Fully-Parallel Quantum Turbo Decoder

Zunaira Babar, Hung Viet Nguyen, Panagiotis Botsinis, Dimitrios Alanis,
Daryus Chandra, Soon Xin Ng, Robert G. Maunder and Lajos Hanzo

***Abstract*—Quantum Turbo Codes (QTCs) are known to operate close to the achievable Hashing bound. However, the sequential nature of the conventional quantum turbo decoding algorithm imposes a high decoding latency, which increases linearly with the frame length. This posses a potential threat to quantum systems having short coherence times. In this context, we conceive a Fully-Parallel Quantum Turbo Decoder (FPQTD), which eliminates the inherent time dependencies of the conventional decoder by executing all the associated processes concurrently. Due to its parallel nature, the proposed FPQTD reduces the decoding times by several orders of magnitude, while maintaining the same performance. We have also demonstrated the significance of employing an odd-even interleaver design in conjunction with the proposed FPQTD. More specifically, it is shown that an odd-even interleaver reduces the computational complexity by 50%, without compromising the achievable performance.**

***Keywords*—Quantum Error Correction, Turbo Codes, Fully-Parallel decoding, Iterative Decoding.**

ACRONYMS

EXIT	EXtrinsic Information Transfer
FPTD	Fully-Parallel Trubo Decoder
FPQTD	Fully-Parallel Quantum Trubo Decoder
MAP	Maximum *A Posteriori*
PCM	Parity Check Matrix
QBER	QuBit Error rate
QCC	Quantum Convolutional Code
QECC	Quantum Error Correction Code
QIRCC	Quantum IRregular Convolutional Code
QTC	Quantum Turbo Code
SISO	Soft-In Soft-Out

I. INTRODUCTION

Quantum Error Correction Codes (QECCs) are indispensable for the reliable transmission of fragile quantum information (or qubits) over noisy quantum channels. In its literal sense, a quantum channel can be a transmission medium, including free-space channels and optical fiber links, which may find application in quantum key distribution systems [1], [2], quantum teleportation [3], quantum secure direct communication [4], [5] as well as distributed quantum computing networks [6], [7]. Furthermore, a noisy quantum channel may also be interpreted as the imperfections in quantum computing hardware, namely quantum flips inflicted by quantum decoherence and faulty quantum gates. In this context, efficient QECCs are essential for the practical realization of quantum communication as well as quantum computing systems. From the perspective of classic communications, this is also particularly important because the quantum domain parallel computations offer a potential solution to the joint optimization in large-scale communication systems [8]–[10].

Analogous to the realm of classical code design [11], [12], which aims for approaching Shannon's capacity limit, QECCs are designed to operate close to the quantum channel's capacity [13]–[15], or more specifically to the Hashing bound, which constitutes a lower bound on the achievable capacity of a quantum channel. In pursuit of this objective, quantum-domain counterparts of the capacity-achieving classical turbo codes [16] were conceived in [17], [18]. The proposed Quantum Turbo Codes (QTCs) are based on the serial concatenation of Quantum Convolutional Codes (QCCs) [19]–[22]. Later, Wilde and Hseih [23] extended the concept of pre-shared entanglement to QTCs for the sake of designing codes having an unbounded minimum distance, implying that the minimum distance increases with the frame length. In [24] Wilde *et al.* improved the quantum turbo decoding algorithm by introducing the notion of *extrinsic* information. The QTC designs of [17], [18], [23], [24] are based on the tedious analysis of the distance spectra of QCCs. To dispense with this time-consuming design approach, in [25] we appropriately adapted the classical non-binary EXtrinsic Information Transfer (EXIT) charts [26] for designing QTCs. Finally, in [27] we conceived Quantum IRregular Convolutional Code (QIRCC) for facilitating a Hashing bound approaching QTC design.

Owing to the astounding performance of QTCs and motivated by the recently proposed fully-parallel decoder conceived for classical turbo codes [28]–[31], in this paper we focus on improving the latency associated with the iterative quantum turbo decoding process. If the decoding times are significant as compared to the coherence time, then the qubits may decohere faster than they can be corrected. This would in turn render the error correction procedure useless. Against this background, our novel contributions are:

- *We have conceived the Fully-Parallel Quantum Turbo Decoder (FPQTD) counterpart of the classical Fully-Parallel Turbo Decoder (FPTD) of [28], which circumvents the sequential nature of the conventional quantum turbo decoding algorithm of [17], [18], thereby*

The authors are with the School of Electronics and Computer Science, University of Southampton, SO17 1BJ, United Kingdom. Email: {zb2g10, hvn08r, pb1y14, da4g11, dc2n14, sxn, rm, lh}@ecs.soton.ac.uk.

The financial support of the European Research Council under the Advanced Fellow Grant, that of the Royal Society's Wolfson Research Merit Award and that of the Engineering and Physical Sciences Research Council under Grant EP/L018659/1 is gratefully acknowledged. The use of the IRIDIS High Performance Computing Facility at the University of Southampton is also acknowledged. The research data for this paper is available at http://dx.doi.org/10.5258/SOTON/393128.

incurring a lower latency. In addition to the plausible benefit of imposing a reduced processing delay and hence an increased throughput, having a low latency is particularly crucial in the quantum domain because of the short coherence time of the qubits.

- We have benchmarked the performance of the proposed FPQTD against the conventional quantum turbo decoder in terms of its achievable QuBit Error Rate (QBER) as well as the required decoding time periods. *In particular, our results demonstrate that the fully-parallel architecture reduces the total decoding time periods by a factor of* $0.8N_1$ *for the rate-*$1/9$ *QTC of [24], where* N_1 *is the input frame length. Hence, the benefits accrued increase with the frame length*.
- We demonstrate the explicit benefit of using an odd-even interleaver design in the context of quantum turbo decoding. *It is shown that an odd-even interleaving pattern reduces the computational complexity by* 50%*, while exhibiting the same QBER performance.*

The rest of the paper is organized as follows. Section II provides a rudimentary introduction to stabilizer codes. We then present the general structure of QTCs in Section III. This is followed by a description of the conventional quantum turbo decoder in Section IV-A, while our proposed FPQTD is detailed in Section IV-B. Finally, the performance of our proposed scheme is quantified in Section V, followed by our conclusions in Section VI.

II. Review of Stabilizer Codes

QTCs belong to the family of stabilizer codes, which are inherently similar to the classical linear block codes. We commence our discourse with a brief review of the stabilizer formalism. For a detailed description, please refer to [27], [32]. Let us first recall some fundamental definitions from [33].

Pauli Operators: The $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ Pauli operators are defined by the following matrices:

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

where the $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ operators anti-commute with each other.

Pauli Group: A single qubit Pauli group $\mathcal{G}_1$ is a group formed by the Pauli matrices of Eq. (1), which is closed under multiplication. Therefore, it consists of all the Pauli matrices together with the multiplicative factors ± 1 and $\pm i$, which may be formulated as:

$$\mathcal{G}_1 \equiv \{\pm\mathbf{I}, \pm i\mathbf{I}, \pm\mathbf{X}, \pm i\mathbf{X}, \pm\mathbf{Y}, \pm i\mathbf{Y}, \pm\mathbf{Z}, \pm i\mathbf{Z}\}. \tag{2}$$

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

Depolarizing Channel: A depolarizing channel, which is characterized by the probability p, inflicts an error $\mathcal{P} \in \mathcal{G}_n$ on n qubits, where each qubit may independently experience either a bit-flip ($\mathbf{X}$), a phase-flip ($\mathbf{Z}$) or both ($\mathbf{Y}$) with a probability of $p/3$ each, when considering the so-called symmetric depolarizing channel having identical flip probabilities.

An $[n, k]$ stabilizer code, constructed over a code space $\mathcal{C}$, maps the information word (logical qubits) $|\psi\rangle \in \mathbb{C}^{2^k}$ onto the codeword (physical qubits) $|\overline{\psi}\rangle \in \mathbb{C}^{2^n}$, where $\mathbb{C}^d$ denotes the d-dimensional Hilbert space. The resultant stabilizer code is defined by the stabilizer group $\mathcal{H}$, which may be uniquely characterized by a set of $(n-k)$ independent commuting Pauli generators $g_j \in \mathcal{G}_n$, for $1 \leq j \leq (n-k)$. More explicitly, the stabilizer group $\mathcal{H}$ contains both g_j and all the products of g_j for $1 \leq j \leq (n-k)$ and forms an abelian subgroup of $\mathcal{G}_n$. A unique feature of these stabilizer generators is that they do not perturb the state of valid codewords, while yielding an eigenvalue of -1 for the invalid codewords. Consequently, the eigenvalue is -1 if the channel error $\mathcal{P} \in \mathcal{G}_n$ anti-commutes with the stabilizer g_j, while it is $+1$ if $\mathcal{P}$ commutes with g_j. Hence, the operation of jth stabilizer generator may be expressed as:

$$g_j|\hat{\psi}\rangle = \begin{cases} |\overline{\psi}\rangle, & g_j\mathcal{P} = \mathcal{P}g_j \\ -|\overline{\psi}\rangle, & g_j\mathcal{P} = -\mathcal{P}g_j, \end{cases} \tag{3}$$

where $|\hat{\psi}\rangle = \mathcal{P}|\overline{\psi}\rangle$ is the received codeword. The ± 1 eigenvalues give the corresponding error syndrome, when observed using auxiliary qubits. The resultant syndrome is 0 for an eigenvalue of $+1$, while it is 1 for an eigenvalue of -1. Hence, stabilizer codes observe the error syndromes without reading the actual quantum information. The classical syndrome decoding approach [34] may then be invoked for estimating the errors incurred during transmission. However, errors, which differ only by an element of the stabilizer group, have the same impact on the codewords and therefore can be corrected by the same recovery operations. This gives quantum codes the intrinsic property of degeneracy [35].

The Pauli operators $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ may also be represented as two binary digits, i.e. we have:

$$\mathbf{I} \to I \equiv (0,0), \quad \mathbf{X} \to X \equiv (0,1), \\ \mathbf{Y} \to Y \equiv (1,1), \quad \mathbf{Z} \to Z \equiv (1,0), \tag{4}$$

which constitute the effective Pauli group G_1. Similarly, an n-qubit Pauli operator may be mapped onto a $2n$-bit vector belonging to the effective Pauli group G_n, such that the first n bits represent the $\mathbf{Z}$ operator, while the next n bits represent the $\mathbf{X}$ operator. The elements of the effective Pauli group G_n differ from the corresponding elements of the Pauli group $\mathcal{G}_n$ by a multiplicative constant, implying that we have:

$$G_n = [\mathcal{G}_n] = \mathcal{G}_n/\{\pm 1 \pm i\}, \tag{5}$$

where $[.]$ denotes the effective Pauli group. Based on this Pauli-to-binary isomorphism, stabilizer codes may be characterized in terms of an equivalent binary Parity Check Matrix (PCM) notation, which satisfies the commutativity constraint of the stabilizer generators [36], [37]. The $(n-k)$ stabilizers of an $[n, k]$ stabilizer code constitute the rows of the binary PCM H, which is a concatenation of a pair of $(n-k) \times n$ binary

matrices H_z and H_x, as given below:

$$H = (H_z|H_x)\,. \tag{6}$$

Each row of H corresponds to an independent stabilizer of $\mathcal{H}$, so that the ith columns of H_z and H_x act on the ith qubit. Given the matrix notation of Eq. (6), the commutative property of stabilizer generators is transformed into the orthogonality of rows with respect to the symplectic product (also referred to as a twisted product), which is formulated as:

$$H_z H_x^T + H_x H_z^T = 0. \tag{7}$$

Based on the mapping of Eq. (4), a channel error $\mathcal{P}$ can be represented by the effective error $P = [P_z : P_x]$, which is a concatenation of n bits for $\mathbf{Z}$ errors represented by P_z, followed by another n bits for $\mathbf{X}$ errors denoted by P_x. The resultant syndrome is given by the symplectic product of H and P, which is equivalent to $H[P_x : P_z]^T$. Thus, the quantum-domain syndrome is equivalent to the classical-domain binary syndrome and a basic quantum-domain decoding procedure is similar to the syndrome based decoding of the equivalent classical code [37]. However, due to the degenerate nature of quantum codes, quantum decoding aims for finding the most likely error coset, while the classical syndrome decoding finds the most likely error.

III. System Architecture of Quantum Turbo Codes

Fig. 1 shows the general schematic of the encoder and decoder of a QTC, relying on a pair of serially concatenated stabilizer codes. In our setting, the outer code $\mathcal{C}_1$ is an $[n_1, k_1, m_1]$ QCC, while the inner code is an $[n_2, k_2, m_2]$ QCC, resulting in an overall coding rate of $(k_1 k_2/n_1 n_2)$. At the transmitter, the outer encoder $\mathcal{V}_1$ encodes the logical qubits $|\psi_1\rangle$ into the physical qubits $|\overline{\psi}_1\rangle$, with the aid of $(n_1 - k_1)$ auxiliary qubits, which are initialized to state $|0\rangle$. This encoding process may be modeled as:

$$|\overline{\psi}_1\rangle = \mathcal{V}_1\left(|\psi_1\rangle \otimes |0\rangle^{\otimes n_1 - k_1}\right). \tag{8}$$

The physical qubits $|\overline{\psi}_1\rangle$ are then interleaved by the quantum interleaver (π) before being fed to the inner encoder. More specifically, the interleaved qubits $|\psi_2\rangle$ constitute the logical qubits for the inner encoder $\mathcal{V}_2$, which encodes them into $|\overline{\psi}_2\rangle$ using $(n_2 - k_2)$ auxiliary qubits analogous to Eq. (8). The n physical qubits $|\overline{\psi}_2\rangle$ of the inner encoder, where we have $n = n_1 n_2$, are then transmitted to the receiver over a depolarizing channel, which imposes an n-tuple error $\mathcal{P}_2 \in \mathcal{G}_n$ on the transmitted stream.

Both the encoders $\mathcal{V}_1$ and $\mathcal{V}_2$ are Clifford unitary operators [38], acting on n_1 and n_2 qubits, respectively. In general, such Clifford encoders may be implemented using the Hadamard ($\mathbf{H}$), phase ($\mathbf{S}$) and controlled-NOT (C-NOT) gates, which are defined as follows [33]:

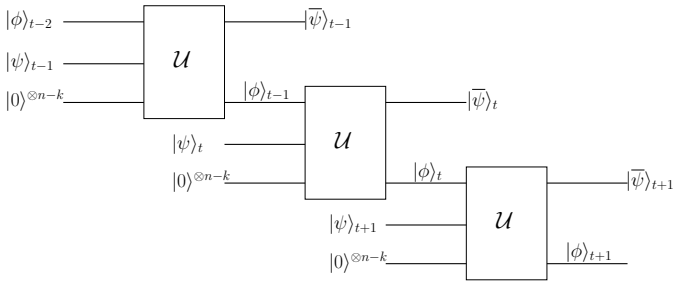


Fig. 2: Encoder $\mathcal{V}$ of an $[n, k, m]$ quantum convolutional code.

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$
$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{9}$$

A unique property of Clifford operations is that they preserve the elements of the Pauli group under conjugation such that for $\mathcal{P} \in \mathcal{G}_n$, we have [38]:

$$\mathcal{V}\mathcal{P}\mathcal{V}^\dagger \in \mathcal{G}_n. \tag{10}$$

This in turn ensures that the Clifford encoding operation intrinsically preserves the commutativity of the associated stabilizer generators depicted in Eq. (7). It is pertinent to mention here that the Clifford encoder $\mathcal{V}$ of an $[n, k, m]$ QCC, having m memory qubits $|\phi\rangle$, may be constructed from an $(n + m)$-qubit seed transformation $\mathcal{U}$, as illustrated in Fig. 2. More specifically, the encoder $\mathcal{V}$ consists of repeated applications of the seed transformation $\mathcal{U}$ such that the adjacent seed transformations have an overlap of m memory qubits. At time instant t, the sub-encoder $\mathcal{U}$ of Fig. 2 takes as its input the previous memory state $|\phi\rangle_{t-1}$ as well as the logical qubits $|\psi\rangle_t$ and the auxiliary qubits to generate the updated memory state $|\phi\rangle_t$ for the next time instant as well as the physical qubits $|\overline{\psi}\rangle_t$. More explicitly, analogous to the classical convolutional codes, the memory qubits $|\phi\rangle_{t-1}$ are flushed out of the shift registers as part of the physical qubits, while the incoming information is fed into the registers[1]. The overall encoder may be formulated as:

$$\begin{aligned}\mathcal{V} &= \mathcal{U}_{[1,\ldots,n+m]}\mathcal{U}_{[n+1,\ldots,2n+m]}\ldots\mathcal{U}_{[(N-1)n+1,\ldots,Nn+m]}, \\ &= \prod_{t=1}^{N}\mathcal{U}_{[(t-1)n+1,\ldots,tn+m]},\end{aligned} \tag{11}$$

where N is the length of the convolutional code and $\mathcal{U}_{[(t-1)n+1,\ldots,tn+m]}$ acts on $(n + m)$ qubits, i.e. m memory qubits $|\phi\rangle_{t-1}$, k logical qubits $|\psi\rangle_t$ and $(n-k)$ auxiliary qubits.

[1]Please refer to [39, Chapter 9] for further details about the implementation of quantum circuits with shift registers.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2581978, IEEE Access

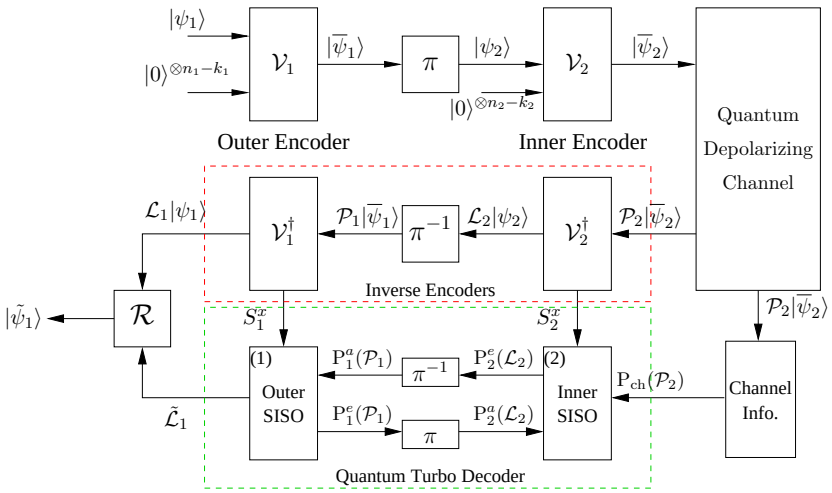


Fig. 1: General schematic of quantum turbo codes. $\mathrm{P}_i^a(.)$, $\mathrm{P}_i^e(.)$ *and* $\mathrm{P}_i^o(.)$ *denote the a-priori, extrinsic and a-posteriori probabilities related to the* i*th decoder.*

At the receiver, the received physical information $|\hat{\psi}_2\rangle = \mathcal{P}_2|\overline{\psi}_2\rangle$ is processed by the inverse inner encoder[2] $\mathcal{V}_2^\dagger$, yielding the logical information and auxiliary qubits. Since the input of the inverse encoder is perturbed by transmission errors, both the output logical information and the auxiliary qubits are also corrupted. More explicitly, we have:

$$\begin{aligned}\mathcal{V}_2^\dagger\mathcal{P}_2|\overline{\psi}_2\rangle &= \mathcal{V}_2^\dagger\mathcal{P}_2\mathcal{V}_2(|\psi\rangle\otimes|0\rangle^{\otimes n_2-k_2}) \\ &= (\mathcal{L}_2|\psi_2\rangle)\otimes(\mathcal{S}_2|0\rangle^{\otimes n_2-k_2}),\end{aligned} \tag{12}$$

where $\mathcal{L}_2$ is the error imposed on the logical qubits of the inner encoder, while $\mathcal{S}_2$ is the error inflicted on the (n_2-k_2) auxiliary qubits. The resultant logical information is then de-interleaved to serve as the input $\mathcal{P}_1|\overline{\psi}_1\rangle$ of the outer inverse encoder. Analogous to the inverse encoder of Eq. (12), the inverse encoder $\mathcal{V}_1^\dagger$ generates the erroneous logical qubits $\mathcal{L}_1|\psi_1\rangle$ of the outer encoder and the associated erroneous auxiliary qubits $\mathcal{S}_1|0\rangle^{\otimes n_1-k_1}$ as its output.

Recall that stabilizer codes invoke the syndrome decoding approach for estimating the channel errors. The auxiliary qubits $\mathcal{S}_2|0\rangle^{\otimes n_1-k_1}$ and $\mathcal{S}_1|0\rangle^{\otimes n_2-k_2}$ of the inner and outer inverse encoders, respectively, are measured before being fed to the corresponding syndrome-based Soft-In Soft-Out (SISO) decoders. Upon measurement the auxiliary qubits collapse to the classical syndromes S_2^x and S_1^x, which only depend on the $\mathbf{X}$-component of the errors $\mathcal{S}_2$ and $\mathcal{S}_1$, respectively. More precisely, the syndrome sequence $|0\rangle^{\otimes n_1-k_1}$ (and similarly $|0\rangle^{\otimes n_2-k_2}$) is invariant to the $\mathbf{Z}$-component of $\mathcal{S}$, since $\mathbf{Z}|0\rangle = |0\rangle$. Therefore, the syndrome-based SISO decoders of Fig. 1 engage in degenerate iterative decoding [18] for estimating the error coset $\tilde{\mathcal{L}}_1$ imposed on the logical qubits of the outer decoder, given only the $\mathbf{X}$-component of $\mathcal{S}$. More explicitly, the inner SISO decoder of Fig. 1 exploits the channel information $\mathrm{P}_{\mathrm{ch}}(\mathcal{P}_2)$, the *a-priori* information $\mathrm{P}_2^a(\mathcal{L}_2)$ gleaned from the outer decoder (initialized to be equiprobable for the first iteration) and the syndrome S_2^x for computing the *extrinsic* information pertaining to the error imposed on the logical qubits of the inner decoder, which may be denoted as $\mathrm{P}_2^e(\mathcal{L}_2)$. The resultant extrinsic information $\mathrm{P}_2^e(\mathcal{L}_2)$ is de-interleaved (π^{-1}), so that the permuted output $\mathrm{P}_1^a(\mathcal{P}_1)$ serves as the *a-priori* information pertaining to the error imposed on the physical qubits of the outer decoder. Then the outer SISO decoder of Fig. 1 computes both the *a-posteriori* information $\mathrm{P}_1^o(\mathcal{L}_1)$ as well as the *extrinsic* information $\mathrm{P}_1^e(\mathcal{P}_1)$ using the *a-priori* information $\mathrm{P}_1^a(\mathcal{P}_1)$ and the syndrome S_1^x. The output $\mathrm{P}_1^e(\mathcal{P}_1)$ is then interleaved to yield $\mathrm{P}_2^a(\mathcal{L}_2)$, which is fed back to the inner SISO decoder of Fig. 1. This iterative procedure continues, until either convergence to a vanishingly low QBER is achieved or the maximum affordable number of iterations is reached. Finally, a Maximum *A Posteriori* (MAP) decision is made based on the *a-posteriori* information $\mathrm{P}_1^o(\mathcal{L}_1)$ for estimating the most likely error coset $\tilde{\mathcal{L}}_1$ imposed on the logical qubits of the outer decoder. A recovery operation $\mathcal{R}$, which is based on the estimated error coset $\tilde{\mathcal{L}}_1$, may then be applied to the erroneous logical qubits $\mathcal{L}_1|\psi_1\rangle$ of the outer inverse decoder, yielding the estimated logical information $|\tilde{\psi}_1\rangle$.

[2]In contrast to an encoder, which encodes logical qubits onto the physical qubits, an inverse encoder carries out the inverse operation by mapping physical qubits onto the corresponding logical qubits.

IV. Quantum Turbo Decoder

A. Conventional Decoder

The quantum turbo decoder of Fig. 1 operates over the equivalent classical representation of the Clifford encoders $\mathcal{V}_1$ and $\mathcal{V}_2$. More explicitly, an n-qubit encoder, acting on a 2^n-dimensional Hilbert space, has a $2^n \times 2^n$ unitary matrix, which describes the evolution of the associated n-qubit system. However, according to the Heisenberg representation of Gottesman-

Knill theorem [40], the $2^n \times 2^n$ matrix may be simplified for Clifford encoders by only tracking the evolution of the operators $\{\mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_n, \mathbf{X_1}, \mathbf{X}_2, \ldots, \mathbf{X}_n\}$, where $\mathbf{Z}_j$ and $\mathbf{X}_j$ represents the Pauli $\mathbf{Z}$ and $\mathbf{X}$ operator, respectively, acting on the jth qubit and the identity $\mathbf{I}$ on all other qubits. Consequently, the operation of a Clifford encoder may 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. Another point to notice here is that two Clifford encoders $\mathcal{V}$ and $\mathcal{V}'$, which are related through a global phase such that $\mathcal{V}' = e^{j\theta}\mathcal{V}$, yield the same output under conjugation. Therefore, the global phase can be ignored, since it has a trivial impact. This in turn implies that the n-qubit encoder $\mathcal{V}$ can be completely defined by its action on the binary equivalent (Eq. (4)) of the Pauli operators $\{\mathbf{Z}_1, \mathbf{Z}_2, \ldots, \mathbf{Z}_n, \mathbf{X_1}, \mathbf{X}_2, \ldots, \mathbf{X}_n\}$, which may be denoted as $\{Z_1, Z_2, \ldots, Z_n, X_1, X_2, \ldots, X_n\}$. Hence, the Clifford transformation $\mathcal{V}$ has an equivalent $2n \times 2n$ binary symplectic matrix V for which we have:

$$[\mathcal{V}\mathcal{P}\mathcal{V}^\dagger] = [\mathcal{P}]V = PV. \tag{13}$$

The n-qubit operators $\{Z_1, Z_2, \ldots, Z_n, X_1, X_2, \ldots, X_n\}$, which are used for characterizing V, are known as the unencoded operators. In particular, the unencoded operators $\{Z_{k+1}, \ldots, Z_n\}$ stabilize the unencoded state of Eq. (8), i.e. $(|\psi\rangle \otimes |0_{n-k}\rangle)$, and are therefore termed as the unencoded stabilizer generators. By contrast, the operators $\{X_{k+1}, \ldots, X_n\}$ anti-commute with the corresponding unencoded stabilizer generator Z_j, resulting in an error syndrome of 1. They may be referred to as the pure errors. Furthermore, the unencoded logical operators acting on the logical qubits are $\{Z_1, X_1, \ldots, Z_k, X_k\}$, which commute with the unencoded stabilizers $\{Z_{k+1}, \ldots, Z_n\}$. The encoder V maps the unencoded operators $\{Z_1, X_1, \ldots, Z_n, X_n\}$ onto the encoded operators $\{\overline{Z}_1, \overline{X}_1, \ldots, \overline{Z}_n, \overline{X}_n\}$, which may be represented as follows:

$$\begin{aligned} \overline{X}_j &= \left[\overline{\mathbf{X}}_j\right] = \left[\mathcal{V}\mathbf{X}_j\mathcal{V}^\dagger\right] = X_j V, \\ \overline{Z}_j &= \left[\overline{\mathbf{Z}}_j\right] = \left[\mathcal{V}\mathbf{Z}_j\mathcal{V}^\dagger\right] = Z_j V. \end{aligned} \tag{14}$$

Let us recall that Clifford operations preserve the commutativity of the stabilizer generators. Hence, the resultant encoded stabilizers $\{\overline{Z}_{k+1}, \ldots, \overline{Z}_n\}$ constitute the stabilizers of Eq. (3), while $\{\overline{X}_{k+1}, \ldots, \overline{X}_n\}$ are the pure errors t_j of the resultant stabilizer code, which trigger a non-trivial syndrome. Moreover, $\{\overline{Z}_1, \overline{X}_1, \ldots, \overline{Z}_k, \overline{X}_k\}$ are the encoded logical operators, which commute with all the stabilizers. In particular, the logical operators map one codeword onto the other codeword within the codespace of the stabilizer code. The $(2n \times 2n)$-element binary symplectic encoding matrix V is therefore given by:

$$V = \begin{pmatrix} \overline{Z}_1 \\ \vdots \\ \overline{Z}_k \\ \overline{Z}_{k+1} \\ \vdots \\ \overline{Z}_n \\ \overline{X}_1 \\ \vdots \\ \overline{X}_k \\ \overline{X}_{k+1} \\ \vdots \\ \overline{X}_n \end{pmatrix} \equiv \begin{pmatrix} \overline{Z}_1 \\ \vdots \\ \overline{Z}_k \\ g_1 \\ \vdots \\ g_{n-k} \\ \overline{X}_1 \\ \vdots \\ \overline{X}_k \\ t_1 \\ \vdots \\ t_{n-k} \end{pmatrix}, \tag{15}$$

where $\{\overline{Z}_{k+1}, \ldots, \overline{Z}_n\}$ constitute the binary PCM of Eq. (6).

Based on the equivalent binary encoder of Eq. (15), the operation of the ith inverse encoder $\mathcal{V}_i^\dagger$ depicted in Eq. (12) may be expressed as:

$$P_i V_i^{-1} = (L_i : S_i), \tag{16}$$

where we have $P_i = [\mathcal{P}_i]$, $L_i = [\mathcal{L}_i]$ and $S_i = [\mathcal{S}_i]$. Similarly, when the inner and outer components of a QTC are convolutional codes, their seed transformations are $2(n+m) \times 2(n+m)$-element symplectic matrices, which may be denoted as U_i for the ith encoder. For the ith inverse encoder, the operation of Eq. (16) at time instant t may be reformulated as:

$$(M_{i,t-1} : L_{i,t} : S_{i,t}) = (M_{i,t}, P_{i,t})\, U_i^{-1}, \tag{17}$$

where M denotes the effective m-qubit error inflicted on the memory qubits. More explicitly, for an $[n_i, k_i, m_i]$ QCC, we have $M_{i,t} = [M_{i,t}^1, M_{i,t}^2, \ldots, M_{i,t}^{m_i}]$, $L_{i,t} = [L_{i,t}^1, L_{i,t}^2, \ldots, L_{i,t}^{k_i}]$, $S_{i,t} = [S_{i,t}^1, S_{i,t}^2, \ldots, S_{i,t}^{n_i-k_i}]$ and $P_{i,t} = [P_{i,t}^1, P_{i,t}^2, \ldots, P_{i,t}^{n_i}]$ for $1 \leq t \leq N_i$. For clarity, we will ignore the subscript 'i' wherever our discussions apply to both the inner as well as the outer decoders.

The quantum turbo decoder of Fig. 1 consists of two serially concatenated SISO decoders, each obeying the general schematic of Fig. 3. In Fig. 3, the Pauli operators $\mathcal{P}$, $\mathcal{L}$ and $\mathcal{S}$ are replaced by the effective operators P, L and S^x, respectively. Please note that $[\mathcal{S}] = S$, which may be represented as $S = S^x + S^z$, where S^x and S^z are the X and Z components of S. Recall from Section III that the measurement of S only reveals the syndrome S^x. Therefore, the syndrome-based SISO decoder of Fig. 3 only depends on S^x. Furthermore, for the sake of avoiding any potential numerical instability as well as for reducing the computational complexity, we have used logarithmic probabilities in Fig. 3, which are denoted as $\bar{\mathrm{P}}$ in contrast to the probabilities P of Fig. 1, i.e. we have:

$$\bar{\mathrm{P}}(x) = \ln\left(\mathrm{P}(x)\right). \tag{18}$$

Classical SISO decoders rely on the trellis of the constituent convolutional codes. By contrast, the SISO decoder of Fig. 3

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2581978, IEEE Access

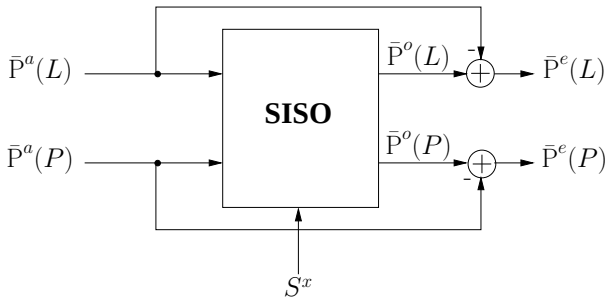


Fig. 3: General schematic of a SISO decoder. $\bar{\mathrm{P}}^a(.)$, $\bar{\mathrm{P}}^e(.)$ *and* $\bar{\mathrm{P}}^o(.)$ *denote the a-priori, extrinsic and a-posteriori logarithmic probabilities.*

invoked for quantum turbo decoding operates over the circuit-based representation of Eq. (16) or equivalently Eq. (17), as detailed in [18]. We may further 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:

$$M_t = (M_{t-1} : L_t : S_t)\, U_M, \tag{19}$$

$$P_t = (M_{t-1} : L_t : S_t)\, U_P. \tag{20}$$

Using the circuit-based representation of Eq. (19) and Eq. (20), the SISO decoder of Fig. 3 computes the *extrinsic* probabilities as follows:

1) The process begins by calculating the *a-priori* transition metric $\bar{\gamma}_t$ for all valid transitions using:

$$\bar{\gamma}_t\left(M_{t-1}, L_t, S_t\right) = \bar{\mathrm{P}}^a\left(L_t\right) + \bar{\mathrm{P}}^a\left(P_t\right), \tag{21}$$

where we have $P_t = (M_{t-1} : L_t : S_t)U_P$. In the classical convolutional codes, all transitions present in their state transition diagram are defined as being valid. By contrast, in the circuit-based representation of QCCs, all possible combinations of $(M_{t-1} = \mu, L_t = \lambda, S_t = \sigma)$, for $\mu \in G_m$, $\lambda \in G_k$ and $\sigma = (\sigma^x + \sigma^z) \in G_{n-k}$, having $\sigma^x = S_t^x$, are considered as valid transitions.

2) The *a-priori* transition metric of Eq. (21) and the *a-priori* forward state metric $\bar{\alpha}_{t-1}$, gleaned from the previous time instant, are then used for calculating the *extrinsic* forward state metric $\bar{\alpha}_t$ as[3]:

$$\begin{aligned}\bar{\alpha}_t\left(M_t\right) &\triangleq \bar{\mathrm{P}}\left(M_t | S_{\leq t}^x\right) \\ &= \max_{\substack{\{\mu\in G_m, \lambda\in G_k, \sigma\in G_{n-k}|\\ \sigma^x = S_t^x, M_t = (\mu,\lambda,\sigma)U_M\}}}{}^{*} \left[\bar{\gamma}_t\left(\mu,\lambda,\sigma\right) + \bar{\alpha}_{t-1}\left(\mu\right)\right],\end{aligned} \tag{22}$$

where we have $S_{\leq t}^x \triangleq \left(S_j^x\right)_{0\leq j\leq t}$. Eq. (22) is a recursive formula, which ensures that the resultant extrinsic forward state metric $\bar{\alpha}_t$ constitutes the *a-priori* information for the next time instant. This implies that for calculating $\bar{\alpha}_{t'}$ we first have to calculate the forward state metric for all the previous time instances $t < t'$. Hence, the calculation of Eq. (22) spans over N time periods for $t = N$.

3) Next, the *extrinsic* backward state metric $\bar{\beta}_{t-1}$ is computed using the *a-priori* transition metric $\bar{\gamma}_t$ of Eq. (21) and the *a-priori* backward state metric $\bar{\beta}_t$ gleaned from the time instant $(t+1)$ as follows:

$$\begin{aligned}&\bar{\beta}_{t-1}\left(M_{t-1}\right) \triangleq \bar{\mathrm{P}}\left(M_{t-1} | S_{>t-1}^x\right) \\ &= \max_{\substack{\{\lambda\in G_k, \sigma\in G_{n-k}|\\ \sigma^x = S_t^x\}}}{}^{*} \left[\bar{\gamma}_t\left(M_{t-1},\lambda,\sigma\right) + \bar{\beta}_t\left(M_t\right)\right],\end{aligned} \tag{23}$$

where we have $M_t = (M_{t-1} : \mu : \sigma)U_M$ and $S_{>t}^x \triangleq \left(S_j^x\right)_{t<j\leq N}$. The resultant *extrinsic* information $\bar{\beta}_{t-1}$ is employed as the *a-priori* information for the time instant $t-2$. Hence, similar to the computation of the forward recursive coefficients $\bar{\alpha}_t$ of Eq. (22), the processing of the backward coefficients is also spread over N time periods. However, unlike the forward coefficients, which are computed in the direction of increasing t, i.e. from $t = 1$ to $t = N$, the backward coefficients are calculated in the reverse direction, i.e. from $t = N$ to $t = 1$.

4) Finally, the *a-posteriori* transition metric $\bar{\delta}_t$ is computed for all valid transitions using:

$$\begin{aligned}&\bar{\delta}_t\left(M_{t-1}, L_t, S_t\right) = \\ &\bar{\gamma}_t\left(M_{t-1}, L_t, S_t\right) + \bar{\alpha}_{t-1}\left(M_{t-1}\right) + \bar{\beta}_t\left(M_t\right),\end{aligned} \tag{24}$$

where we have $M_t = (M_{t-1} : L_t : S_t)U_M$. Eq. (24) combines the *a-priori* transition metric $\bar{\gamma}_t$ with the extrinsic forward state coefficient $\bar{\alpha}_{t-1}$ gleaned from the previous time instant and the extrinsic backward state coefficient $\bar{\beta}_t$ gleaned from $(t+1)$. If the forward and backward coefficients are already available, the *a-posteriori* transition metric can be calculated in parallel for the entire frame.

5) Based on Eq. (24), the *a-posteriori* logarithmic probabilities pertaining to the logical error L_t and the

[3] We exploit the Jacobian logarithm, which is defined as [41]:

$$\begin{aligned}\max^{*}\left[\bar{\rho_1}, \bar{\rho_2}\right] &\triangleq \ln\left(e^{\bar{\rho_1}} + e^{\bar{\rho_2}}\right) \\ &= \max(\bar{\rho_1}, \bar{\rho_2}) + \ln\left(1 + e^{-|\bar{\rho_1} - \bar{\rho_2}|}\right) \\ &= \max(\bar{\rho_1}, \bar{\rho_2}) + f_c\left(|\bar{\rho_1} - \bar{\rho_2}|\right).\end{aligned}$$

For more than two operands, Jacobian logarithm can be extended using the associative property. For the sake of reducing the computational complexity, the correction function f_c can be approximated using a pre-computed look-up table, resulting in an approximate-log function [41]. Alternatively, if the difference between $\bar{\rho_1}$ and $\bar{\rho_2}$ is significant, the exact-log may also be approximated as max-log, yielding [41]:

$$\max^{*}\left[\bar{\rho_1}, \bar{\rho_2}\right] \approx \max(\bar{\rho_1}, \bar{\rho_2}).$$

The complexity reduction associated with the max-log comes at the cost of a modest performance degradation. However, the performance of the approximate-log based decoder is similar to that of the exact-log based decoder, despite its reduced complexity.

physical error P_t are given by:

$$\bar{\mathrm{P}}^{o}\left(L_t\right) \triangleq \bar{\mathrm{P}}\left(L_t|S^x\right) = \max_{\substack{\{\mu\in G_m,\sigma\in G_{n-k}|\\ \sigma^x=S_t^x\}}}{}^{*} \left[\bar{\delta}_t\left(\mu,L_t,\sigma\right)\right], \quad (25)$$

$$\bar{\mathrm{P}}^{o}\left(P_t\right) \triangleq \bar{\mathrm{P}}\left(P_t|S^x\right) = \max_{\substack{\{\mu\in G_m,\lambda\in G_k,\sigma\in G_{n-k}|\\ \sigma^x=S_t^x,P_t=(\mu,\lambda,\sigma)U_P\}}}{}^{*} \left[\bar{\delta}_t\left(\mu,L_t,\sigma\right)\right], \quad (26)$$

where we have $S^x \triangleq \left(S_t^x\right)_{0\le t\le N}$.

6) The corresponding *extrinsic* logarithmic probabilities may then be calculated using:

$$\bar{\mathrm{P}}^{e}\left(L_t\right) = \bar{\mathrm{P}}^{o}\left(L_t\right) - \bar{\mathrm{P}}^{a}\left(L_t\right), \quad (27)$$

$$\bar{\mathrm{P}}^{e}\left(P_t\right) = \bar{\mathrm{P}}^{o}\left(P_t\right) - \bar{\mathrm{P}}^{a}\left(P_t\right). \quad (28)$$

Both the inner as well as the outer SISO decoders of Fig. 1 execute the SISO algorithm encapsulated in Eq. (21) to Eq. (28) during each decoding iteration. Explicitly, as seen in Fig. 1, the channel information and the *a-priori* information $\bar{\mathrm{P}}^{a}\left(L_{2,t}\right)$ gleaned from the outer SISO decoder constitute the inputs of the inner SISO decoder, which is driven by the syndrome sequence S_2^x. The channel information gives the *a-priori* information pertaining to the error on the physical qubits of the inner decoder P_2, which is computed by assuming that each qubit is independently transmitted over a quantum depolarizing channel having a depolarizing probability of p. For the jth qubit at time instant t, we have:

$$\bar{\mathrm{P}}^{a}\left(P_{2,t}^{j}\right) = \bar{\mathrm{P}}_{\mathrm{ch}}\left(P_{2,t}^{j}\right) = \begin{cases} \ln(1-p), & \text{if } P_{2,t}^{i} = I \\ \ln(p/3), & \text{if } P_{2,t}^{i} \in \{X,Z,Y\}, \end{cases} \quad (29)$$

where $1 \le j \le n_2$, while $1 \le t \le N_2$. During each iteration, the inner SISO decoder calculates the *extrinsic* information for each k_2-qubit $L_{2,t}$ using Eq. (21) to Eq. (25) and Eq. (27). This has to be carried out sequentially for $1 \le t \le N_2$ due to the time-dependencies exhibited in Eq. (22) to Eq. (24). Intuitively, we may consider the SISO decoder to be composed of N_2 algorithmic blocks, which are capable of executing Eq. (21) to Eq. (28), as demonstrated in the schematic of Fig. 4. During the first N_2 time periods, the N_2 algorithmic blocks operate sequentially from the first block to the last block for processing Eq. (21) and Eq. (22), as shown in Fig. 4 with bold arrows. During the next N_2 time periods, the N_2 algorithmic blocks execute the rest of the algorithm, commencing from the last block. Hence, the processing time of the inner SISO algorithm of a conventional quantum turbo decoder spans over $2N_2$ time periods for each decoding iteration.

Thereafter, the *extrinsic* information $\bar{\mathrm{P}}^{e}(L_2)$ is de-interleaved, yielding $\bar{\mathrm{P}}^{a}(P_1)$, which is fed to the outer SISO decoder for computing the *extrinsic* information $\bar{\mathrm{P}}^{e}(P_1)$ using Eq. (21) to Eq. (28). It may be noticed here that a qubit-based interleaver/de-interleaver is used in the configuration of Fig. 1. Consequently, the logarithmic probabilities $\bar{\mathrm{P}}^{e}(L_{2,t})$ are marginalized to $\bar{\mathrm{P}}^{e}(L_{2,t}^{j})$, for $1 \le j \le k_2$, before the de-interleaver and then they are recombined thereafter, assuming that the constituent qubits are independent. The operation of the outer SISO decoder, consisting of N_1 algorithmic blocks, requires another $2N_1$ time periods. This results in a total of $(2N_1 + 2N_2)$ time periods for each iteration. The two SISO decoders exchange their information iteratively, until either convergence to a vanishingly low QBER is achieved or the maximum number of decoding iterations is reached. After the last decoding iteration, a MAP decision is made based on the *a-posteriori* information $\bar{\mathrm{P}}^{o}(L_1)$, produced by the outer SISO decoder, for estimating the most likely error coset $\tilde{L}_1$.

B. Fully-Parallel Decoder

As a counterpart of the conventional quantum turbo decoding algorithm, which requires $(2N_1 + 2N_2)$ time periods for each decoding iteration, we conceive a Fully-Parallel Quantum Turbo Decoder (FPQTD), which dispenses with the time dependencies associated with the conventional decoding process. More explicitly, all the N_2 algorithmic blocks of the inner SISO decoder as well as the N_1 algorithmic blocks of the outer decoder operate concurrently in each decoding iteration, as illustrated in Fig. 5. For the sake of achieving this parallelism, the conventional SISO algorithm of Eq. (21) to Eq. (26) is modified as follows:

1) The process commences by calculating the *a-posteriori* transition metric $\bar{\delta}_t$ for all valid transitions using:

$$\bar{\delta}_t\left(M_{t-1},L_t,S_t\right) = \bar{\mathrm{P}}^{a}\left(L_t\right) + \bar{\mathrm{P}}^{a}\left(P_t\right) + \bar{\alpha}_{t-1}\left(M_{t-1}\right) + \bar{\beta}_t\left(M_t\right), \quad (30)$$

where we have $P_t = (M_{t-1} : L_t : S_t)U_P$, while $M_t = (M_{t-1} : L_t : S_t)U_M$. For executing all algorithmic blocks concurrently, the *a-priori* information pertaining to the logical error L_t and the physical error P_t as well as the *a-priori* forward state metric $\bar{\alpha}_{t-1}$ and the *a-priori* backward state metric $\bar{\beta}_t$ are gleaned from the previous decoding iteration. By contrast, the $\bar{\delta}_t$ of Eq. (24) relies on the updated *a-priori* forward and backward state metrics received from the adjacent $(t-1)$st and $(t+1)$st algorithmic blocks, respectively, resulting in sequential processing.

2) The *a-posteriori* transition metric $\bar{\delta}_t$ of Eq. (30) may then be invoked for calculating the *extrinsic* probabilities using Eq. (25) to Eq. (28), which serve as the *a-priori* information for the other SISO decoder in the next decoding iteration, hence eliminating the time dependencies between the two decoders.

3) Since in the fully-parallel architecture the algorithmic blocks exploit the *a-priori* information received during the previous decoding iteration, we substitute Eq. (24) in Eq. (22), which yields:

$$\bar{\alpha}_t\left(M_t\right) = \max_{\substack{\{\mu\in G_m,\lambda\in G_k,\sigma\in G_{n-k}|\\ \sigma^x=S_t^x,M_t=(\mu,\lambda,\sigma)U_M\}}}{}^{*} \left[\bar{\delta}_t\left(\mu,\lambda,\sigma\right)\right] - \bar{\beta}_t\left(M_t\right). \quad (31)$$

Each algorithmic block updates the *extrinsic* forward state metric $\bar{\alpha}_t$ using Eq. (31), which is fed to the $(t+1)$st algorithmic block for use in the next iteration.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2581978, IEEE Access

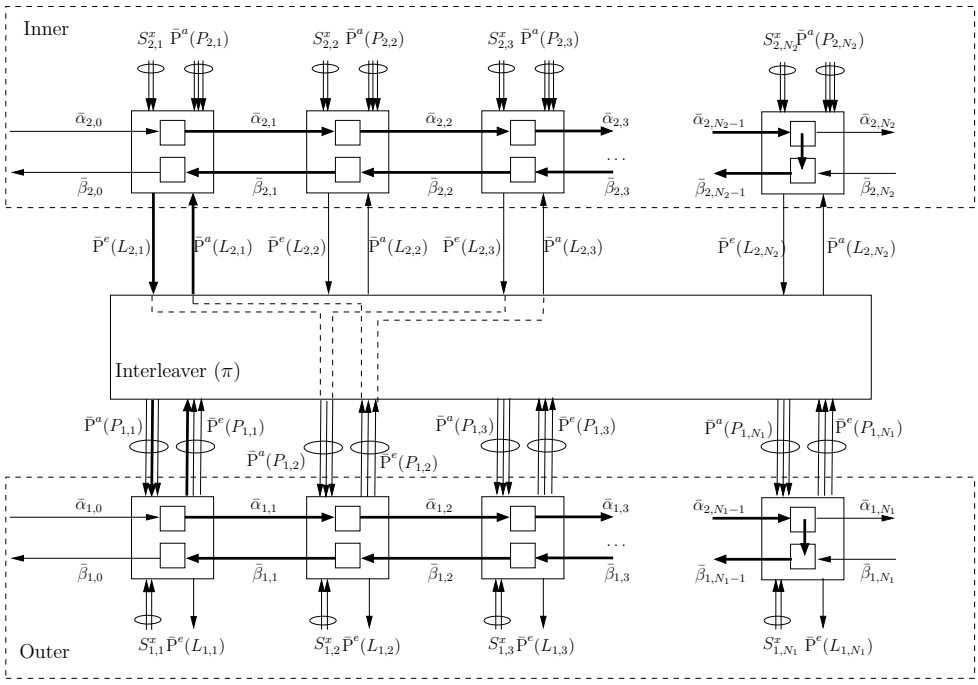


Fig. 4: Schematic of a conventional quantum turbo decoder. The algorithmic blocks are processed in the order of the bold arrows. *The inner and outer components are assumed to be rate-*$1/3$ *convolutional codes.*

4) Similarly, the extrinsic backward state metric $\bar{\beta}_{t-1}$ is updated using:

$$\bar{\beta}_{t-1}\left(M_{t-1}\right) = \max_{\substack{\{\lambda \in G_k, \sigma \in G_{n-k} | \\ \sigma^x = S_t^x\}}}^{*} \left[\bar{\delta}_t\left(M_{t-1}, \lambda, \sigma\right)\right] - \bar{\alpha}_{t-1}\left(M_{t-1}\right), \tag{32}$$

which is fed to the $(t-1)$st algorithmic block for use in the next iteration.

Hence, in the proposed FPQTD, relying on Eq. (30) to Eq. (32), both the inner as well as the outer decoders operate on the basis of the *a-priori* information gathered from the previous decoding iteration and the resultant *extrinsic* information is utilized during the next decoding iteration. Consequently, the time dependencies exhibited in the conventional turbo decoding algorithm are broken down, since all the operations of the $(N_1 + N_2)$ algorithmic blocks rely on the *a-priori* information of the previous iteration. The resultant parallel architecture only requires a single time period for processing all the $(N_1 + N_2)$ algorithmic blocks.

It is pertinent to mention here that *a-priori* information is not available for the first decoding iteration. Following the usual convention, the *a-priori* information $\bar{\mathrm{P}}^a\left(L_{2,t}\right)$ of the inner SISO decoder and $\bar{\mathrm{P}}^a\left(P_{1,t}\right)$ of the outer SISO decoder is initialized to be equiprobable, or equivalently to $[0, 0, \ldots, 0]$, for all algorithmic blocks. Similarly, the *a-priori* forward state metric $\bar{\alpha}_{t-1}$ of the algorithmic blocks having indices $t \in [2, N]$ and the *a-priori* backward state metric $\bar{\beta}_t$ of the algorithmic blocks having indices $t \in [1, N-1]$ are set to $[0, 0, \ldots, 0]$. Recall that the syndrome decoding process outputs information pertaining to the errors rather than to the actual information. Therefore, in all decoding iterations, the *a-priori* forward state metric $\bar{\alpha}_0$ of the first algorithmic block is set according to the actual error inflicted on the memory qubits. More explicitly, once all the physical qubits are processed by the inverse encoder, the memory registers are measured, which reveals the X-component of the error inflicted on it. Then $\bar{\alpha}_0$ may be initialized on the basis of the measured error. Furthermore, for all decoding iterations, the *a-priori* backward state metric $\bar{\beta}_{N_2}$ of the inner decoder is initialized according to the channel model, while $\bar{\beta}_{N_1}$ of the outer decoder is initialized on the basis of $\bar{\mathrm{P}}^a\left(P_{1,N_1}\right)$.

Analogous to the classic FPTD [28]–[31], an odd-even interleaver can be used for further reducing the computational complexity of the FPQTD. More specifically, an odd-even interleaving pattern can be exploited to connect the odd numbered algorithmic blocks of the inner decoder with the odd numbered blocks of the outer decoder, while the inner algorithmic blocks having an even index are only connected to the outer algorithmic blocks having an even index, as shown in Fig. 5. In essence, the inner and outer algorithmic blocks are divided into two independent sets, which are marked as black and white in Fig. 5. Let us assume that the inner and outer components of Fig. 1 are rate-$1/3$ QCCs. Then the encoded output of the outer

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2581978, IEEE Access

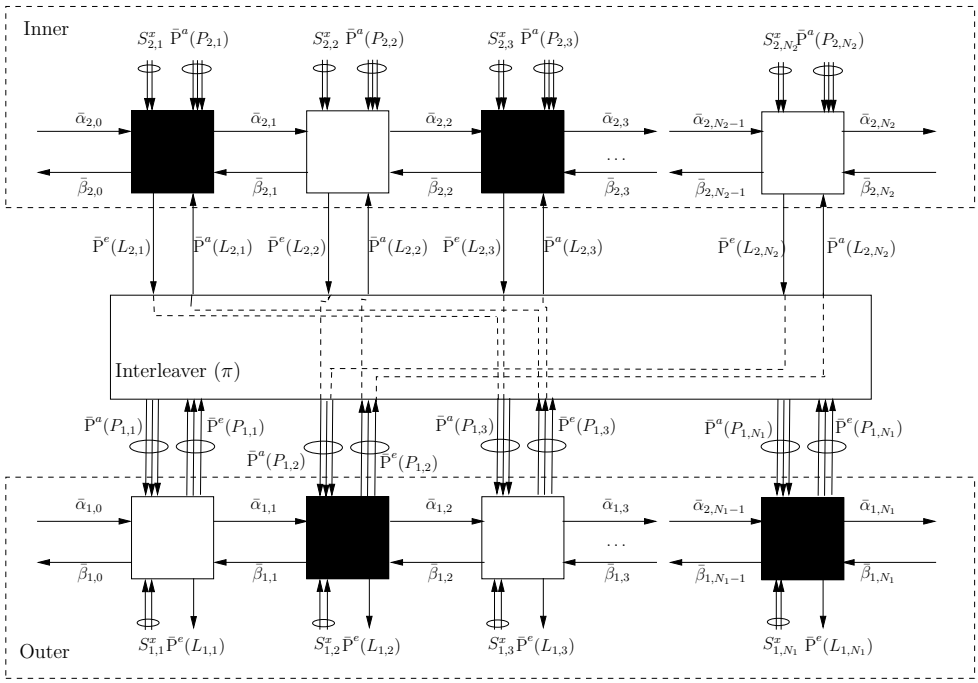


Fig. 5: Schematic of a fully-parallel quantum turbo decoder. *The inner and outer components are assumed to be rate-*$1/3$ *convolutional codes.*

encoder consists of three qubits, which may be represented as $|\overline{\psi}_{1,t}\rangle^{123}$ for the tth output. The odd-even connection of Fig. 5 can be achieved by re-arranging the output of the outer encoder before the interleaver, so that we have $\{|\overline{\psi}_{1,1}\rangle^1|\overline{\psi}_{1,2}\rangle^1 \ldots |\overline{\psi}_{1,N_1}\rangle^1|\overline{\psi}_{1,1}\rangle^2|\overline{\psi}_{1,2}\rangle^2 \ldots |\overline{\psi}_1, N_1\rangle^2|\overline{\psi}_{1,1}\rangle^3 |\overline{\psi}_{1,2}\rangle^3 \ldots |\overline{\psi}_1, N_1\rangle^3\}$. Similarly, the output of the de-interleaver at the decoder is also re-arranged before being fed to the outer inverse encoder. When the inner and outer algorithmic blocks are discretely distributed in the odd and even sets, then the FPQTD procedure may be modified so that each decoding iteration consumes two time periods. During the first time period, all odd blocks of the inner decoder and all even blocks of the outer decoder, which are marked in black in Fig. 5, operate concurrently. During the next time period, all even blocks of the inner decoder and all odd blocks of the outer decoder, which are marked in white in Fig. 5, operate using the *a-priori* information gleaned from the previous time period. This doubles the rate of convergence, as the *extrinsic* information propagates faster between the algorithmic blocks as well as between the inner and outer decoders. Consequently, while each decoding iteration consumes two time periods, the total number of decoding iterations is reduced to half, as it will be demonstrated in Section V-B. Hence, the complexity is reduced by 50%, while the latency/throughput remains the same.

V. Results and Discussions

In this section, we quantify the explicit benefits of our proposed FPQTD by analyzing the performance of a rate-$1/9$ QTC, consisting of two serially concatenated $[3, 1, 3]$ QCCs. In particular, for both the inner as well as the outer components, we have used the configuration termed as "PTO1R" in [23], [24], whose seed transformation (decimal notation) is:

$$U = \{1355, 2847, 558, 2107, 3330, 739, 2009, 286, 473, 1669, 1979, 189\}_{\text{decimal}} \quad (33)$$

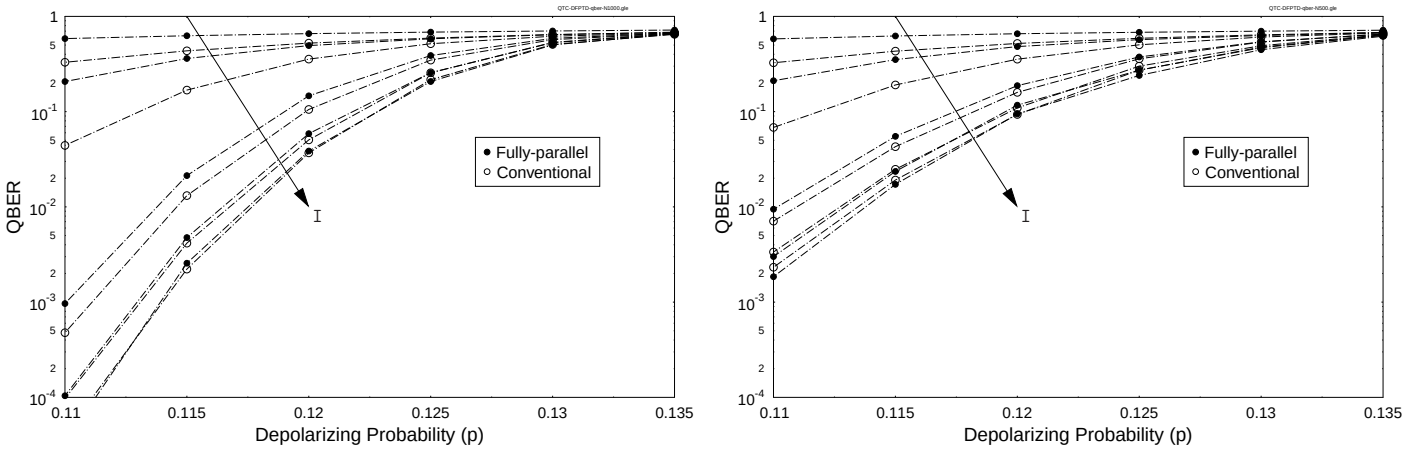
More explicitly, the elements of Eq. (33) represent the decimal equivalent of the rows of the (12×12)-element binary seed transformation U corresponding to the Pauli seed transformation $\mathcal{U}$ of Eq. (11). Furthermore, we have used approximate-log for evaluating the $\max^*$ operator[4].

A. Performance Comparison with Conventional Decoder

In Fig. 6a, we compare the QBER performance of the proposed FPQTD to that of the conventional decoder for an interleaver length of $3,000$ qubits. Since we have used rate-$1/3$ QCCs, an interleaver length of $3,000$ qubits implies that we have $N_1 = 1000$, while $N_2 = 3000$. Hence, the conventional quantum turbo decoding would require $(2N_1 + 2N_2) = 4000$ time periods for each decoding iteration. In Fig. 6a, the performance of the conventional decoder

[4]Please refer to Footnote 3.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2016.2581978, IEEE Access



(a) Interleaver length of $3,000$ qubits.

(b) Interleaver length of $1,500$ qubits.

Fig. 6: Achievable QBER performance for $\mathtt{I} \in \{1, 2, 4, 6, 8\}$ iterations of the conventional decoder, while $\mathtt{I} \in \{10, 20, 40, 60, 80\}$ iterations are used for the fully-parallel turbo decoder.

p	Conventional	Fully-Parallel
0.125	6.5	80
0.12	4.6	50
0.115	3.4	35
0.11	2.8	28

TABLE I: Average number decoding iterations required for the conventional and fully-parallel quantum turbo decoder.

is plotted for $\mathtt{I} \in \{1, 2, 4, 6, 8\}$ decoding iterations, while $\mathtt{I} \in \{10, 20, 40, 60, 80\}$ iterations are invoked for the FPQTD. It may be observed that at a higher iteration index (or equivalently close to convergence), the FPQTD requires about ten times more iterations than the conventional decoder for the sake of achieving a similar performance. We further compare the average number of decoding iterations invoked by the proposed FPQTD to that of the conventional decoder in Table I. It may be observed in Table I that the FPQTD requires on average about 10 to 12 times more iterations than the conventional scheme. The slower convergence of FPQTD is imposed by its parallel nature. More explicitly, since the information is not propagated through the algorithmic blocks as well as to the other decoder in the same decoding iteration, the FPQTD requires significantly more decoding iterations for propagating the information, thus imposing a higher computational complexity, which is quantified in Table I in terms of the average number of decoding iterations required for attaining convergence. Nevertheless, the FPQTD brings with it huge benefits in terms of the total number of time periods required for decoding. More explicitly, while the conventional decoder requires a total of $(2N_1+2N_2)\times \mathtt{I}$ time periods, i.e. $8000 \times \mathtt{I}$ when $N_1 = 1000$ and $N_2 = 3000$, the number of time periods required by the fully-parallel scheme is as low as the number of decoding iterations. This is because our FPQTD scheme requires a single time period for each decoding iteration. Since the FPQTD requires about ten times more iterations, it reduces the total number of decoding time periods by a factor of 800, thereby reducing the associated latency (or equivalently increasing the maximum tolerable clock-rate and hence the throughput).

Let us now extend our analysis to an interleaver length of $1,500$ qubits in Fig. 6b, which exhibits the same trend as that of Fig. 6a. Hence, regardless of the interleaver length, the fully-parallel scheme converges to the same QBER performance as that of the conventional decoder by invoking around ten times more iterations. We further compare the performance of the two schemes in Fig. 7 by quantifying their discrepancy from the Hashing bound at a QBER of 10^{-4} for different interleaver lengths. It may be observed in Fig. 7 that the FPQTD exhibits the same performance as that of the conventional scheme for all interleaver lengths, provided that ten times more iterations are invoked. Hence, the FPQTD is likely to reduce decoding times by a factor of $(2N_1 + 2N_2)/10 = 0.8N_1$ for any input frame length N_1 of the rate-$1/9$ QTC of [24].

B. Impact of Odd-Even Interleaver

In Fig. 8, we quantify the benefits of exploiting the knowledge of the odd-even interleaving pattern in the fully-parallel architecture. More specifically, we compare the performance of FPQTD having a random interleaver to that of an odd-even interleaver. Fig. 8 portrays the performance of the random interleaver for $\mathtt{I} \in \{10, 20, 40, 60, 80\}$ iterations, while $\mathtt{I} \in \{5, 10, 20, 30, 40\}$ iterations are used for the odd-even interleaver. As observed in Fig. 8, the odd-even interleaving pattern yields faster decoding convergence without compromising the achievable QBER performance. In particular, the odd-even interleaving gives around 50% reduction in the

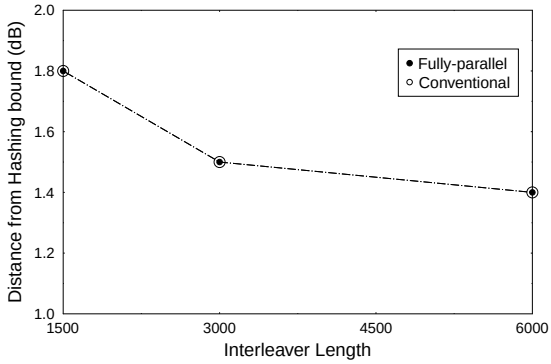


Fig. 7: Distance from the Hashing bound for conventional ($\mathtt{I}$ = 8) and full-parallel turbo decoder ($\mathtt{I}$ = 80) at QBER = 10^{-4}.

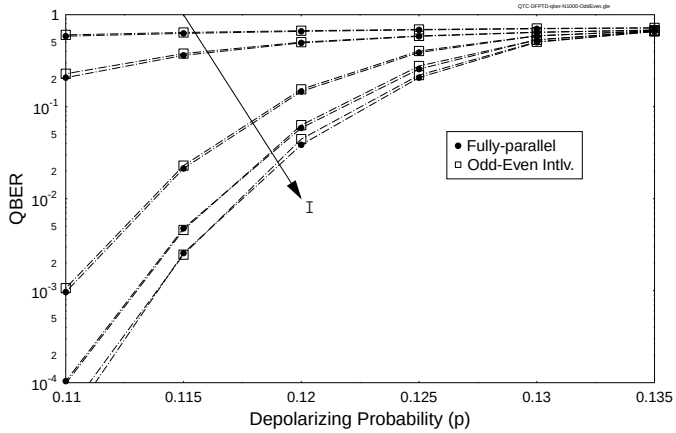


Fig. 8: Achievable QBER performance of a fully-parallel quantum turbo decoder, when a random and an odd-even interleaver are used. $\mathtt{I} \in \{10, 20, 40, 60, 80\}$ iterations are invoked for the random interleaver, while $\mathtt{I} \in \{5, 10, 20, 30, 40\}$ iterations are used for the odd-even interleaver.

number of decoding iterations, which is also seen from the average number of decoding iterations tabulated in Table II. Furthermore, since an odd-even QFPTD decoder uses two time slots for each decoding iteration, the total latency is the same as that of QFPTD relying on a random interleaver. However, the overall complexity is reduced to half.

VI. Conclusions

In this contribution, we have conceived a fully-parallel architecture for quantum turbo decoding. The proposed scheme circumvents the inherent time dependencies associated with the conventional quantum turbo decoding by allowing all the constituent algorithmic blocks to operate concurrently. Consequently, while the decoding delay or latency of the conventional sequential decoding is a function of the frame length, the decoding delay incurred by the proposed QFPTD is independent of the frame length. We have demonstrated that QFPTD reduces the total number of decoding time periods by a factor of 800 for a frame length of $1,000$ qubits. This is particularly important for quantum systems, which have low coherence times at the time of writing. We have also quantified the benefits of employing an odd-even interleaver pattern in conjunction with FPQTD. More specifically, the odd-even interleaver design reduces the computational complexity by half, while exhibiting the same QBER.

p	random	odd-even
0.125	80	41
0.12	50	26
0.115	35	18
0.11	28	15

TABLE II: Average number decoding iterations required for the fully-parallel quantum turbo decoding with random and odd-even interleavers.

References

[1] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, pp. 78–88, January 1983. [Online]. Available: http://doi.acm.org/10.1145/1008908.1008920

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. New York: IEEE Press, 1984, pp. 175–179.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.70.1895

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

[5] 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

[6] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, June 2008. [Online]. Available: http://dx.doi.org/10.1038/nature07127

[7] R. Beals, S. Brierley, O. Gray, A. W. Harrow, S. Kutin, N. Linden, D. Shepherd, and M. Stather, "Efficient distributed quantum computing," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 469, no. 2153, 2013. [Online]. Available: http://rspa.royalsocietypublishing.org/content/469/2153/20120686

[8] P. Botsinis, D. Alanis, Z. Babar, S. Ng, and L. Hanzo, "Non-coherent quantum multiple symbol differential detection for wireless systems," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2015.

[9] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems," *IEEE Transactions on Communications*, vol. 63, no. 10, pp. 3713–3727, Oct 2015.

[10] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, "Non-dominated quantum iterative routing optimization for wireless multihop networks," *IEEE Access*, vol. 3, pp. 1704–1728, 2015.

[11] S. Lin and D. J. Costello, *Error Control Coding, Second Edition*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 2004.

[12] 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 Edition*. New York, USA: John Wiley IEEE Press, March 2011.

[13] 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

[14] P. W. Shor, "The quantum channel capacity and coherent information," *Lecture Notes, MSRI Workshop on Quantum Computation*, 2002.

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

[16] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Technical Program of the IEEE International Conference on Communications, ICC '93 Geneva*, vol. 2, May 1993, pp. 1064–1070 vol.2.

[17] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," in *IEEE International Symposium on Information Theory*, July 2008, pp. 310–314.

[18] D. Poulin, J. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776–2798, June 2009.

[19] 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

[20] H. Ollivier and J. P. Tillich, "Quantum convolutional codes: fundamentals," *quant-ph/0401134*, 2004.

[21] G. D. Forney, M. Grassl, and S. Guha, "Convolutional and tail-biting quantum error-correcting codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 865–880, March 2007.

[22] M. Grassl and M. Rotteler, "Constructions of quantum convolutional codes," in *IEEE International Symposium on Information Theory*, June 2007, pp. 816–820.

[23] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *IEEE International Symposium on Information Theory Proceedings*, Aug. 2011, pp. 445 – 449.

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

[25] Z. Babar, S. X. Ng, and L. Hanzo, "EXIT-chart aided near-capacity quantum turbo code design," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2014.

[26] J. Kliewer, S. X. Ng, and L. Hanzo, "Efficient computation of EXIT functions for non-binary iterative decoding," *IEEE Transactions on Communications*, vol. 54, no. 12, pp. 2133–2136, December 2006.

[27] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[28] R. Maunder, "A fully-parallel turbo decoding algorithm," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2762–2775, Aug 2015.

[29] H. A. Ngo, R. Maunder, and L. Hanzo, "Extrinsic information transfer charts for characterizing the iterative decoding convergence of fully parallel turbo decoders," *IEEE Access*, vol. 3, pp. 2100–2110, 2015.

[30] H. Ngo, R. Maunder, and L. Hanzo, "Fully parallel turbo equalization for wireless communications," *IEEE Access*, vol. 3, pp. 2652–2664, 2015.

[31] A. Li, L. Xiang, T. Chen, R. Maunder, B. Al-Hashimi, and L. Hanzo, "VLSI implementation of fully-parallel LTE turbo decoders," *Access, IEEE*, vol. PP, no. 99, pp. 1–1, 2016.

[32] Z. Babar, P. Botsinis, D. Alanis, S. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2015.

[33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

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

[35] E. Pelchat and D. Poulin, "Degenerate Viterbi decoding," *IEEE Transactions on Information Theory*, vol. 59, no. 6, pp. 3915–3921, 2013.

[36] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A*, vol. 55, pp. 4054–4059, Jun 1997. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.55.4054

[37] D. MacKay, G. Mitchison, and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, Oct 2004.

[38] J. Dehaene and B. De Moor, "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

[39] D. Lidar and T. Brun, *Quantum Error Correction*. Cambridge University Press, 2013. [Online]. Available: http://books.google.co.uk/books?id=XV9sAAAAQBAJ

[40] D. Gottesman, *The Heisenberg Representation of Quantum Computers*. [online] http://arxiv.org/pdf/quant-ph/9807006v1.pdf, December 2001.

[41] P. Robertson, E. Villebrun, and P. Hoeher, "A comparison of optimal and sub-optimal map decoding algorithms operating in the log domain," in *Communications, 1995. ICC '95 Seattle, 'Gateway to Globalization', 1995 IEEE International Conference on*, vol. 2, Jun 1995, pp. 1009–1013 vol.2.

Zunaira Babar received her B.Eng. degree in electrical engineering from the National University of Science & Technology (NUST), Islamabad, Pakistan, in 2008, and the M.Sc. degree (Distinction) and the Ph.D degree in wireless communications from the University of Southampton, UK, in 2011 and 2015, respectively. She is currently working as a Research Fellow in the Southampton Wireless group at the University of Southampton.

Her research interests include quantum error correction codes, channel coding, coded modulation, iterative detection and cooperative communications.

Hung Viet Nguyen received the B.Eng. degree in Electronics & Telecommunications from Hanoi University of Science and Technology (HUST), Hanoi, Vietnam, in 1999, the M.Eng. in Telecommunications from Asian Institute of Technology (AIT), Bangkok, Thailand, in 2002 and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 2013. Since 1999 he has been a lecturer at the Post & Telecommunications Institute of Technology (PTIT), Vietnam. He is involved in the OPTIMIX and CONCERTO European projects. He is currently a postdoctoral researcher at Southampton Wireless (SW) group, University of Southampton, UK. His research interests include cooperative communications, channel coding, network coding and quantum communications.

Panagiotis Botsinis (S'12) received the M.Eng. degree from the School of Electrical and Computer Engineering of the National Technical University of Athens (NTUA), Greece, in 2010, as well as the M.Sc. degree with distinction and the Ph.D. degree in Wireless Communications from the University of Southampton, UK, in 2011 and 2015, respectively. He is currently working as a Research Fellow in the Southampton Wireless group at the School of Electronics and Computer Science of the University of Southampton, UK. Since October 2010, he has been a member of the Technical Chamber of Greece.

His research interests include quantum-assisted communications, quantum computation, iterative detection, OFDM, MIMO, multiple access systems, coded modulation, channel coding, cooperative communications, as well as combinatorial optimization.

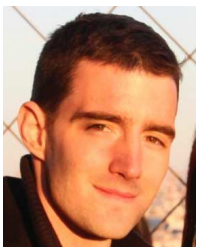
Dimitrios Alanis (S'13) received the M.Eng. degree in Electrical and Computer Engineering from the Aristotle University of Thessaloniki in 2011 and the M.Sc. degree in Wireless Communications from the University of Southampton in 2012. He is currently working towards the PhD degree with the Southampton Wireless (SW) Group, School of Electronics and Computer Science of the University of Southampton.

His research interests include quantum computation and quantum information theory, quantum search algorithms, cooperative communications, resource allocation for self-organizing networks, bio-inspired optimization algorithms and classical and quantum game theory.

Daryus Chandra received the M.Eng. degree in electrical engineering from Universitas Gadjah Mada (UGM), Indonesia, in 2014. He is currently pursuing the Ph.D degree with the Southampton Wireless group, School of Electronics and Computer Science, University of Southampton. He is a recipient of scholarship award from Indonesia Endowment Fund for Education (LPDP). His research interests includes channel codes, quantum error correction codes, and quantum communications.

Dr Soon Xin Ng (S'99-M'03-SM'08) received the B.Eng. degree (First class) in electronics engineering and the Ph.D. degree in wireless communications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow working on collaborative European research projects known as SCOUT, NEWCOM and PHOENIX. Since August 2006, he has been a member of academic staff in the School of Electronics and Computer Science, University of Southampton. He is involved in the OPTIMIX and CONCERTO European projects as well as the IUATC and UC4G projects. He is currently an Associate Professor of Telecommunications with the University of Southampton. He has authored over 180 papers and co-authored two John Wiley/IEEE Press books in his research field.

His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum error correction codes and joint wireless-and-optical-fiber communications. He is a a Chartered Engineer and a Fellow of the Higher Education Academy in the UK.



Robert G. Maunder has studied with Electronics and Computer Science, University of Southampton, UK, since October 2000. He was awarded a first class honors BEng in Electronic Engineering in July 2003, as well as a PhD in Wireless Communications in December 2007. He became a lecturer in 2007 and an Associated Professor in 2013. Rob's research interests include joint source/channel coding, iterative decoding, irregular coding and modulation techniques. For further information on this research, please refer to http://users.ecs.soton.ac.uk/rm.

Lajos Hanzo Lajos Hanzo (M'91-SM'92-F'04) received his degree in electronics in 1976 and his doctorate in 1983. In 2009 he was awarded the honorary doctorate "Doctor Honoris Causa" by the Technical University of Budapest. During his 38-year career in telecommunications he has held various research and academic posts in Hungary, Germany and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised about 100 PhD students, co-authored 20 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10,000 pages, published 1,500+ research entries at IEEE Xplore, acted both as TPC and General Chair of IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. Currently he is directing a 100-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Councilâs Advanced Fellow Grant and the Royal Societyâs Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses.

Lajos is a Fellow of the Royal Academy of Engineering, of the Institution of Engineering and Technology, and of the European Association for Signal Processing. He is also a Governor of the IEEE VTS. During 2008-2012 he was the Editor-in-Chief of the IEEE Press and a Chaired Professor also at Tsinghua University, Beijing. He has 22,000+ citations. For further information on research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk.