Quantum State Compression with Polar Codes

Jack Weinberg[1,2], Avijit Mandal[1,3], and Henry D. Pfister[1,2,3]

[1]Department of Electrical and Computer Engineering, Duke University
[2]Department of Mathematics, Duke University
[3]Duke Quantum Center, Duke University

***Abstract*—In the quantum compression scheme proposed by Schumacher, Alice compresses a message that Bob decompresses. In that approach, there is some probability of failure and, even when successful, some distortion of the state. For sufficiently large blocklengths, both of these imperfections can be made arbitrarily small while achieving a compression rate that asymptotically approaches the source coding bound. However, direct implementation of Schumacher compression suffers from poor circuit complexity. In this paper, we consider a slightly different approach based on classical syndrome source coding. The idea is to use a linear error-correcting code and treat the state to be compressed as a superposition of error patterns. Then, Alice can use quantum gates to apply the parity-check matrix to her message state. This will convert it into a superposition of syndromes. If the original superposition was supported on correctable errors (e.g., coset leaders), then this process can be reversed by decoding. An implementation of this based on polar codes is described and simulated. As in classical source coding based on polar codes, Alice maps the information into the "frozen" qubits that constitute the syndrome. To decompress, Bob utilizes a quantum version of successive cancellation coding.**

I. Introduction

Quantum computation is the use of quantum mechanical effects for information processing. At sufficient scale, quantum computers hold promise for myriad problems including integer factorization, cryptography, and the simulation of physical systems which are intractable on contemporary classical computers [1]. As with classical computers, efficient methods for the compression of quantum information will be instrumental for practical quantum computation [2]. In 1995, Schumacher proposed the first method for rate-optimal lossless quantum state compression [3] and it can be seen as a generalization of Shannon's original protocol for rate-optimal lossless classical compression. However, direct implementation on a quantum computer is quite complex because, for n qubits, it involves rearranging the 2^n basis elements in a complicated fashion [4].

One can also use linear error-correcting codes to implement rate-optimal classical compression [5]–[7]. Here, we describe the associated method for rate-optimal quantum compression based on linear error-correcting codes. In particular, we use polar codes [8]. Polar codes are known to be rate-optimal for many coding and compression problems [7]–[10] and, for many of these, they allow efficient encoding and decoding. Until recently, however, extensions to quantum problems did not naturally lead to efficient decoding algorithms.

This research was supported in part by the National Science Foundation (NSF) under Grants 2106213 and 2120757.

For the pure-state classical-quantum (CQ) channel, belief-propagation with quantum messages (BPQM) can provide optimal decoding for systems defined by tree-like factor graphs [11]–[14]. This approach has also been extended to binary-input symmetric CQ channels and polar codes [15]–[17]. In this paper, an efficient quantum successive cancellation decoding algorithm is defined for the proposed scheme.

We begin with an overview of requisite classical and quantum coding theory. Then, we describe the compression protocol and provide results describing its asymptotic performance. Next, we provide simulation results for our protocol with blocklength 8 and 16. Finally, we conclude with a discussion of this protocol's relationship with, and implications for, quantum compression more generally.

II. Background

A. Binary Linear Codes

An $[N, K]$ binary linear code $\mathcal{C}$ is a K-dimensional subspace of $\mathbb{F}_2^N$. Such a code can be defined as the row space of a generator matrix $G \in \mathbb{F}_2^{K \times N}$ or as the null space of a parity-check matrix $H \in \mathbb{F}_2^{(N-K)\times N}$. For an error vector $z \in \mathbb{F}_2^N$, the syndrome of z is defined as $s = zH^T$. We note that $s = 0$ if and only if $z \in \mathcal{C}$. Since $\mathcal{C}$ is a subgroup of the additive group of $\mathbb{F}_2^N$, it follows that $\mathbb{F}_2^N$ can be partitioned into cosets of $\mathcal{C}$ and all elements in a coset will have the same syndrome. In each coset, one can choose a coset leader by selecting an element of minimum Hamming weight and breaking ties arbitrarily [18]. For communication over a binary symmetric channel (BSC), the transmitted codeword $x \in \mathbb{F}_2^N$ may be corrupted by an error vector $z \in \mathbb{F}_2^N$, resulting in the received bit string $y = x + z$. The decoder returns the codeword closest to a codeword with ties broken arbitrarily. Such a scheme can also be implemented by syndrome decoding, where the syndrome $s = yH^T$ is computed first and then the error estimate $\hat{z} \in \mathbb{F}_2^n$ is computed from s by selecting the coset leader of the coset associated with syndrome s [5].

B. Polar Codes

Arikan's polar transformation is defined by an invertible matrix $G_N \in \mathbb{F}_2^{N \times N}$ that maps $\mathbb{F}_2^N$ to itself via $x = uG_N$ [8]. The vector x is transmitted over a memoryless channel with capacity C to give the output y. For the i-th input bit, one can define an effective channel whose input is u_i and whose output is (y, u_1^{i-1}). As N tends to infinity, the capacities of the individual effective channels become polarized and, for any

$\varepsilon \in (0, 1/2)$, the proportion of "good" channels (i.e., channels with capacity greater than $1 - \varepsilon$) converges to C while the proportion of "bad" channels (i.e., channels with capacities less than $1 - \varepsilon$) converges to $1 - C$. When using a polar code for communication, one only sends information over the good channels. Thus, the N bit message consists of K "information" bits which constitute a message and $N - K$ "frozen" bits which are known by the receiver and thus carry no information. By freezing the bad channels, one enables the successive cancellation decoder to recover bits transmitted across good channels with high probability. The polar transformation G_N on N bits may be defined recursively as follows:

- R_N is the $N \times N$ permutation matrix for the reverse shuffle permutation $(1, 3, ..., N-1, 2, 4, ..., N)$.
- $G_N \coloneqq (I_{N/2} \otimes G_2) R_N (I_2 \otimes G_{N/2})$, $G_2 \coloneqq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

While originally designed for error correction on classical channels, polar codes have been adapted to many problems.

C. Syndrome Source Coding

Syndrome source coding is one popular method for adapting linear codes to lossless compression [5], [7]. In syndrome source coding, one compresses the vector $x \in \mathbb{F}_2^N$ by computing its syndrome $s = xH^T$ using the parity-check matrix H of a linear code . To decompress, the decoder maps the syndrome s to the coset leader of its associated coset. This scheme is successful if and only if the message to be compressed is a coset leader [5]. Likewise, syndrome decoding of an error is successful if and only if the error is a coset leader. Thus, syndrome source coding is successful if and only if the vector to be compressed is an error that is correctable by the syndrome decoder of the code. We also note that the successive cancellation decoder for polar codes is easily transformed into a polar syndrome decoder [7] which, for the BSC, corrects the same errors as the original decoder.

D. Quantum Formalism

The set of natural numbers is denoted by $\mathbb{N} = \{1, 2, \ldots\}$ and we use the shorthand $[n] \coloneqq \{1, \ldots, n\}$ for $n \in \mathbb{N}$. We denote the n-dimensional Hilbert space by $\mathcal{H}_n$. We call a unit length vector $|\psi\rangle \in \mathcal{H}_n$ a *pure state*. An ensemble of m pure states $\{p_i, |\psi_i\rangle\}$ in which p_i is the probability of choosing the pure state $|\psi_i\rangle$ is represented using a positive semidefinite, unit trace matrix ρ which we call a *density matrix*. In other words, for the ensemble $\{p_i, |\psi_i\rangle\}$, ρ can be written as

$$\rho = \sum_{i \in [m]} p_i |\psi_i\rangle\langle\psi_i| .$$

The map $|\psi\rangle \to U|\psi\rangle$ for unitary $U \in \mathbb{C}^{n \times n}$ is called the *unitary evolution* of the state $|\psi\rangle \in \mathcal{H}_n$. Thus, the action of U on the ensemble $\{p_i, |\psi_i\rangle\}$ is described by $\tilde{\rho}$, where

$$\tilde{\rho} = \sum_{i \in [m]} p_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger$$

and $U^\dagger$ is the Hermitian transpose of U. An m-outcome projective measurement on a state in $\mathcal{H}_n$ is implemented through a set of m orthogonal projection matrices $\Pi_j \in \mathbb{C}^{n \times n}$ for $1 \le j \le m$, where $\delta_{i,j}$ is the Kronecker delta function. These projection matrices satisfy $\Pi_i \Pi_j = \delta_{i,j} \Pi_i$ and $\sum_j \Pi_j = I$. We denote this measurement by $\hat{\Pi} = \{\Pi_j\}|_{j=1}^m$. When we apply the measurement $\hat{\Pi}$ on the state ρ, the probability of outcome j is $p_j = \mathrm{Tr}(\Pi_j \rho)$ and the resulting post-measurement state is $\rho_j = (\Pi_j \rho \Pi_j)/\mathrm{Tr}(\Pi_j \rho)$. We use the notation ρ_{A^N} to denote the tensor product state of N quantum states in quantum systems $A_1, \ldots A_N$ such that

$$\rho_{A^N} = \rho_{A_1} \otimes \cdots \otimes \rho_{A_N},$$

where ρ_{A_i} corresponds to quantum state in A_i. Similarly, we use the shorthand notation $|\psi_{x^N}\rangle_{A^N}$ to denote the tensor product of pure states in system $A_1, \ldots, A_N$ i.e.

$$|\psi_{x^N}\rangle_{A^N} = |\psi_{x_1} \ldots \psi_{x_N}\rangle_{A^N} = |\psi_{x_1}\rangle_{A_1} \otimes \cdots \otimes |\psi_{x_N}\rangle_{A_N} .$$

We also define the embedding of $\mathbb{F}_2^N$ into $\mathbb{C}^{2^N}$ via the mapping $(a_1, a_2, ..., a_N) \in \mathbb{F}_2^N$ to $|a_1 a_2 ... a_N\rangle$. Similarly, given a one-to-one boolean function $f : \mathbb{F}_2^M \to \mathbb{F}_2^N$ with $N \ge M$, we define $E(f)$ to be its embedding into the space of isometries from $A = \mathbb{C}^{2^M}$ to $B = \mathbb{C}^{2^N}$ via

$$E(f) \coloneqq \sum_{x^M \in \mathbb{F}_2^M} {}_B\big|f(x^M)\big\rangle \left\langle x^M\right|_A . \tag{1}$$

E. Quantum Compression by Schumacher

Schumacher [3] proposed a direct generalization of Shannon's protocol for lossless compression to the quantum setting. To understand Schumacher's protocol, we begin with definitions related to classical compression. As usual, the aim of the compression protocol is for Alice to compress a message which Bob subsequently decompresses. Consider N-bit strings produced by a classical source with alphabet $\mathcal{X}$, alphabet size $|\mathcal{X}| = n$ and distribution p_X. The entropy $H(X)$ of such a source is defined as

$$H(X) \coloneqq -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x).$$

The sample entropy $\overline{H}(x^N)$ of a sequence x^N is defined as

$$\overline{H}(x^N) \coloneqq -\frac{1}{N} \log\big(p_{X^N}(x^N)\big).$$

The δ-typical set $T_\delta^{X^N}$ is defined as

$$T_\delta^{X^N} \coloneqq \{x^N : |\overline{H}(x^N) - H(X)| < \delta\}.$$

With these classical definitions, we are equipped to understand the quantum problem. Consider a *quantum information source* described by the state ρ. We can express the state ρ using the eigenvalue decomposition as

$$\rho = \sum_{x \in \mathcal{X}} p_X(x) |\psi_x\rangle\langle\psi_x| , \tag{2}$$

where $p_X(x)$ corresponds to the probability of choosing the pure state $|\psi_x\rangle$ and $\langle\psi_x|\psi_{x'}\rangle = 0$ if $x \neq x'$. The von Neumann entropy of ρ is defined by

$$S(\rho) \coloneqq -\mathrm{Tr}(\rho \log \rho) = -\sum_{x \in \mathcal{X}} p_X(x) \log(p_X(x)).$$

In other words, the state ρ can be represented by the ensemble $\{p_X(x), |\psi_x\rangle\}$. ρ can be decomposed in many ways using non-orthogonal states. However, the representation of state ρ in terms of eigenvectors achieves von Neumann entropy which ensures maximum compressibility. Similarly, consider joint quantum state ρ_{A^N} with N states drawn from the ensemble $\{p_X(x), |\psi_x\rangle\}$. Using the representation of ρ in Eq. (2), we can decompose ρ_{A^N} in the following form

$$\rho_{A^N} = \sum_{x^N \in \mathcal{X}^N} p_{X^N}(x^N) \, |\psi_{x_1} \ldots \psi_{x_N}\rangle\!\langle\psi_{x_1} \ldots \psi_{x_N}|_{A^N} \, ,$$

where $p_{X^N}(x^N) = p_X(x_1) \ldots p_X(x_N)$. The classical sequences $x^N \in \mathcal{X}^N$ correspond to the indices of the quantum state in the decomposition of ρ_{A^N}. To define quantum typicality, we construct the typical subspace as follows

$$T_\delta^{\rho_{A^N}} = \text{span}\{|\psi_{x^N}\rangle : x^N \in T_\delta^{X^N}\}.$$

This is exactly the subspace spanned by states $|\psi_{x^N}\rangle$ whose labels $x^N \in \mathcal{X}^N$ are δ-typical with respect to the distribution $p_{X^N}(x^N)$. In other words, the notion of quantum typical is similar to classical typicality but quantum typicality is considered in the eigenbasis. Schumacher compression exploits this notion of quantum typicality and the typical subspace corresponding to the state ρ_{A^N} to achieve the quantum compression limit i.e. the von Neumann entropy $S(\rho)$ [9]. The typical projector projects into the typical subspace $T_\delta^{\rho_{A^N}}$ and is given by

$$\Pi_{A^N}^{\rho,\delta} = \sum_{x^N \in T_\delta^{X^N}} |\psi_{x^N}\rangle\!\langle\psi_{x^N}|_{A^N} \, .$$

Consider the projective measurement defined by

$$\{\Pi_{A^N}^{\rho,\delta}, I - \Pi_{A^N}^{\rho,\delta}\}.$$

If the first outcome occurs, then the quantum state is projected onto a typical subspace. If the second outcome occurs, it is projected onto the orthogonal complement and failure is declared. With the addition of a flag qubit F, the action of this measurement on the density matrix ρ_{A^N} is given by

$$\rho_{A^N} \mapsto (I - \Pi_{A^N}^{\rho,\delta})\rho_{A^N}(I - \Pi_{A^N}^{\rho,\delta}) \otimes |0\rangle\!\langle 0|_F + \Pi_{A^N}^{\rho,\delta}\rho_{A^N}\Pi_{A^N}^{\rho,\delta} \otimes |1\rangle\!\langle 1|_F \, .$$

This measurement is called the typical subspace projection as it projects to the δ-typical subspace of A^N. In general, this also causes a small distortion of the state because a small fraction state's mass lies outside of the typical set. More precisely, it follows from $\text{Tr}\left(\Pi_{A^N}^{\rho,\delta}\right) < 2^N$ that $\|\rho_{A^N} - \mathcal{E}(\rho_{A^N})\| > 0$ if ρ is non-singular, where $\mathcal{E}$ is the channel defined by the typical subspace projection. However, this error vanishes as $N \to \infty$ provided that $\delta > 0$ and $S(\rho) < 1$. After the projection, Alice's task is to compress the projected state $\Pi_{A^N}^{\rho,\delta}\rho_{A^N}\Pi_{A^N}^{\rho,\delta}$ before sending it to Bob. Since

$$\text{Tr}\left(\Pi_{A^N}^{\rho,\delta}\right) = \left|\Pi_{A^N}^{\rho,\delta}\right| \le 2^{N(S(\rho)+\delta)},$$

there is a bijective boolean function that maps the classical typical sequences to the set of binary sequences of length $N(S(\rho) + \delta)$ denoted by $f : T_\delta^{X^N} \to \{0,1\}^{N[S(\rho)+\delta]}$. Thus, Alice can use Eq. (1) to construct the isometry $U_f = E(f)$ mapping A^N to $\mathbb{C}^{2^{N[S(\rho)+\delta]}}$. Observe that this isometry maps the set of message strings into the set of typical strings used in Shannon's protocol. To decompress Alice's state, Bob applies $U_f^\dagger$ on the received state. This strategy approaches the fundamental limiting compression rate of $S(\rho)$.

F. Quantum Compression via Syndrome Source Coding

Linear codes may also be adapted to implement lossless quantum state compression. We describe this adaptation here in a generic way before later addressing the particular case of polar codes, which is the main subject of this paper. As described in section II-C, any linear code can be used to implement lossless classical compression via syndrome source coding. Let $\mathcal{C}$ be an $[N, K]$ binary linear code with full-rank parity-check matrix H. Let H' be an invertible extension of H that is formed by adding K rows to the bottom of H so that H' is full rank. Suppose Alice wants to compress a state drawn a quantum information source described by $\rho^{\otimes N}$, where ρ describes a single qubit state with spectral decomposition

$$\rho = (1-p)\,|\psi_0\rangle\!\langle\psi_0| + p\,|\psi_1\rangle\!\langle\psi_1| \, .$$

Then, Alice and Bob may compress and decompress $\rho^{\otimes N}$ by embedding the syndrome-source coding protocol for $\mathcal{C}$ into the quantum domain as follows:

1) Alice applies $U_\rho^{\otimes N}$ to her state, where U_ρ is the unitary that diagonalizes ρ, to get
$$\overline{\rho} = U_\rho \rho U_\rho^\dagger = (1-p)\,|0\rangle\!\langle 0| + p\,|1\rangle\!\langle 1| \, .$$
2) Alice applies the quantum instrument map $\mathcal{E}$ defined by $\overline{\rho} \mapsto (\Pi_K^N \overline{\rho} \Pi_K^N) \otimes |1\rangle\langle 1|_B + ((I_N - \Pi_K^N)\overline{\rho}(I_N - \Pi_K^N)) \otimes |0\rangle\langle 0|_B$ to her state, where $\Pi_K^N := \sum_{x^N \in T} \left|x^N\right\rangle \left\langle x^N\right|$ and T is the set of computational basis states indexed by coset leaders of $\mathcal{C}$ (i.e., the set of errors correctable by syndrome decoding). The state of the resulting system is denoted by $\tilde{\rho}'$.
3) Alice measures system B with the projective measurement $\{|0\rangle\!\langle 0|, |1\rangle\!\langle 1|\}$. If the outcome is $|0\rangle$, failure is declared. Otherwise, the outcome is $|1\rangle$ and she applies the unitary embedding of H', represented by $U_{H'} = E(H'x)$, to $\tilde{\rho}'$. We use the extended matrix H' because the matrix H is typically not invertible and thus cannot be embedded into a unitary. Then, Alice sends the first $N-K$ qubits to Bob. This is equivalent to computing the partial trace over the system $\mathcal{I}$ which consists of the last K qubits. Thus, Bob receives the state $\Psi = \text{Tr}_{\mathcal{I}}(U_{H'}\rho U_{H'}^\dagger)$, which is the mapping into syndrome space of the projection of ρ onto the correctable errors in T.
4) To decompress Ψ, Bob implements syndrome decoding as an isometry. Consider the isometry mapping $N-K$ qubits to N qubits, that is defined by
$$U_D = \sum_{x^N \in T} {}_{A^N}\left|x^N\right\rangle \left\langle Hx^N\right| .$$

Applying U_D to Ψ gives $\tilde{\rho}'$ because the image of Π_K^N is supported on T by construction and thus U_D inverts both the partial trace and the syndrome mapping. Finally, Bob applies $U_\rho^{\dagger\otimes N}$ to invert the diagonalization operation applied by Alice. This gives the desired approximation of Alice's initial state.

III. Protocol

Suppose Alice wants to store an N-qubit tensor product state using as few qubits as possible; she intends to give her stored state to Bob who will then decompress it to recover Alice's original state. Alice's message may be understood as being drawn from a quantum information source described by the state $\rho^{\otimes N}$ where ρ describes a single qubit state. Suppose that ρ has a spectral decomposition

$$\rho = (1-p)\,|\psi_0\rangle\langle\psi_0| + p\,|\psi_1\rangle\langle\psi_1|\,,$$

where $\psi_0, \psi_1 \in \mathcal{H}_2$ are eigenvectors of state ρ. Subsequently, we refer to the probabilities $\{p, 1-p\}$ as probabilities of source qubits for the state ρ. We also assume that Alice has access to the unitary $U_\rho \in \mathbb{C}^{2\times 2}$ such that diagonalizes ρ. This assumption is valid because Alice knows the state ρ and we assume that Bob also knows the unitary U_ρ, which he uses while recovering the compressed state.

Below, we describe how polar codes can be used to implement lossless quantum compression, which we call Schumacher compression in a generic sense. Since U_ρ corresponds to a qubit unitary, both Alice and Bob can inexpensively apply it to their states to realize our compression protocol. We propose that Alice encode her state by embedding the syndrome source coding procedure into the group of unitary operators on her state space. Following the discussion in section II-B, we can embed the binary polar transform G_N into a unitary transform V_N on N qubits (c.f., [19]). While G_N is designed to act on binary vectors via right multiplication (i.e., $u \mapsto uG_N$), we define V_N act on qubits via left multiplication. Thus, we have $V_N = E(G_N^T)$ and this gives

- $V_2 \coloneqq E(G_2^T(x_1, x_2)^T) = \mathrm{CNOT}_{2\to 1}$.
- $U_N^R \coloneqq E(R_N^T x^N) = E(R_N x^N)$ is a SWAP operator on qubits defined by the permutation $(1, 3, ..., N-1, 2, 4, ..., N)$.
- $V_N \coloneqq E(G_N^T x^N) = E((I_{N/2} \otimes G_2^T) R_N (I_2 \otimes G_{N/2}^T) x^N)$ which implies $V_N \coloneqq (\mathbb{I}_{N/2} \otimes V_{N/2})\, U_N^R\, (\mathbb{I}_{N-2} \otimes V_2)$.

where $\mathbb{I}_M$ denotes the identity operator on M qubits. We propose the following compression protocol:

1) Alice and Bob design an N-bit classical polar code for the BSC with error probability p, or BSC(p). They agree on the set $\mathcal{I}$ of indices for the K information qubits so that $\mathcal{I}^c$ contains the indices of the $N-K$ frozen bits. Let $f\colon \mathbb{F}_2^{N-K} \to \mathbb{F}_2^N$ be the boolean function defined by polar syndrome decoding that maps syndromes to error patterns. Let T be the range of f (i.e., the set of correctable error patterns for polar syndrome decoding).
2) Alice applies a unitary $U_\rho^{\otimes N}$ to $\rho^{\otimes N}$ where U_ρ is a change of basis operator from the eigenbasis of ρ to the computational basis: she obtains the state $\overline{\rho} = U_\rho^{\otimes N} \rho^{\otimes N} U_\rho^{\otimes N\dagger}$.
3) Alice encodes the message:
   (a) Alice must apply the quantum instrument map $\mathcal{E}$ defined by $\overline{\rho} \mapsto (\Pi_K^N \overline{\rho} \Pi_K^N) \otimes |1\rangle\langle 1|_B + ((I_N - \Pi_K^N)\overline{\rho}(I_N - \Pi_K^N)) \otimes |0\rangle\langle 0|_B$ to her state, where $\Pi_K^N \coloneqq \sum_{x^N \in T} |x^N\rangle\langle x^N|$ is the projection onto the set of correctable error patterns, obtaining $\tilde{\rho}'$. However, directly applying this isometry is intractable for large block lengths. Thus, Alice instead makes use of the efficient quantum successive cancellation decoding algorithm described in Section IV to apply this projection.
   (b) Alice measures system B with the projective measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. If the outcome is $|0\rangle\langle 0|$, failure is declared. Otherwise, the outcome is $|1\rangle\langle 1|$ and she applies V_N to system A.
   (c) Alice sends the frozen qubits with indices in $\mathcal{I}^c$ to Bob. Thus, Bob receives quantum state Ψ where $\Psi = \mathrm{Tr}_{\mathcal{I}}\left(\frac{1}{p_B} V_N \left(I_N \otimes |1\rangle\langle 1|_B\right) \tilde{\rho}' \left(I_N \otimes |1\rangle\langle 1|_B\right) V_N^\dagger\right)$ and $p_B = \mathrm{Tr}((I_N \otimes |1\rangle\langle 1|_B)\,\tilde{\rho}')$.
4) To decode, Bob must apply the isometry $U_D = E(f)$ to the received qubits. However, directly applying this isometry is intractable for large block lengths. Thus, Bob instead makes use of the efficient quantum successive cancellation decoding algorithm described in Section IV to decompress Alice's state. Lastly, Bob applies $U_\rho^{\dagger\otimes N}$ to invert the diagonalization operation Alice applied, thus obtaining an approximation of Alice's initial state.

Whereas Schumacher compression, as it was initially proposed, involves projecting Alice's state onto the subspace of δ-typical strings, in the new protocol, Alice projects onto the subspace of errors which are correctable with respect to a polar code. In the next section, we will discuss how Bob can utilize efficient quantum successive cancellation decoding to realize the required isometry in practice.

IV. Efficient Implementation

Belief propagation (BP) is the name used for a class of message-passing algorithms that provide low-complexity decoding for the codes represented by factor graphs [20]. Such codes include low-density parity check (LDPC) [21] and polar [8] codes. While some versions appeared earlier, BP was named by Pearl in 1982 [22] and was later shown to be efficient for decoding codes [23]–[25]. Recently, BP has been generalized via belief propagation with quantum messages (BPQM) for pure-state CQ channels [11]–[14] and subsequently for general binary symmetric CQ (BSCQ) channels [15]–[17].

In this paper, we exploit the factor graph structure of the polar code to recover the compressed quantum state using a BPQM-type algorithm. In our method, the decoder receives frozen qubits constituting the compressed quantum state which

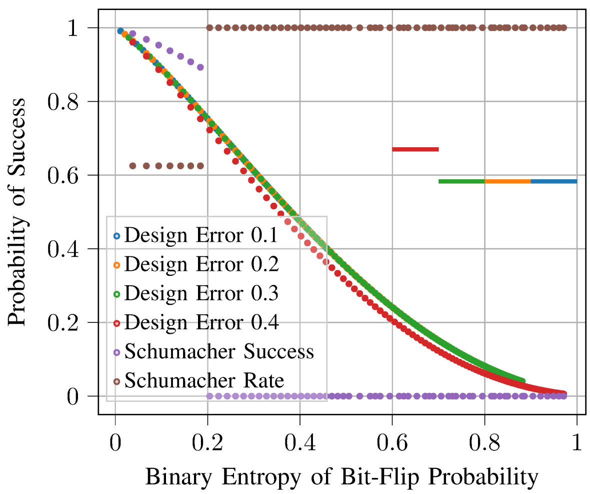

Fig. 1: Probability of success as a function of binary entropy bit-flip probability for blocklength 16. Horizontal lines indicate compression rates.

are used to recover information qubits via successive cancellation decoding of a polar code [8]. In classical BP for a polar code, while decoding a noisy codeword the decoder utilizes channel error probabilities as inputs. It combines these messages across the factor graph, employing successive cancellation decoding to determine the error pattern. Similarly, BP can be used for compression where we recover the complete binary sequence/codeword from the frozen bits. In this scenario, the frozen bits are used as a syndrome i.e. a compressed sequence and instead of channel error probabilities, the decoder uses source probabilities as input.

The syndrome-based algorithm can be lifted to the quantum domain by considering all possible messages sent back from frozen qubits in superposition when frozen qubits are used as a syndrome. This allows the combining of messages classically while accounting for the indeterminate nature of quantum information. This observation plays a key role in our lifted BP algorithm. While the classical messages, when passed through the factor graph, become conditional on nature depending on the number of frozen qubits and are written as a list of probabilities, the quantum part of the algorithm involves designing appropriate unitary based on these conditional classical messages.

This idea extends Arikan's method of source polarization [6] to give a coherent quantum decompressor i.e. source decoder. In [26], we also show how the same idea can be used to realize the coherent quantum compressor i.e. source encoder. Initially, the information qubits are prepared as ancilla qubits in state $|0\rangle$. To realize the successive cancellation for decoding bit u_i, we construct a factor graph with root node u_i and decoder output for past bits as $\hat{u}_1^{i-1}$ from the decoding factor graph of the polar code. The factor graph takes message probabilities associated with the distribution of the source qubits after diagonalization as inputs. The messages are passed through the factor graph through check-node ($\boxast$) and bit-node ($\circledast$) combining rules. In the probability domain, the check-node and bit-node combining rules of messages p_1 and p_2 are realized as

$$\begin{aligned} p_1 \boxast p_2 &= p_1(1-p_2)+p_2(1-p_1) \\ p_1 \circledast p_2 &= \frac{p_1 p_2}{p_1 p_2+(1-p_1)(1-p_2)}. \end{aligned}$$

Since the frozen qubits are in a superposition of $|0\rangle$, $|1\rangle$ qubit states, while decoding the root nodes corresponding to the frozen qubits, a conditional message is sent back to continue the successive cancellation decoding. To decode root nodes associated with information qubits, we construct an appropriate unitary based on conditional messages sent back from the frozen qubits and apply the conditional unitary to decide whether or not to flip the information qubit (which is set as an ancilla in state $|0\rangle$).

Our method can be thought of as the "quantization" of a classical SC decoder and polar source coding [6], [7] methods; i.e. adopting the SC decoder to maintain the superposition of the compressed quantum data. The primary drawback of this algorithm is that decoding each information qubit depends on all the preceding frozen qubits. So, the required conditioning grows linearly with the number of frozen qubits that precede each information qubit. It may be possible to reduce the complexity of conditioning by efficiently computing and storing the required condition in a smaller number of ancilla qubits. While we do not provide an exact complexity comparison with existing literature [4], we believe improvements could allow the order $N\log(N)$ complexity of polar codes. For a complete description, see [26].

V. Numerical Results

In Figure 1, we plot the probability of successful quantum state compression for length 16 as a function of bit-flip probability p for various code designs via Monte Carlo simulation. For blocklengths 8 and 16 (see [26]), our protocol performs as we would expect: the probability of successful compression strictly decreases as entropy increases and the compression rates of codes designed via Monte Carlo simulation strictly increase as design error probability increases. For larger blocklengths, we expect this protocol to achieve higher accuracy and lower compression rates as source entropy decreases.

VI. Discussion

In this paper, we consider the problem of quantum state compression and propose an efficient solution using polar codes. We provide an efficient quantum successive cancellation decoding algorithm based on the factor graph of polar codes. This provides low-complexity compression and decompression protocols that allow Alice to reliably transmit a multi-qubit quantum state to Bob at a rate approaching the source entropy. Since our algorithm is based on lifting a classical message-passing decoder to operate on a quantum superposition, the analysis only depends on the classical performance of the polar code. Thus, we can achieve the Schumacher compression limit $S(\rho)$ using this protocol. We have also implemented our algorithm for arbitrary length $N = 2^\nu$ in Python. The code can be found on GitHub [27].

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

[2] S. L. Braunstein, C. A. Fuchs, D. Gottesman, and H.-K. Lo, "A quantum analog of huffman coding," *IEEE Transactions on information theory*, vol. 46, no. 4, pp. 1644–1649, 2000.

[3] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, no. 4, pp. 2738–2747, 1995. DOI: 10.1103/physreva.51.2738.

[4] R. Cleve and D. P. DiVincenzo, "Schumacher's quantum data compression as a quantum computation," *Physical Review A*, vol. 54, no. 4, p. 2636, 1996.

[5] T. Ancheta, "Syndrome-source-coding and its universal generalization," *IEEE Transactions on Information Theory*, vol. 22, no. 4, pp. 432–436, 1976. DOI: 10.1109/tit.1976.1055578.

[6] E. Arikan, "Source polarization," in *2010 IEEE International Symposium on Information Theory*, IEEE, 2010, pp. 899–903.

[7] H. S. Cronie and S. B. Korada, "Lossless source coding with polar codes," *2010 IEEE International Symposium on Information Theory*, 2010. DOI: 10.1109/isit.2010.5513561.

[8] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009. DOI: 10.1109/tit.2009.2021379.

[9] M. M. Wilde, "Chapter 17," in *Quantum Information theory*. Cambridge University Press, 2013, pp. 417–428.

[10] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1175–1187, 2013. DOI: 10.1109/tit.2012.2218792.

[11] J. M. Renes, "Belief propagation decoding of quantum channels by passing quantum messages," *New Journal of Physics*, vol. 19, no. 7, p. 072001, 2017. [Online]. Available: http://arxiv.org/abs/1607.04833.

[12] N. Rengaswamy, K. P. Seshadreesan, S. Guha, and H. D. Pfister, "Belief propagation with quantum messages for quantum-enhanced classical communications," *npj Quantum Inf.*, vol. 7, no. 1, p. 97, Jun. 2021. DOI: 10.1038/s41534-021-00422-1.

[13] C. Piveteau and J. M. Renes, "Quantum message-passing algorithm for optimal and efficient decoding," *Quantum*, vol. 6, p. 784, 2022.

[14] H. D. Pfister, C. Piveteau, J. M. Renes, and N. Rengaswamy, "Belief propagation for classical and quantum systems: Overview and recent results," *IEEE BITS the Information Theory Magazine*, 2023.

[15] S. Brandsen, A. Mandal, and H. D. Pfister, "Belief propagation with quantum messages for symmetric classical-quantum channels," in *2022 IEEE Information Theory Workshop (ITW)*, IEEE, 2022, pp. 494–499.

[16] A. Mandal, S. Brandsen, and H. D. Pfister, "Belief-propagation with quantum messages for polar codes on classical-quantum channels," in *2023 IEEE International Symposium on Information Theory (ISIT)*, IEEE, 2023, pp. 613–618.

[17] A. Mandal, S. Brandsen, and H. D. Pfister, *Polar codes for cq channels: Decoding via belief-propagation with quantum messages*, 2024. arXiv: 2401.07167.

[18] L. J. H. van, "Linear codes," in *Coding theory*. Springer, 1971, pp. 15–41.

[19] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," in *2012 IEEE International Symposium on Information Theory Proceedings*, IEEE, 2012, pp. 334–338.

[20] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.

[21] R. Gallager, "Low-density parity-check codes," *IRE Transactions on information theory*, vol. 8, no. 1, pp. 21–28, 1962.

[22] J. Pearl, "Reverend bayes on inference engines: A distributed hierarchical approach," in *Probabilistic and Causal Inference: The Works of Judea Pearl*, 2022, pp. 129–138.

[23] R. J. McEliece, D. J. C. MacKay, and J.-F. Cheng, "Turbo decoding as an instance of pearl's" belief propagation" algorithm," *IEEE Journal on selected areas in communications*, vol. 16, no. 2, pp. 140–152, 1998.

[24] F. R. Kschischang and B. J. Frey, "Iterative decoding of compound codes by probability propagation in graphical models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 2, pp. 219–230, 1998.

[25] M. C. Davey and D. J. MacKay, "Low density parity check codes over gf (q)," in *1998 Information Theory Workshop (Cat. No. 98EX131)*, IEEE, 1998, pp. 70–71.

[26] J. Weinberg, A. Mandal, and H. D. Pfister, "Quantum state compression with polar codes," *arXiv preprint arXiv:2402.18684*, 2024.

[27] J. Weinberg, A. Mandal, and H. D. Pfister, *Code Repository for Quantum State Compression with Polar Codes*, https://github.com/Aviemathelec1995/QSCpolar, 2024.