 042333, Apr. 2010. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.81.042333

[101] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 334–338.

[102] Z. Babar, S. X. Ng, and L. Hanzo, "Reduced-complexity syndrome-based TTCM decoding," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1220–1223, Jun. 2013.

[103] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A*, vol. 55, no. 6, pp. 4054–4059, Jun. 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.55.4054

[104] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, pp. 2881–2884, Nov. 1992. [Online]. Available: http://dx.doi.org/%7B10.1103/PhysRevLett.69.2881%7D

[105] J. Dehaene and B. D. Moor, "The Clifford group, stabilizer states, and linear and quadratic operations over GF(2)," *Phys. Rev. A*, vol. 68, p. 042318, Oct. 2003. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.68.042318

[106] D. Gottesman. (Dec. 2001). "The Heisenberg representation of quantum computers." [Online]. Available: http://arxiv.org/pdf/quant-ph/9807006v1.pdf

[107] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 127–153, Feb. 2014.

[108] S. ten Brink, "Rate one-half code for approaching the Shannon limit by 0.1 dB," *Electron. Lett.*, vol. 36, no. 15, pp. 1293–1294, Jul. 2000.

[109] L. Kong, S. X. Ng, R. G. Maunder, and L. Hanzo, "Maximum-throughput irregular distributed space-time code for near-capacity cooperative communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 3, pp. 1511–1517, Mar. 2010.

[110] S. Ibi, T. Matsumoto, R. Thoma, S. Sampei, and N. Morinaga, "EXIT chart-aided adaptive coding for multilevel BICM with turbo equalization in frequency-selective MIMO channels," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3757–3769, Nov. 2007.

[111] Z. Babar, S. X. Ng, and L. Hanzo, "Near-capacity code design for entanglement-assisted classical communication over quantum depolarizing channels," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4801–4807, Dec. 2013.

[112] A. Grant, "Convergence of non-binary iterative decoding," in *Proc. IEEE Global Telecommun. Conf.*, vol. 2. Nov. 2001, pp. 1058–1062.

[113] S. X. Ng, O. R. Alamri, Y. Li, J. Kliewer, and L. Hanzo, "Near-capacity turbo trellis coded modulation design based on EXIT charts and union bounds," *IEEE Trans. Commun.*, vol. 56, no. 12, pp. 2030–2039, Dec. 2008.

[114] M. Tüchler, "Design of serially concatenated systems depending on the block length," *IEEE Trans. Commun.*, vol. 52, no. 2, pp. 209–218, Feb. 2004.

[115] M. Tüchler and J. Hagenauer, "EXIT charts of irregular codes," in *Proc. Conf. Inf. Sci. Syst.*, Mar. 2002, pp. 465–490.

[116] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1827–1832, Sep. 1999.

[117] D. P. Divincenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 580–598, Mar. 2002.

ZUNAIRA BABAR, photograph and biography not available at the time of publication.

PANAGIOTIS BOTSINIS, photograph and biography not available at the time of publication.

DIMITRIOS ALANIS, photograph and biography not available at the time of publication.

SOON XIN NG, photograph and biography not available at the time of publication.

LAJOS HANZO, photograph and biography not available at the time of publication.

● ● ●

AUTHOR QUERIES