Fault-tolerant preparation of quantum polar codes encoding one logical qubit

Ashutosh Goswami [ORCID],[1,*] Mehdi Mhalla,[2,†] and Valentin Savin[1,‡]

[1]*Université Grenoble Alpes, CEA-Léti, F-38054 Grenoble, France*
[2]*Université Grenoble Alpes, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France*

This paper explores an approach to fault-tolerant quantum computing (FTQC), relying on quantum polar codes. We consider quantum polar codes of Calderbank-Shor-Steane type, encoding one logical qubit, which we refer to as $\mathcal{Q}_1$ codes. First, we show that a subfamily of $\mathcal{Q}_1$ codes is equivalent to the well-known family of Shor codes. Moreover, we show that $\mathcal{Q}_1$ codes significantly outperform Shor codes, of the same length and minimum distance. Second, we consider the fault-tolerant preparation of $\mathcal{Q}_1$ code states. We give a recursive procedure to prepare a $\mathcal{Q}_1$ code state, based on two-qubit Pauli measurements only. The procedure is not by itself fault-tolerant; however, the measurement operations therein provide redundant classical bits, which can be advantageously used for error detection. Fault tolerance is then achieved by combining the proposed recursive procedure with an error detection method. Finally, we consider the fault-tolerant error correction of $\mathcal{Q}_1$ codes. We use Steane error correction, which incorporates the proposed fault-tolerant code state preparation procedure. We provide numerical estimates of the logical error rates for $\mathcal{Q}_1$ and Shor codes of length 16 and 64 qubits, assuming a circuit-level depolarizing noise model. Remarkably, the $\mathcal{Q}_1$ code of length 64 qubits achieves a logical error rate very close to 10^{-6} for the physical error rate $p = 10^{-3}$, therefore demonstrating the potential of the proposed polar-codes-based approach to FTQC.

I. INTRODUCTION

Large-scale quantum computers are expected to use quantum error correcting (QEC) codes to provide resilience against noise [1]. A QEC code encodes one or more logical qubits into many noisy physical qubits, so that the logical qubits are more robust against noise than the physical qubits. However, a QEC code alone does not provide the ability to do fault-tolerant quantum computation (FTQC). To avoid the uncontrolled propagation of errors, it must be complemented with several *fault-tolerant* procedures [2], aimed at (1) preparing logical code states, (2) operating on the logical subspace, and (3) performing error correction.

In this paper, we explore an approach to FTQC, relying on quantum polar codes. Introduced first in 2009 for classical systems [3], and then generalized to the quantum case [4–7], polar codes arguably represent one of the most important advances of the past decade in the coding theory. In the classical setting, polar codes are the first family of explicit codes that provably achieve the capacity of any symmetric, binary-input, discrete, memoryless classical channel, and come equipped with an efficient decoding algorithm, known as *successive cancellation* (SC), whose complexity scales log-linearly with the code length [3]. In the quantum setting, they achieve the coherent information (one-shot capacity) of any quantum channel [4,6,7], and further, the efficient classical polar

decoder can be adapted for Pauli channels by considering a syndrome decoding approach [4,7]. Quantum polar codes are thus of both theoretical and practical importance, due to their theoretically proven optimal error correction capacity and their practical, low-complexity successive-cancellation-based decoding.

It is important to note that a fast decoder is key to performing fault-tolerant error correction. Indeed, the QEC decoder needs to be fast enough to fight against the qubit decoherence, energy efficient to meet possibly stringent power-consumption requirements, and highly scalable to meet the needs of fault tolerance [8]. Moreover, as noticed in [8], the decoding must be faster than the syndrome extraction rate, since otherwise the latency overhead becomes exponential in the number of non-Clifford gates, hindering any quantum advantage. Achieving all these constraints is extremely challenging, and might not be possible by existing solutions.

Hence, it is worth investigating polar codes in the context of FTQC, where they may potentially provide a viable alternative to present solutions based on topological [9–11], or more generally quantum low-density parity-check (LDPC) codes [12–15].

Yet, despite their excellent error correction properties, polar codes have been hardly explored for quantum computing, except the work in [16] on magic state distillation. Here we focus on two closely related ingredients of FTQC, namely, fault-tolerant code state preparation and fault-tolerant error correction. Note that, unlike quantum LDPC codes, quantum polar codes have high-weight stabilizer generators, which prevent fault-tolerant state preparation and error correction from

being implemented by repeated syndrome measurements. Indeed, quantum LDPC code states can be prepared and error corrected by repeated syndrome measurements, where stabilizer generators are measured by using the standard phase kickback trick [2]. Errors are detected by the difference between syndromes, and since the syndrome values can also contain errors, several measurement rounds have to be decoded simultaneously to achieve fault tolerance [17]. Since this approach is no longer fault-tolerant for codes with high-weight stabilizer generators, alternative solutions have to be devised for quantum polar codes. The main contributions of this paper are as follows.

We consider quantum polar codes of Calderbank-Shor-Steane (CSS) type that encode one logical qubit, which we refer to as $\mathcal{Q}_1$ codes. We show that $\mathcal{Q}_1$ codes are a natural generalization of the well-known family of Shor codes, providing improved error correction performance.

We then consider the fault-tolerant preparation of $\mathcal{Q}_1$ code states. By taking advantage of the quantum polar code structure, we propose a procedure to prepare $\mathcal{Q}_1$ code states, by recursively performing Pauli $Z \otimes Z$ or Pauli $X \otimes X$ measurements. This procedure is not by itself fault-tolerant; however, the measurement operations therein provide redundant classical bits, which can be advantageously used for error detection. Hence, to achieve fault tolerance, the proposed procedure is complemented by an error detection method [18].

Indeed, unlike the LDPC case, where the syndrome extraction can be repeated to deal with errors in generator measurements, in our case, the measurements cannot be repeated, as they may correspond to anticommuting Pauli operators. Therefore, to ensure the fault tolerance, we have introduced an error detection gadget, which takes advantage of the redundancy in the measurement outcome.

Finally, we consider the fault-tolerant error correction of $\mathcal{Q}_1$ codes, using Steane error correction [19,20]. We provide numerical estimates of the logical error rate (LER), assuming a circuit-level depolarizing noise model, for $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes of length $N = 16$ and $N = 64$. Remarkably, the $\mathcal{Q}_1$ code of length 64 qubits achieves an LER very close to 10^{-6} for the physical error rate $p = 10^{-3}$, therefore, demonstrating the potential of the proposed polar-codes-based approach to FTQC.

II. CSS QUANTUM POLAR CODES

We refer to Appendix A and Appendix B for the relevant background on classical and quantum polar codes. Here we introduce the notation and summarize the definitions needed to understand the main results of the paper.

The quantum polar transform Q_N, where $N = 2^n$, with $n > 0$, is the unitary operation on N qubits that operates in the computational basis as the classical polar transform P_N. Precisely, for any $\boldsymbol{u} = (u_1, \dots, u_N) \in \{0, 1\}^N$, we define $Q_N |\boldsymbol{u}\rangle = |P_N \boldsymbol{u}\rangle$, where $P_N = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{\otimes n}$. Hence, Q_N can be realized by recursively applying the quantum CNOT gate, transversely, on subblocks of 2^k qubits, for $k = 0, \dots, n-1$ (see Fig. 1).

Let $\mathcal{S} = \{1, \dots, N\}$ denote an N-qubit quantum system. For a CSS quantum polar code [4], the system $\mathcal{S}$ is partitioned
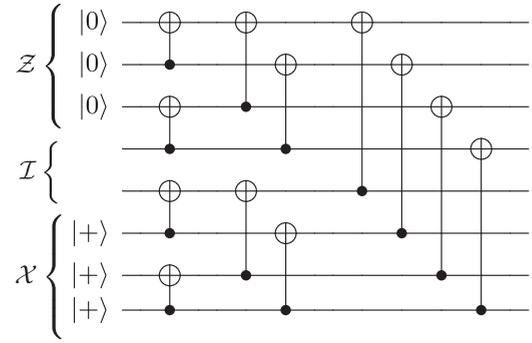
FIG. 1. The quantum polar code, with $N = 2^3$, frozen sets $\mathcal{Z} = \{1, 2, 3\}$, $\mathcal{X} = \{6, 7, 8\}$ (chosen only for the simplicity of illustration), and frozen states $|\boldsymbol{u}\rangle_{\mathcal{Z}} = |0, 0, 0\rangle$, and $|\bar{\boldsymbol{v}}\rangle_{\mathcal{X}} = |+, +, +\rangle$.

into $\mathcal{S} = \mathcal{Z} \cup \mathcal{I} \cup \mathcal{X}$, and the input quantum state of the polar transform is taken as follows.

For $\mathcal{Z} \subseteq \mathcal{S}$, the quantum state is frozen to a known Pauli Z basis state $|\boldsymbol{u}\rangle_{\mathcal{Z}}$, where $\boldsymbol{u} := (u_1, \dots, u_n) \in \{0, 1\}^{|\mathcal{Z}|}$. For $\mathcal{X} \subseteq \mathcal{S}$, with $\mathcal{Z} \cap \mathcal{X} = \emptyset$, it is frozen to a known Pauli X basis state $|\bar{\boldsymbol{v}}\rangle_{\mathcal{X}}$, where $\boldsymbol{v} \in \{0, 1\}^{|\mathcal{X}|}$ and we use the notation $|\bar{0}\rangle := |+\rangle$, and $|\bar{1}\rangle := |-\rangle$. The remaining subset $\mathcal{I} := \mathcal{S} \setminus (\mathcal{X} \cup \mathcal{Z})$ is used to encode quantum information $|\phi\rangle_{\mathcal{I}}$.

Therefore, the logical code state, denoted by $|\widetilde{\phi}\rangle_{\mathcal{S}}$, is given by $|\widetilde{\phi}\rangle_{\mathcal{S}} = Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |\phi\rangle_{\mathcal{I}} \otimes |\bar{\boldsymbol{v}}\rangle_{\mathcal{X}})$.

III. $\mathcal{Q}_1$ CODES: QUANTUM POLAR CODES WITH ONE LOGICAL QUBIT

As $\mathcal{Q}_1$ codes encode only one qubit, the information set $\mathcal{I} = \{i\}$, for some $i \in \mathcal{S} = \{1, \dots, N\}$. Given the index i, the frozen sets $\mathcal{Z}$ consists of the set of indices preceding i, i.e., $\mathcal{Z} := \{1, \dots, i-1\}$, and the frozen set $\mathcal{X}$ consists of the set of indices succeeding i, i.e., $\mathcal{X} := \{i+1, \dots, N\}$.

The choice of the frozen sets $\mathcal{Z}$ and $\mathcal{X}$, given the information qubit position i, is simply explained by the sequential nature of the SC decoding, and the fact that only errors on the information position i need to be decoded. To correct X errors, virtual channels [21] are decoded in order, from 1 to N. Freezing a virtual channel $j > i$ in Z basis would be of no help in decoding the virtual channel i, while freezing it in X basis amounts to ignoring X errors that happen on it. A similar observation holds for Z errors, by noticing that in this case virtual channels are decoded in reversed (decreasing) order, from N to 1 (see also Appendix B 2, Fig. 6).

In case the information position is a power of two, i.e., $i = 2^k$, $0 \leqslant k \leqslant n$, the corresponding $\mathcal{Q}_1$ code is a Shor code [22,23]. This follows from Theorem 1 below, which is proven in Appendix C 1. We refer to these codes as *Shor-$\mathcal{Q}_1$ codes*, or simply Shor codes, when no confusion is possible.

Theorem 1. For a given $i = 2^k$, $0 \leqslant k \leqslant n$, the logical states $|\widetilde{0}\rangle_{\mathcal{S}}$ and $|\widetilde{1}\rangle_{\mathcal{S}}$ of the $\mathcal{Q}_1(N, i)$ code are as follows (up to a normalization factor),

$$|\widetilde{0}\rangle_{\mathcal{S}} = \otimes_{r=1}^{2^k} \left(\otimes_{c=1}^{2^{n-k}} |+\rangle_{r,c} + \otimes_{c=1}^{2^{n-k}} |-\rangle_{r,c} \right), \tag{1}$$

$$|\widetilde{1}\rangle_{\mathcal{S}} = \otimes_{r=1}^{2^k} \left(\otimes_{c=1}^{2^{n-k}} |+\rangle_{r,c} - \otimes_{c=1}^{2^{n-k}} |-\rangle_{r,c} \right), \tag{2}$$
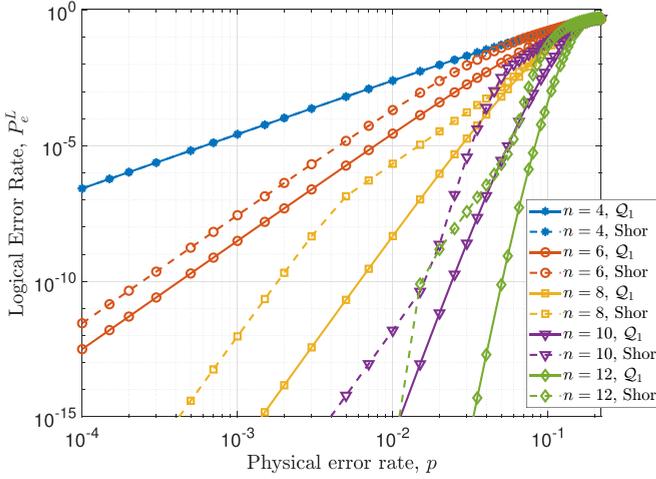
FIG. 2. LER of $\mathcal{Q}_1$ and Shor codes, for the depolarizing channel.

where r and c are row and column indexes, with $\mathcal{S}$ being reshaped as a $2^k \times 2^{n-k}$ matrix of qubits.

The *construction* of a $\mathcal{Q}_1$ code refers to the choice of the information position i, which determines how well the code protects the encoded quantum information. Hence, the position $i \in \mathcal{S}$ should be chosen in a way to optimize the LER performance, depending on the specific noisy quantum channel. For the subfamily of Shor-$\mathcal{Q}_1$ codes, the choice is restricted to positions $i = 2^k, 0 \leqslant k \leqslant n$. (We refer to Appendix B 2 for the construction of CSS quantum polar codes, and to Appendix C 2 for more details on the construction of $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes.)

For depolarizing quantum channels, we use the density evolution technique [3,24] to numerically estimate the LER of $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes. The numerical results are shown in Fig. 2 for both $\mathcal{Q}_1$ and Shor codes, for even recursion levels $n = 4$ to 12, where the corresponding best index i is given in Table II (discussed in Appendix C). It can be observed that the $\mathcal{Q}_1$ code in general outperforms the Shor code, for a given n. From the corresponding values of i given in Table II, one may further note that the $\mathcal{Q}_1$ and Shor codes have the same quantum minimum distance, for a given n. The superior performance of $\mathcal{Q}_1$ codes owes to the SC decoding, which is able to decode beyond the minimum distance of the code, by effectively exploiting the channel polarization property of polar codes.

For the odd recursion levels, our numerical results indicate performance gains, depending on n and the physical error rate value. (Further numerical results for the depolarizing and the quantum erasure channels, as well as the details of the numerical methods, are provided in Appendix C 3.)

IV. MEASUREMENT-BASED PREPARATION OF $\mathcal{Q}_1$ CODE STATES

The conventional encoding of quantum polar codes in Fig. 1 is not fault-tolerant, as errors propagate through the CNOT gates. Further, measuring the stabilizer generators using the standard "phase kickback trick" [2], similar to the case of quantum LDPC codes [13], is also not fault-tolerant, due to the high weights of generators.

Hence, we propose a procedure to prepare $\mathcal{Q}_1$ code states, based on two-qubit Pauli measurements only. We describe our procedure in two steps. First, we assume that all the operations are error-free, and show that the proposed procedure does indeed prepare a $\mathcal{Q}_1$ code state. Then we consider our procedure under the effect of errors (i.e., noisy gates and measurements) and show that it can be made fault-tolerant by incorporating an error detection gadget, exploiting the redundancy in the measurement outcomes.

We consider the preparation of logical $|0\rangle$ and $|+\rangle$ states, for which all the input qubits are frozen in either Z or X basis. Consequently, we consider the preparation of general $\mathcal{Q}_1$ code states, with frozen sets $\mathcal{Z} = \{1, \ldots, i\}$ and $\mathcal{X} = \{i+1, \ldots, N\}$, for some arbitrary $1 \leqslant i \leqslant N$, where $N = 2^n$, $n \geqslant 1$. Further, since our preparation procedure is recursive, to clearly indicate the length of the prepared $\mathcal{Q}_1$ state, we will use the notation $i(n) := i$, $\mathcal{Z}(n) := \mathcal{Z}$, and $\mathcal{X}(n) := \mathcal{X}$. Therefore, we want to prepare the following N-qubit $\mathcal{Q}_1$ state on the system $\mathcal{S} = \{1, \ldots, N\}$,

$$|q_N\rangle_{\mathcal{S}} := Q_N(|\boldsymbol{u}, \overline{\boldsymbol{v}}\rangle_{\mathcal{S}}) = Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}(n)} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}(n)}), \quad (3)$$

where $\boldsymbol{u} \in \{0, 1\}^{i(n)}$ and $\boldsymbol{v} \in \{0, 1\}^{N-i(n)}$. When no confusion is possible, we may simply write $|q_N\rangle$ instead of $|q_N\rangle_{\mathcal{S}}$. Here we consider $\mathcal{Q}_1$ states defined by the same value of $i(n)$ as equivalent, regardless of the corresponding frozen values $\boldsymbol{u}, \boldsymbol{v}$. Put differently, equivalent $\mathcal{Q}_1$ states are defined by the same stabilizer generators, up to sign factors.

To prepare $|q_N\rangle_{\mathcal{S}}$ from (3), we will use the following measurement-based procedure.

Procedure 1 (measurement-based Preparation). Given a n-bit sequence $b_1 \cdots b_n \in \{0, 1\}$, our measurement-based procedure on $N = 2^n$ qubit system $\mathcal{S} = \{1, \ldots, N\}$ is as follows.

(1) First, $\mathcal{S}$ is initialized in a Pauli Z basis state $|\boldsymbol{u}\rangle_{\mathcal{S}}$, $\boldsymbol{u} \in \{0, 1\}^N$.

(2) Then two-qubit Pauli measurements are recursively applied for n levels. The recursion is the same as the recursion of the quantum polar transform (see Fig. 1), except the CNOT gate is replaced by either Pauli $X \otimes X$ or $Z \otimes Z$ measurement. Precisely, if $b_k = 0$ (or, $b_k = 1$), we apply Pauli $X \otimes X$ (or, $Z \otimes Z$) measurements at the kth, $k = 1, \ldots, n$ recursion level.

Theorem 2. Consider the $\mathcal{Q}_1$ state $|q_N\rangle_{\mathcal{S}}$ from (3), with $1 \leqslant i(n) \leqslant N$. Let $b_1 \cdots b_n$ be the binary representation of $i(n) - 1$, with b_n being the most significant bit, i.e., $i(n) - 1 = \sum_{k=1}^{n} b_k 2^{k-1}$. Then $|q_N\rangle_{\mathcal{S}}$ can be prepared, using the measurement-based procedure in Procedure 1, corresponding to the n bit sequence $b_1 \cdots b_n$.

The measurement-based preparation for $N = 8, i(n) = 3$ is illustrated in Fig. 3.

We first show in Lemma 1 that given two equivalent $\mathcal{Q}_1$ states of length $K/2$, $K = 2^k$, we can prepare a $\mathcal{Q}_1$ state of length K by performing $Z \otimes Z$ or $X \otimes X$ measurements transversely on them. Further, when we apply Pauli $Z \otimes Z$ measurements, we have $i(k) = i(k-1) + K/2 > K/2$ and when we apply Pauli $X \otimes X$ measurements, we have $i(k) = i(k-1) \leqslant K/2$. The proof of Theorem 2 then simply follows from Lemma 1, by noting that $b_k = 1 \Leftrightarrow i(k) > K/2$ (hence, $b_k = 0 \Leftrightarrow i(k) \leqslant K/2$).
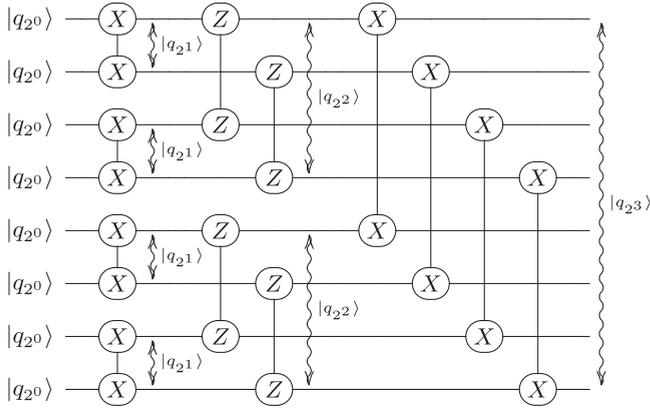
FIG. 3. Measurement-based preparation of $|q_N\rangle_{\mathcal{S}}$ in (3), with $N = 8$, $i(n) = 3$, where slightly flattened circles connected by a vertical wire denote either a $X \otimes X$ or a $Z \otimes Z$ measurement on the corresponding qubits, and $|q_{2^k}\rangle$ are equivalent $\mathcal{Q}_1$ states of length 2^k ($|q_{2^0}\rangle$ is a Pauli Z basis state).

Lemma 1. Consider two equivalent $\mathcal{Q}_1$ states on $K/2$-qubit systems $\mathcal{S}_1 := \{1, \ldots, K/2\}$ and $\mathcal{S}_2 := \{K/2 + 1, \ldots, K\}$ as follows, $|q^1_{\frac{K}{2}}\rangle_{\mathcal{S}_1} := Q_{\frac{K}{2}}|u_1, \overline{v_1}\rangle_{\mathcal{S}_1}$ and $|q^2_{\frac{K}{2}}\rangle_{\mathcal{S}_2} := Q_{\frac{K}{2}}|u_2, \overline{v_2}\rangle_{\mathcal{S}_2}$, where $u_1, u_2 \in \{0, 1\}^{i(k-1)}$ and $v_1, v_2 \in \{0, 1\}^{\frac{K}{2} - i(k-1)}$, with $1 \leqslant i(k-1) \leqslant K/2$. Let $\mathcal{S} := \mathcal{S}_1 \cup \mathcal{S}_2$ be the joint system, then we have the following two cases.

Case 1: If we apply transversal Pauli $Z \otimes Z$ measurements on the corresponding qubits of $\mathcal{S}_1$ and $\mathcal{S}_2$, we get the $K/2$ bit measurement outcome as follows:

$$m = P_{\frac{K}{2}}(u', x) \in \{0, 1\}^{\frac{K}{2}}, \qquad (4)$$

where $u' = u_1 \oplus u_2 \in \{0, 1\}^{i(k-1)}$ and $x \in \{0, 1\}^{\frac{K}{2} - i(k-1)}$ is a random vector, and $P_{\frac{K}{2}}$ is the classical polar transform. After measurements, the state of $\mathcal{S}$ is a $\mathcal{Q}_1$ state, $|q_K\rangle_{\mathcal{S}} = Q_K|(u', x, u_2), \overline{v_1 \oplus v_2}\rangle_{\mathcal{S}}$, with $i(k) = i(k-1) + K/2 > K/2$, and where x is determined from the measurement outcome m in (4) by, $x = P_{\frac{K}{2}}(m)|_{\mathcal{X}(k-1)}$, *i.e.*, the subvector of $P_{\frac{K}{2}}(m) \in \{0, 1\}^{K/2}$ corresponding to indices in the set $\mathcal{X}(k-1)$.

Case 2: If we apply transversal Pauli $X \otimes X$ measurements on the corresponding qubits of $\mathcal{S}_1$ and $\mathcal{S}_2$, we get the $K/2$ bit measurement outcome as follows:

$$m = P^\top_{\frac{K}{2}}(z, v') \in \{0, 1\}^{\frac{K}{2}}, \qquad (5)$$

where $z \in \{0, 1\}^{i(k-1)}$ is a random vector, and $v' = v_1 \oplus v_2 \in \{0, 1\}^{\frac{K}{2} - i(k-1)}$. After measurements, the state on $\mathcal{S}$ is a $\mathcal{Q}_1$ state $|q_K\rangle_{\mathcal{S}} = Q_K|u_1 \oplus u_2, \overline{(v_1, z, v')}\rangle_{\mathcal{S}}$, with $i(k) = i(k-1) \leqslant K/2$ and from (5), $z = P^\top_{\frac{K}{2}}(m)|_{\mathcal{Z}(k-1)}$.

The proof of Lemma 1 is given in Appendix D 1. Cases 1 and 2 from Lemma 1 are also illustrated in Figs. 11 and 12, respectively, in Appendix D 1.

V. FAULT-TOLERANT MEASUREMENT-BASED PROCEDURE

We now consider our measurement-based procedure under the effect of Pauli noise. We assume the standard

implementation of Pauli $Z \otimes Z$ and $X \otimes X$ measurements, where a bare ancilla qubit is initialized in either Pauli Z or Pauli X basis state, then two CNOT gates are applied between data and ancilla qubits, and finally the ancilla qubit is measured in Pauli Z or X basis. Therefore, any two-qubit Pauli measurement decomposes into four basic *components*, namely, one single-qubit initialization, two CNOT gates, and one single-qubit measurement (see Fig. 10 in Appendix D 1).

As the preparation of $|q_N\rangle_{\mathcal{S}}$ consists of N single-qubit initializations, followed by $N/2 \log N$ two-qubit Pauli measurements, the total number of components in the preparation is equal to $N(1 + 2 \log N)$.

We assume that each component fails independently with some probability p, according to a circuit-level Pauli noise model as follows.

A failure in a CNOT gate corresponds to applying the perfect CNOT gate, followed by a two-qubit Pauli error on the output qubits of the CNOT gate. A failure in initialization in Pauli Z (or X) basis corresponds to the perfect initialization, followed by an X (or Z) error on the initialized qubit. A failure in Pauli Z (or X) measurement corresponds to first applying a Pauli X (or Z) error on the qubit to be measured, and then doing the perfect Pauli Z (or X) measurement.

We note that the preparation in Procedure 1 is not fault-tolerant by itself. Due to failures in the components, the measurement outcomes of transversal Pauli $Z \otimes Z$ or $X \otimes X$ measurements are noisy. Precisely, we have $m = P_{\frac{K}{2}}(u', x) \oplus e_X$ instead of (4), and $m = P^\top_{\frac{K}{2}}(z, v') \oplus e_Z$ instead of (5), where $e_X, e_Z \in \{0, 1\}^{K/2}$ are unknown error terms. Recall from Lemma 1 that vectors x and z are determined from m, and they are necessary to know the prepared state $|q_K\rangle_{\mathcal{S}}$ after Pauli $Z \otimes Z$ and $X \otimes X$ measurements, respectively. However, due to unknown error terms, the methods in Lemma 1 may not correctly determine x and z. Accepting a wrong estimate $\hat{x} \neq x$ and $\hat{z} \neq z$ amounts to extra X and Z errors on the respective prepared states, given by the vectors $P_K(0, \hat{x} \oplus x, 0, 0)$, and $P^\top_K(0, 0, \hat{z} \oplus z, 0)$, respectively.

To make the measurement-based preparation fault-tolerant, we consider the following error detection procedure.

Procedure 2 (Measurement-Based Preparation with Error Detection). Consider the preparation of a $\mathcal{Q}_1$ state of length N from Procedure 1. We further incorporate an error detection gadget within each level of recursion, $k = 1, \ldots, n$, consisting of the following two steps.

(1) For all 2^{n-k} instances of prepared $|q_K\rangle$ states at the kth level of recursion, we first determine the syndrome of the error in the measurement outcome m as follows. When Pauli $Z \otimes Z$ measurements are performed (i.e., Case 1 of Lemma 1), we determine the syndrome of the error term e_X in the measurement outcome m as, $P_{\frac{K}{2}}(e_X)|_{\mathcal{Z}(k-1)} = P_{\frac{K}{2}}(m)|_{\mathcal{Z}(k-1)} \oplus u'$. Similarly, when Pauli $X \otimes X$ measurements are performed (i.e., Case 2 of Lemma 1), we determine the syndrome of the error term e_Z as, $P^\top_{\frac{K}{2}}(e_Z)|_{\mathcal{X}(k-1)} = P^\top_{\frac{K}{2}}(m)|_{\mathcal{X}(k-1)} \oplus v'$.

(2) If the syndrome is the zero vector for all the 2^{n-k} instances of $|q_K\rangle$, we determine the value of x or z for all prepared states as in Lemma 1, and proceed to the next level of recursion. Otherwise, we declare a preparation failure.

TABLE I. Comparison of $\mathcal{Q}_1$ codes with surface and color codes.

Codes	Code length (N), Min. distance (d)	Pseudothreshold	Logical error rate		
			$p = 5 \times 10^{-3}$	$p = 10^{-3}$	$p = 10^{-4}$
Surface codes[a] [10, Fig. 4(a)]	$N = 49$, $d = 7$	3.5×10^{-3}	9×10^{-3}	9×10^{-6}	9×10^{-10} (extrapolated)
	$N = 81$, $d = 9$	4.2×10^{-3}	7×10^{-3}	8×10^{-7} (extrapolated)	2×10^{-12} (extrapolated)
Hexagonal color codes[a] [27, Fig. 3]	$N = 61$, $d = 9$	3×10^{-4}	5×10^{-1}	3×10^{-2}	10^{-6}
$\mathcal{Q}_1$ codes	$N = 64$, $d = 8$	10^{-2}	8×10^{-4}	2×10^{-6}	3×10^{-10}

[a]For a fair comparison with $\mathcal{Q}_1$ codes, reported logical error rates for surface and color codes should be multiplied by two, since they account for only one type of errors. Moreover, following [27], the corresponding pseudothresholds are defined as the physical error rate p in which the logical error rate curve $P^L(p)$ intersects with the line $P^L = 2p/3$. We also note that the surface codes in [10] are actually of length $N = 2d^2 - 2d + 1$; the code length reported here $N = d^2$ corresponds to the rotated surface code variant (minimizing the number of qubits for a given minimum distance).

In case Procedure 2 fails, we may restart the procedure from the beginning, by initializing N qubits in a Pauli Z basis state.

The fault tolerance of the successfully prepared state (*i.e.*, when errors are not detected at any recursion level $k = 1$ to n), follows from Theorem 3, which is proven in Appendix D 2.

Theorem 3. Consider the measurement-based preparation with error detection from Procedure 2. Suppose a successful preparation of $|q_N\rangle$, where T_n component failures occur during the preparation. Let $\boldsymbol{e}_X^f, \boldsymbol{e}_Z^f \in \{0, 1\}^N$ be the final Pauli X and Z errors in the noisy prepared state $|q_N'\rangle$, due to the component failures. Then there exist equivalent errors $\boldsymbol{e}_X'^f \equiv \boldsymbol{e}_X^f$ and $\boldsymbol{e}_Z'^f \equiv \boldsymbol{e}_Z^f$, so that $\text{wt}(\boldsymbol{e}_X'^f) \leqslant T_n$ and $\text{wt}(\boldsymbol{e}_X'^f) \leqslant T_n$, where $\text{wt}(\boldsymbol{u})$ denotes the Hamming weight of $\boldsymbol{u}$.

Theorem 3 implies that the weight of X and Z errors on a successfully prepared state remains small given a sufficiently low component failure probability p. In particular, it upper bounds the average weight of the final error by $N(1 + 2\log N)p$. Our numerical simulation suggests that the average error weight is much lower than $N(1 + 2\log N)p$, which is expected as we discard the preparations where errors are detected.

VI. FAULT-TOLERANT ERROR CORRECTION

For fault-tolerant error correction of $\mathcal{Q}_1$ codes, we consider Steane error correction (see Appendix B 3 for the details of Steane error correction applied to CSS quantum polar codes). The $\mathcal{Q}_1$ states, needed in the Steane error correction, are prepared using Procedure 2, assuming a circuit-level depolarizing noise model. Further, as Procedure 2 consists of error detection, we consider $\mathcal{Q}_1$ code states of small lengths $N = 16, 64$.

Let $p_{\text{prep}} = \lim_{R\to\infty} \frac{t}{R}$ be the preparation rate, where t is the number of successful preparations out of R preparation attempts. For a component failure probability $p = 10^{-3}$, our numerical simulation gives $p_{\text{prep}} \approx 0.88$ and $p_{\text{prep}} \approx 0.47$, respectively, for $\mathcal{Q}_1(N = 16, i = 7)$ and $\mathcal{Q}_1(N = 64, i = 23)$ codes (see Fig. 16 in Appendix E 2).

The numerical estimate of the LER for $\mathcal{Q}_1$ and Shor codes of length $N = 16$ and $N = 64$ qubits are given in Fig. 4. The LER has been estimated by Monte Carlo (MC) simulation of the Steane error correction procedure, until a number of f logical errors are reported, where f is taken to be between

50 and 200. We also provide a theoretical upper bound of the LER based on density evolution (DE), providing a trustworthy extrapolation of the LER for smaller values of p. It can be also observed that the pseudothreshold (crossing point between the LER curve and the diagonal line [25,26]) of the $\mathcal{Q}_1(N = 16, i = 7)$ code is $p_{\text{th}} \approx 0.001$, while for the $\mathcal{Q}_1(N = 64, i = 23)$ code, we get $p_{\text{th}} \approx 0.01$.

We have provided more details about the numerical simulation of fault-tolerant error correction in Appendix E.

In Table I we compare the error correction performance of the $\mathcal{Q}_1$ code of length $N = 64$, with previous simulations on surface and color codes of similar lengths from the literature, under circuit-level depolarizing noise [10,27]. We can see that the $\mathcal{Q}_1$ code has a better pseudothreshold value than the considered surface and color codes. In terms of logical error rates, the performance of the $\mathcal{Q}_1$ code is between that of the two surface codes, while being significantly better than that of the color code. This establishes that polar codes are of independent interest and may provide a potential alternative for FTQC.

However, we emphasize that the above comparison must be interpreted carefully. For example, even though we have
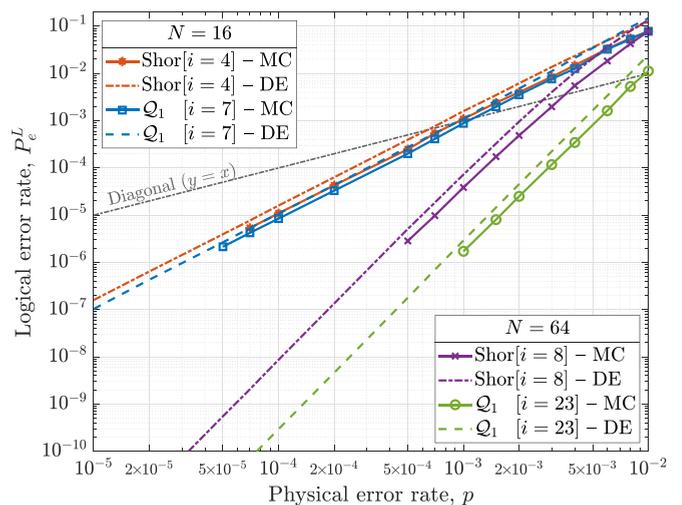
FIG. 4. Monte Carlo (MC) and density-evolution (DE)-based evaluation of the LER, for $\mathcal{Q}_1$ and Shor codes of length $N = 16$ and $N = 64$.

considered similar code lengths, the overhead in terms of qubits may be quite different for each scheme. As we use Steane error correction, we need two code states for each round of correction. Hence, the number of ancilla qubits per round of error correction is twice the code length. Offline preparation of these ancilla qubits may further incur qubit overheads due to error detection, especially at high physical error rates. Surface and color codes are based on error syndrome extraction by measuring stabilizer generators. For surface code, each generator measurement requires one ancilla, hence, requiring approximately the same number of ancilla qubits as the code length. For color codes, the number of ancilla qubits depends, whether the syndrome extraction is done using Shor's extraction technique or using flag qubits [27,28].

Further, time overheads required or the gates applied during each error correction step may also be quite different. For example, $\mathcal{Q}_1$ codes corrects errors after each round of syndrome extraction. However, surface and color codes require d (minimum distance) rounds of syndrome extraction to account for the errors in syndrome, hence incurring an extra time-overhead and requiring more CNOT gates [10,26,27].

VII. DISCUSSION

Polar-encoded quantum computation may be seen as an error correction centric approach to FTQC. It exploits a family of codes that have met with remarkable success, fueled by their excellent error correction performance, under practical, low-complexity decoding. In this paper, we focused on two closely related ingredients of FTQC, namely, fault-tolerant code state preparation and fault-tolerant error correction. We considered polar codes encoding one logical qubit, referred to as $\mathcal{Q}_1$ codes, constituting a case of practical interest to FTQC (they support transversal logical CNOT gate), and which we showed to be a meaningful generalization of the well-known Shor codes. We may also notice that the preparation procedure presented here naturally extends to the case of quantum polar codes encoding several logical qubits, provided they are encoded in consecutive information positions.

Our numerical results suggest that for a circuit-level depolarizing noise model, there exists a pseudothreshold below which the logical error rate is smaller than physical error rate. In particular, the pseudothresholds for $\mathcal{Q}_1$ codes of length $N = 16, 64$ are around 10^{-3} and 10^{-2}, respectively. Moreover, for $N = 64$, the logical error rate is around 10^{-6} for a practically interesting physical error rate 10^{-3}, showing the promise of the proposed fault tolerant error correction.

One can prepare asymptotically large states, by incorporating concatenation [29,30] in our preparation. Precisely, we replace each physical qubit by a logical qubit and then do recursive logical Pauli $Z \otimes Z$ and Pauli $X \otimes X$ measurements. As failure probabilities of the logical measurements is smaller than the physical measurements, we will have a better preparation rate after each level of concatenation. The concatenated codes, however, are not $\mathcal{Q}_1$ codes themselves and would require a greater qubit overhead with respect to the family of $\mathcal{Q}_1$ codes, hence may not be an ideal choice in practice. As explained below, one might avoid using concatenation in practice, with the help of some improvement on our preparation procedure.

First, let us note that the current estimates of the logical error rate needed to run large scale quantum algorithms are around 10^{-15} [10,31], which could be achieved by preparing $\mathcal{Q}_1$ code states of length 256 and 1024, for physical error rates in the range 10^{-3}–10^{-4}. We discuss below two possible improvements, which may allow to prepare larger $\mathcal{Q}_1$ code states, with reasonably high probability, therefore avoiding concatenation in a practical scenario.

The first such improvement would be to consider a factory preparation, where several code states are prepared in parallel. In this scenario, due to the recursive nature of the preparation, one may not have to disregard completely a preparation, every time an error is detected. Therefore, a factory preparation might improve the preparation rate (similar to the magic state distillation case [32,33]).

The second improvement would be to consider error correction in place of error detection. This may work for specific $\mathcal{Q}_1$ codes only, as the classical code defined by the measurement outcomes needs to be a good code, with large enough minimum distance (to ensure good error correction capabilities).

The detailed analysis of the above proposals is left for future works.

Finally, we note that our preparation procedure requires distant interactions between qubits, which may be possible on some quantum technologies only such as ion traps [34,35]. Yet, for quantum systems with local interaction constraints, it may be possible to reduce the number of distant operations required to prepare small $\mathcal{Q}_1$ codes, by arranging the qubits in an appropriate manner (taking advantage of the polar code structure). Distant operations may then be implemented through the use of swap gates [36,37], or by physically moving the qubits around [38–40]. For longer codes, solutions have to be sought that may heavily depend on the specific quantum technology.

APPENDIX A: CLASSICAL POLAR CODES

1. Encoding

The encoding of classical polar codes is done by applying the reversible XOR gate recursively on an N bit input $\boldsymbol{u} = (u_1, \ldots, u_N) \in \{0, 1\}^N$, where $N = 2^n$, with $n > 0$ (see Fig. 5). For a set of positions $\mathcal{F} \subseteq \{1, \ldots, N\}$, the corresponding component $\boldsymbol{u}|_{\mathcal{F}} \in \{0, 1\}^{|\mathcal{F}|}$ of the input vector $\boldsymbol{u}$ is frozen. We may take $\boldsymbol{u}|_{\mathcal{F}}$ to be any vector in $\{0, 1\}^{|\mathcal{F}|}$, but it should be known to both the encoder and the decoder. The set $\mathcal{F}$ is called the *frozen set*. The remaining positions $\mathcal{I} := \{1, \ldots, N\} \setminus \mathcal{F}$ are used to encode information bits. The set $\mathcal{I}$ is called the *information set*.

In the following, we denote by $\mathcal{P}(N, \mathcal{F}, \boldsymbol{u}|_{\mathcal{F}})$, the classical polar code of length N, frozen positions $\mathcal{F}$, and frozen vector $\boldsymbol{u}|_{\mathcal{F}} \in \{0, 1\}^{|\mathcal{F}|}$.

(a) $P_N = P_{N/2} \otimes P_2$

(b) Classical polar code $\mathcal{P}(N = 8, \mathcal{F} = \{1, 2, 3\}, \mathbf{0}|_{\mathcal{F}})$
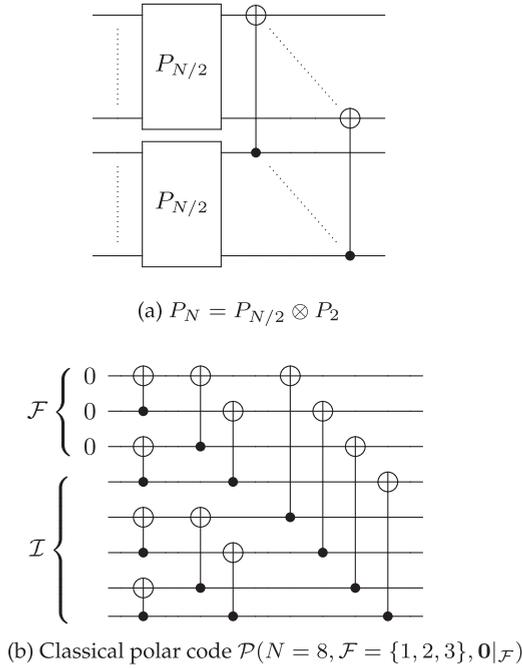
FIG. 5. (a) Polar transform recursion: P_N in terms of $P_{N/2}$. (b) Example of a classical polar code encoding $|\mathcal{I}| = 5$ bits into $N = 2^3$ bits, with frozen set $\mathcal{F} = \{1, 2, 3\}$, and frozen vector $u_{\mathcal{F}} = (0, 0, 0)$. The set $\mathcal{F}$ (thus, $\mathcal{I}$) is chosen only for the purpose and the simplicity of the illustration. In general, it need not consist of consecutive positions.

The action of the $\text{XOR}_{2\to1}$ gate on input $\boldsymbol{u} = (u_1, u_2) \in \{0, 1\}^2$ gives $\boldsymbol{x} = (u_1 \oplus u_2, u_2)$. In matrix form, we may write $\boldsymbol{x} = P_2 \boldsymbol{u}$, where

$$P_2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}. \tag{A1}$$

The classical polar transform, i.e., the recursive application of $\text{XOR}_{2\to1}$ on $N = 2^n$ qubits, is thus given by the matrix

$$P_N = P_2^{\otimes n}. \tag{A2}$$

For any value of the information bits $\boldsymbol{u}_{\mathcal{I}} \in \{0, 1\}^{|\mathcal{I}|}$, $\boldsymbol{x} = P_N(\boldsymbol{u}|_{\mathcal{F}}, \boldsymbol{u}|_{\mathcal{I}}) \in \{0, 1\}^N$ is a codeword of the polar code $\mathcal{P}(N, F, \boldsymbol{u}|_{\mathcal{F}})$. If $\boldsymbol{u}|_{\mathcal{F}}$ is the all zero vector, the polar code $\mathcal{P}(N, \mathcal{F}, \boldsymbol{u}|_{\mathcal{F}})$ is generated by the columns of P_N corresponding to the information set $\mathcal{I}$.

2. Construction

The *construction* of a classical polar code refers to the choice of the information set $\mathcal{I}$ (or, equivalently, the frozen set $\mathcal{F}$). This is done in a *channel-specific way* as follows.

Consider a discrete, memoryless, classical channel $W(y \mid x)$, with binary input $x \in \{0, 1\}$, and output $y \in \mathcal{Y}$. For $\boldsymbol{u} \in \{0, 1\}^N$, let $\boldsymbol{x} = P_N(\boldsymbol{u}) \in \{0, 1\}^N$ (note that here $\mathcal{F}$ and $\mathcal{I}$ need not be defined) and $\boldsymbol{y} \in \mathcal{Y}^N$ be the output corresponding to N uses of the W channel, with inputs $x_1, \ldots, x_N$. For $i = 1, \ldots, N$, let $W^{(i)}(\boldsymbol{y}, \boldsymbol{u}_{1:i-1} \mid u_i)$ denote the so-called *virtual channel*, with input $u_i \in \{0, 1\}$ and output $(\boldsymbol{y}, \boldsymbol{u}_{1:i-1}) \in \mathcal{Y} \times \{0, 1\}^{i-1}$, where $\boldsymbol{u}_{1:i-1} := (u_1, \ldots, u_{i-1})$.

Informally, the *channel polarization theorem* [3] states that, for sufficiently large N, almost all the virtual channels become arbitrarily close to either the noiseless (perfect) channel or to the completely noisy (useless) channel. The *closeness* to the either perfect or useless channel can be expressed in terms of different parameters, such as the mutual information $I(W^{(i)})$, the Bhattacharyya parameter $Z(W^{(i)})$, or the error probability $P_e(W^{(i)})$, which can be computed analytically for some channels (e.g., binary erasure channels), or estimated numerically through *density evolution*, for more general channels [24]. Once one of these parameters is computed for all the virtual channels, they are sorted from the most reliable (closest to the perfect channel) to the least reliable (closest to the useless channel) one.

For a polar code encoding K information bits, the information set $\mathcal{I}$ consists of the indexes corresponding to the K most reliable virtual channels (equivalently, the $N - K$ least reliable virtual channels are frozen). The usefulness of this construction will become apparent in relation to the successive cancellation decoding, discussed in the next section.

3. Decoding

Classical polar codes come equipped with an efficient successive cancellation (SC) decoding algorithm. SC decoding takes advantage of the polar code construction, by estimating inputs $u_1, \ldots, u_N$ sequentially. For $i = 1, \ldots, N$, SC decoding outputs the *maximum a posteriori estimate* $\hat{u}_i$ of u_i, conditional on the observed output $\boldsymbol{y}$ and previous estimates $\hat{\boldsymbol{u}}_{1:i-1} = (\hat{u}_1, \ldots, \hat{u}_{i-1})$. Precisely, we have

$$\hat{u}_i := \begin{cases} u_i, & \text{if } i \in \mathcal{F} \\ \arg\max_{u \in \{0,1\}} W^{(i)}(\boldsymbol{y}, \hat{\boldsymbol{u}}_{1:i-1} \mid u), & \text{if } i \in \mathcal{I} \end{cases}. \tag{A3}$$

If the information set contains indexes of *good virtual channels* (close to the perfect channel), the maximum *a posteriori* estimate $\hat{u}_i$ is equal to the input u_i with high probability. This does not happen for *bad virtual channels* (close to the useless channel), which must then be frozen, so that the corresponding inputs are known to both the encoder and decoder. It is worth noticing that the maximum *a posteriori* decoding of the virtual channels can be performed in an efficient way, by using a message passing algorithm that takes advantage of the recursive structure of the polar code [3]. Overall, the complexity of the SC decoding scales as $O(N \log(N))$.

Finally, we note that polar codes under SC decoding are known to *achieve the channel capacity* [3]. This means that for sufficiently large N, it is possible to choose an information set of size $|\mathcal{I}|$ arbitrary close of $NI(W)$, where $I(W)$ is the channel's mutual information, while ensuring an arbitrary small error probability under SC decoding.

APPENDIX B: QUANTUM POLAR CODES

1. Encoding

The encoding of quantum information for CSS quantum polar codes is briefly given in Sec. II. In this section, we provide more details.

Recall from Sec. II that the quantum polar transform Q_N corresponds to the recursive action of the quantum CNOT gate on an N-qubit quantum state. The quantum CNOT gate induces

(a) $\mathcal{P}(N, \mathcal{Z}, \boldsymbol{u})$

(b) $\mathcal{P}(N, \pi(\mathcal{X}), \pi(\boldsymbol{v}))$
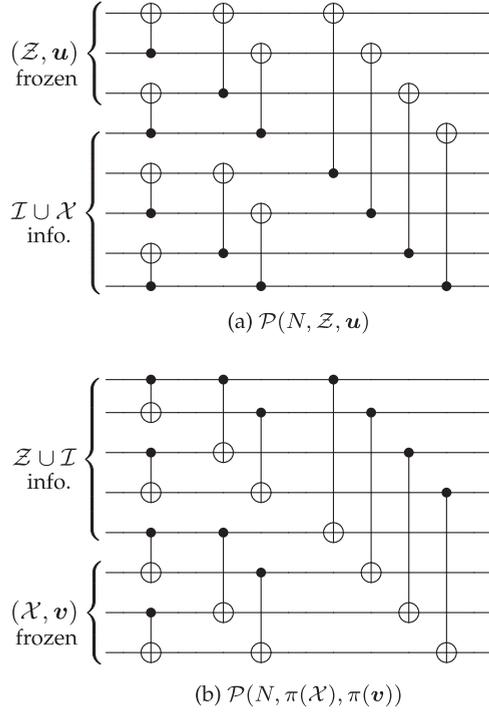
FIG. 6. Classical polar codes in (a) Z basis and (b) X basis, induced by the CSS quantum polar code $\mathcal{Q}(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$. The permutation π in (b) is the reverse order permutation. (Note that in this example the two codes are actually the same.)

the reversible XOR gate in the Pauli Z and Pauli X bases. Precisely, $\text{CNOT}_{2\to1}$ acts as $\text{XOR}_{2\to1}$ in the Pauli Z basis, while it acts as $\text{XOR}_{1\to2}$ in the Pauli X basis. Hence, it follows that Q_N acts as the classical polar transform P_N in the Pauli Z basis, while it acts as the reverse classical polar transform (i.e., with inverted target and control bits) in the Pauli X basis.

It can be seen that the reversed classical polar transform is described by $P_N^\top$, where $P_N^\top$ is the transpose of P_N [4]. Therefore, we have the following, for $\boldsymbol{u} \in \{0, 1\}^N$:

$$Q_N|\boldsymbol{u}\rangle = |P_N\boldsymbol{u}\rangle, \tag{B1}$$

$$Q_N|\overline{\boldsymbol{u}}\rangle = |\overline{P_N^\top\boldsymbol{u}}\rangle. \tag{B2}$$

In the following, we denote by $\mathcal{Q}(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$, the quantum polar code on N qubits, with frozen sets $\mathcal{Z}$ and $\mathcal{X}$, corresponding to the Pauli Z and Pauli X bases, respectively, and with corresponding frozen quantum states $|\boldsymbol{u}\rangle_{\mathcal{Z}}$ and $|\overline{\boldsymbol{v}}\rangle_{\mathcal{X}}$. It induces two classical polar codes, one in Z basis, with frozen set $\mathcal{Z}$, and one in X basis, with frozen set $\mathcal{X}$, where the latter is defined by a reversed polar transform, as illustrated in Fig. 6.

Let π denote the *reverse order permutation* of $\mathcal{S} = \{1, \dots, N\}$, defined by $\pi(i) = N + 1 - i$. Then the classical polar code induced in the Z basis is $\mathcal{P}(N, \mathcal{Z}, \boldsymbol{u})$, while the classical polar code induced in the X basis is $\mathcal{P}(N, \pi(\mathcal{X}), \pi(\boldsymbol{v}))$, where the vector $\pi(\boldsymbol{v})$ is defined by permuting the entries of $\boldsymbol{v}$ according to π, i.e., $\pi(\boldsymbol{v})_i := v_{\pi(i)}$, $\forall i \in \mathcal{X}$.

The X and Z type stabilizer generators of $\mathcal{Q}(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$ are given by the lemma below.

Lemma 2. Let $\mathfrak{e}_i \in \{0, 1\}^N$ be the binary vector, with 0 everywhere except 1 at the ith position. Then the stabilizer group of $\mathcal{Q}(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$ is generated by the following X and Z type operators:

$$(-1)^{v_i} X^{P_N \mathfrak{e}_i}, \quad \forall i \in \mathcal{X}, \tag{B3}$$

$$(-1)^{u_i} Z^{P_N^\top \mathfrak{e}_i}, \quad \forall i \in \mathcal{Z}. \tag{B4}$$

Proof. Note that the input of the polar transform, i.e., the quantum state $|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |\phi\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}}$, is stabilized by the following Pauli operators:

$$(-1)^{v_i} X^{\mathfrak{e}_i}, \quad \forall i \in \mathcal{X}, \tag{B5}$$

$$(-1)^{u_i} Z^{\mathfrak{e}_i}, \quad \forall i \in \mathcal{Z}. \tag{B6}$$

Therefore, the encoded quantum state $|\widetilde{\phi}\rangle_{\mathcal{S}} = Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |\phi\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$ is stabilized by the following Pauli operators:

$$(-1)^{v_i} Q_N X^{\mathfrak{e}_i} Q_N, \quad \forall i \in \mathcal{X}, \tag{B7}$$

$$(-1)^{u_i} Q_N Z^{\mathfrak{e}_i} Q_N, \quad \forall i \in \mathcal{Z}. \tag{B8}$$

The operators in (B7) and (B8) are a generating set of the stabilizer group of $\mathcal{Q}(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$. These generators can be written in terms of classical polar transforms P_N and $P_N^\top$ as follows.

We first consider the case of two qubits, and observe that the sandwiching actions of the CNOT gate on Pauli operators gives, for $\boldsymbol{u} \in \{0, 1\}^2$,

$$\text{CNOT}_{2\to1} X^{\boldsymbol{u}} \text{CNOT}_{2\to1} = X^{P_2\boldsymbol{u}}, \tag{B9}$$

$$\text{CNOT}_{2\to1} Z^{\boldsymbol{u}} \text{CNOT}_{2\to1} = Z^{P_2^\top \boldsymbol{u}}. \tag{B10}$$

Using (B9) and (B10) and (A2), the sandwiching action of Q_N is described by the classical polar transforms P_N and $P_N^\top$, respectively, on X- and Z-type operators. Hence, the stabilizer generators from (B7) and (B8) can be written as given in (B3) and (B4). ∎

Note, from (B3), that the indicator vector of X-type generators are given by the columns of P_N, corresponding to the set $\mathcal{X}$. Further, from (B4), the indicator vectors of the Z-type generators are given by the columns of $P_N^\top$ (i.e., the rows of P_N), corresponding to the set $\mathcal{Z}$.

Similarly to Lemma 2, logical Pauli operators can be determined by passing X and Z operators through the polar transform, as shown in the lemma below.

Lemma 3. Let $\widetilde{X}_i$ and $\widetilde{Z}_i$ be the logical X and Z operators, corresponding to the encoded qubit at the position $i \in \mathcal{I}$. Then

$$\widetilde{X}_i = X^{P_N \mathfrak{e}_i}, \tag{B11}$$

$$\widetilde{Z}_i = Z^{P_N^\top \mathfrak{e}_i}. \tag{B12}$$

2. Construction

The *construction* of a CSS quantum polar code refers to determining the frozen sets $\mathcal{Z}$ and $\mathcal{X}$ (thus, the information set $\mathcal{I}$), which exploits the classical polarization in Z and X bases, respectively [4]. We shall assume a Pauli channel $\mathcal{W}$, with qubit input, given by

$$\mathcal{W}(\rho) = p_I \rho + p_X X\rho X + p_Y Y\rho Y + p_Z Z\rho Z, \tag{B13}$$

where ρ denotes the density matrix of the qubit (mixed) state, and $p_I, p_X, p_Y, p_Z \in [0, 1]$ are probability values, summing to 1.

In Z basis, only X errors matter. Thus, the Z-basis-induced channel, denoted W_Z, captures the effect of X-type errors on the quantum state and is given by

$$W_Z(|u\rangle\langle u|) = (p_I + p_Z)|u\rangle\langle u| + (p_X + p_Y)X|u\rangle\langle u|X, \quad \text{(B14)}$$

where $u \in \{0, 1\}$. Hence, W_Z is a classical binary symmetric channel (BSC), with error probability $p_X + p_Y$. Similarly, the X-basis-induced channel, denoted W_X, captures the effect of Z-type errors on the quantum state and is given by

$$W_X(|\overline{u}\rangle\langle\overline{u}|) = (p_I + p_X)|\overline{u}\rangle\langle\overline{u}| + (p_Z + p_Y)Z|\overline{u}\rangle\langle\overline{u}|Z, \quad \text{(B15)}$$

where $u \in \{0, 1\}$. Hence, W_X is a classical BSC, with error probability $p_X + p_Y$.

To construct the CSS quantum polar code, we exploit the classical polarization of W_Z and W_X channels (see Sec. 3). Note that this construction *ignores the correlations* between X and Z (we will explain how these correlations can be captured a little later, below). The frozen set $\mathcal{Z}$ is determined by the classical polarization of the W_Z channel, under the classical polar transform P_N, while the frozen set $\mathcal{X}$ is determined by the classical polarization of the W_X, under the reversed classical polar transform $P_N^\top$. The remaining information set $\mathcal{I}$ corresponds to virtual channels that are *good* in both Z and X bases. The frozen set $\mathcal{Z}$ corresponds to virtual channels that are *bad* in Z basis. These channels may be either bad or good in X basis, it does not matter, since we need not decode Z errors on corresponding inputs (such errors correspond to Z-type generators, thus they act trivially on the code space). Similarly, the frozen set $\mathcal{X}$ corresponds to virtual channels that are bad in X basis, and which may be either bad or good in Z basis. Precisely, positions in $\mathcal{X}$ that do not impact the decoding of subsequent positions in $\mathcal{I}$ (if any) may correspond to bad virtual channels in Z basis. For instance, this may be the case for some positions in $\mathcal{X}$ that come after the last position in $\mathcal{I}$, i.e., some $j \in \mathcal{X}$, such that $i < j, \forall i \in \mathcal{I}$ [see also Fig. 6(a)].

To *capture the correlations* between X and Z errors, one of the two channels, e.g., W_X, has to be *extended* [4]. The extended channel, denoted by $W_{X'}$, is thus defined by the conditional probability of a Z error, given the X error. Precisely,

$$
\begin{aligned}
W_{X'}(|\overline{u}\rangle\langle\overline{u}|) &= (p_I + p_Z)|0\rangle\langle 0|_X \\
&\otimes \left(\frac{p_I}{p_I + p_Z}|\overline{u}\rangle\langle\overline{u}| + \frac{p_Z}{p_I + p_Z}Z|\overline{u}\rangle\langle\overline{u}|Z \right) \\
&+ (p_X + p_Y)|1\rangle\langle 1|_X \otimes \left(\frac{p_X}{p_X + p_Y}|\overline{u}\rangle\langle\overline{u}| \right. \\
&\left. + \frac{p_Y}{p_X + p_Y}Z|\overline{u}\rangle\langle\overline{u}|Z \right), \quad \text{(B16)}
\end{aligned}
$$

where $\{|0\rangle_X, |1\rangle_X\}$ is an orthogonal basis of an auxiliary system, indicating whether an X error happened or not. Put differently, $W_{X'}$ is a classical mixture of two BSCs, the first with error probability $p_Z/(p_I + p_Z)$ (when no X error happened), and the second with error probability $p_Y/(p_X + p_Y)$ (when an X error happened).

The construction of the CSS quantum polar code, taking into account the correlations between X and Z errors, is done in the same way as above, while replacing the W_X channel by its extended version $W_{X'}$.

3. Steane error correction

We describe here the Steane error correction procedure [19,20] (see also [2, Sec. 4.4]), applied to CSS quantum polar codes. Throughout this section, we consider an encoded state $|\widetilde{\phi}\rangle_{\mathcal{S}} = Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |\phi\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$ of the quantum polar code $Q(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$, that we want to protect against Pauli errors.

Steane's error correction procedure consists of the following steps:

(1) An ancilla system $\mathcal{S}'$ is prepared in either the logical all-$|+\rangle$ state or the logical all-$|0\rangle$ state of $Q(N, \mathcal{Z}, \mathcal{X}, |\boldsymbol{u}\rangle_{\mathcal{Z}}, |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$. The former state is prepared for X-error correction, while the latter of Z-error correction.

(2) A transverse CNOT gate is applied between $\mathcal{S}$ (original) and $\mathcal{S}'$ (ancilla) systems, in such a way that either the X or the Z errors on $\mathcal{S}$ are copied to $\mathcal{S}'$, while the two systems remain separated.

(3) The ancilla system is measured, outputting a random codeword of a classical polar code (in either Z or X basis), corrupted by the error that has been copied to $\mathcal{S}'$.

(4) A classical SC decoding is applied to determine the error (possibly, the corresponding corrective operation is applied on the $\mathcal{S}$ system).

It is easily seen that steps (2) and (3) are fault-tolerant, as they consist only of transverse gates and single-qubit measurements.

By a slight abuse of language, we shall refer to steps (1)–(3) above as *syndrome extraction* [41]. In case of *ideal syndrome extraction*, steps (1)–(3) are assumed to be error-free, and the error corrected at step (4) is the one preexisting on system $\mathcal{S}$, before the syndrome is extracted. In case of *noisy syndrome extraction*, steps (1)–(3) may generate additional errors on systems $\mathcal{S}$ and $\mathcal{S}'$. We will analyze the impact of these errors, together with providing the details of Steane's error correction applied to either X or Z errors, on the two subsections below.

We will consider an ancilla system $\mathcal{S}' = \{1', \ldots, N'\}$ and subsets $\mathcal{Z}', \mathcal{I}', \mathcal{X}' \subseteq \mathcal{S}'$. They are the counterparts of the subsets $\mathcal{Z}, \mathcal{I}, \mathcal{X} \subseteq \mathcal{S}$, in the sense that $i' \in \mathcal{Z}' \Leftrightarrow i \in \mathcal{Z}$, and similarly for $\mathcal{I}'$ and $\mathcal{X}'$.

a. X-error correction. To extract the syndrome for X errors, the ancilla system $\mathcal{S}' = \mathcal{Z}' \cup \mathcal{I}' \cup \mathcal{X}'$ must be prepared in a logical X basis state. Usually, the ancilla state is taken to be the logical all-$|+\rangle$ state, obtained by encoding the all-$|+\rangle$ state on system $\mathcal{I}'$. Here we consider a slightly more general logical X basis state, as follows:

$$|\widetilde{\overline{\boldsymbol{w}'}}\rangle_{\mathcal{S}'} = Q_N(|\boldsymbol{u}'\rangle_{\mathcal{Z}'} \otimes |\overline{\boldsymbol{w}'}\rangle_{\mathcal{I}'} \otimes |\overline{\boldsymbol{v}'}\rangle_{\mathcal{X}'}), \quad \text{(B17)}$$

where $\boldsymbol{u}', \boldsymbol{w}', \boldsymbol{v}'$ are known. Note that frozen values $\boldsymbol{u}'$ and $\boldsymbol{v}'$ may be different from frozen values $\boldsymbol{u}$ and $\boldsymbol{v}$. The reason we consider the above logical state is that our preparation procedure for logical polar code states is measurement based, for which $\boldsymbol{u}', \boldsymbol{w}', \boldsymbol{v}'$ are determined based on random outcomes of measurements therein.

(a) X-error correction: X errors are copied from the original (top) to the ancilla (bottom) system, which is measured in Z basis.

(b) Z-error correction: Z errors are copied from the original (top) to the ancilla (bottom) system, which is measured in X basis.
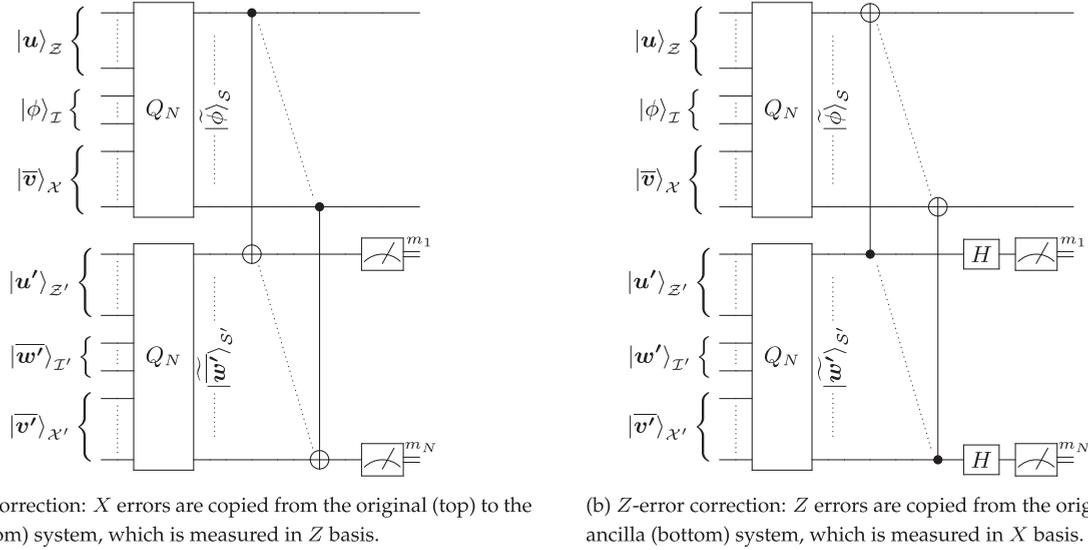
FIG. 7. Steane's error correction procedure.

Steane's X-error syndrome extraction procedure is depicted in Fig. 7(a). After preparing the state $|\widetilde{\overline{w'}}\rangle_{\mathcal{S}'}$ on system $\mathcal{S}'$, the transversal $\text{CNOT}_{\mathcal{S}\to\mathcal{S}'}$ gate is applied on corresponding qubits of systems $\mathcal{S}$ and $\mathcal{S}'$. Then each qubit in the ancilla system $\mathcal{S}'$ is measured in the Pauli Z basis. We denote by $\boldsymbol{m} = (m_1, \ldots, m_N)$ the classical outputs of these measurements.

The following lemma gives the state of the $\mathcal{S}$ system, as well as the measurement result $\boldsymbol{m}$, after the syndrome extraction procedure. We consider errors $\boldsymbol{e}_X$ and $\boldsymbol{e}'_X$ that have happened on systems $\mathcal{S}$ and $\mathcal{S}'$, respectively. We assume that errors $\boldsymbol{e}_X$ and $\boldsymbol{e}'_X$ have happened before the transversal $\text{CNOT}_{\mathcal{S}\to\mathcal{S}'}$ gate is applied, while the transversal $\text{CNOT}_{\mathcal{S}\to\mathcal{S}'}$ gate, as well as the measurement operations, are error-free. We refer to these errors as *preparation errors*. This assumption is made for simplicity only. Indeed, it is not too difficult to see that errors generated on the $\mathcal{S}'$ system, by either the transversal $\text{CNOT}_{\mathcal{S}\to\mathcal{S}'}$ gate or the measurement operations, can actually be incorporated to the error $\boldsymbol{e}'_X$. Errors generated by the transversal $\text{CNOT}_{\mathcal{S}\to\mathcal{S}'}$ gate on the $\mathcal{S}$ system go undetected, but they may be corrected during the next round of error correction.

Lemma 4. Let $\boldsymbol{e}_X$ and $\boldsymbol{e}'_X$ be preparation errors that have happened on systems $\mathcal{S}$ and $\mathcal{S}'$, respectively. Then, after the Steane's X-error syndrome extraction, the state of the system $\mathcal{S}$ is given by

$$X^{\boldsymbol{e}_X}|\widetilde{Z^{\boldsymbol{w}'}\phi}\rangle_{\mathcal{S}} = X^{\boldsymbol{e}_X}Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes Z^{\boldsymbol{w}'}|\phi\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v} \oplus \boldsymbol{v}'}\rangle_{\mathcal{X}}). \quad (\text{B18})$$

Further, the measurement outcome is a noisy codeword of the classical polar code $\mathcal{P}(N, \mathcal{Z}, \boldsymbol{u} \oplus \boldsymbol{u}')$, with frozen set $\mathcal{Z}$ and frozen vector $\boldsymbol{u} \oplus \boldsymbol{u}'$, as follows:

$$\boldsymbol{m} = P_N(\boldsymbol{u} \oplus \boldsymbol{u}', \boldsymbol{a}', \boldsymbol{x}') \oplus \boldsymbol{e}_X \oplus \boldsymbol{e}'_X \in \{0, 1\}^N, \quad (\text{B19})$$

where $\boldsymbol{a}' \in \{0, 1\}^{|\mathcal{I}|}$ and $\boldsymbol{x}' \in \{0, 1\}^{|\mathcal{X}|}$ are random vectors.

Proof. Let $|\phi\rangle_{\mathcal{I}} = \sum_{\boldsymbol{a}\in\{0,1\}^{|\mathcal{I}|}} \phi_{\boldsymbol{a}}|\boldsymbol{a}\rangle_{\mathcal{I}}$. Note also that $|\overline{\boldsymbol{v}}\rangle_{\mathcal{X}} = \sum_{\boldsymbol{x}\in\{0,1\}^{|\mathcal{X}|}} (-1)^{\boldsymbol{v}\cdot\boldsymbol{x}}|\boldsymbol{x}\rangle_{\mathcal{X}}$ (up to a normalization factor, which will be omitted in the sequel). Then the noisy logical

state $X^{\boldsymbol{e}_X}|\widetilde{\phi}\rangle_{\mathcal{S}}$ can be written as

$$X^{\boldsymbol{e}_X}|\widetilde{\phi}\rangle_{\mathcal{S}} = X^{\boldsymbol{e}_X}Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |\phi\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}}) \quad (\text{B20})$$

$$= \sum_{\boldsymbol{a},\boldsymbol{x}} \phi_{\boldsymbol{a}}(-1)^{\boldsymbol{v}\cdot\boldsymbol{x}}|P_N(\boldsymbol{u}, \boldsymbol{a}, \boldsymbol{x}) \oplus \boldsymbol{e}_X\rangle. \quad (\text{B21})$$

Similarly, the noisy ancilla state can be written as

$$X^{\boldsymbol{e}'_X}|\widetilde{\overline{\boldsymbol{w}'}}\rangle_{\mathcal{S}'} = X^{\boldsymbol{e}'_X}Q_N(|\boldsymbol{u}'\rangle_{\mathcal{Z}'} \otimes |\overline{\boldsymbol{w}'}\rangle_{\mathcal{I}'} \otimes |\overline{\boldsymbol{v}'}\rangle_{\mathcal{X}'})$$

$$= \sum_{\boldsymbol{a}',\boldsymbol{x}'} (-1)^{\boldsymbol{w}'\cdot\boldsymbol{a}'+\boldsymbol{v}'\cdot\boldsymbol{x}'}|P_N(\boldsymbol{u}', \boldsymbol{a}', \boldsymbol{x}') \oplus \boldsymbol{e}'_X\rangle. \quad (\text{B22})$$

After the transverse $\text{CNOT}_{\mathcal{S}\to\mathcal{S}'}$ gate is applied, we get the following state on the bipartite $\mathcal{S}\mathcal{S}'$ system:

$$|\theta\rangle_{\mathcal{S}\mathcal{S}'} := \text{CNOT}_{\mathcal{S}\to\mathcal{S}'}(X^{\boldsymbol{e}_X}|\widetilde{\phi}\rangle_{\mathcal{S}} \otimes X^{\boldsymbol{e}'_X}|\widetilde{\overline{\boldsymbol{w}'}}\rangle_{\mathcal{S}'})$$

$$= \sum_{\boldsymbol{a},\boldsymbol{x}} \phi_{\boldsymbol{a}}(-1)^{\boldsymbol{v}\cdot\boldsymbol{x}}|P_N(\boldsymbol{u}, \boldsymbol{a}, \boldsymbol{x}) \oplus \boldsymbol{e}_X\rangle$$

$$\otimes \sum_{\boldsymbol{a}',\boldsymbol{x}'} (-1)^{\boldsymbol{w}'\cdot\boldsymbol{a}'+\boldsymbol{v}'\cdot\boldsymbol{x}'}$$

$$|P_N(\boldsymbol{u} \oplus \boldsymbol{u}', \boldsymbol{a} \oplus \boldsymbol{a}', \boldsymbol{x} \oplus \boldsymbol{x}') \oplus \boldsymbol{e}_X \oplus \boldsymbol{e}'_X\rangle$$

$$= \sum_{\boldsymbol{a},\boldsymbol{x}} \phi_{\boldsymbol{a}}(-1)^{\boldsymbol{w}'\cdot\boldsymbol{a}+(\boldsymbol{v}\oplus\boldsymbol{v}')\cdot\boldsymbol{x}}|P_N(\boldsymbol{u}, \boldsymbol{a}, \boldsymbol{x}) \oplus \boldsymbol{e}_x\rangle$$

$$\otimes \sum_{\boldsymbol{a}',\boldsymbol{x}'} (-1)^{\boldsymbol{w}'\cdot\boldsymbol{a}'+\boldsymbol{v}'\cdot\boldsymbol{x}'}|P_N(\boldsymbol{u} \oplus \boldsymbol{u}', \boldsymbol{a}', \boldsymbol{x}')$$

$$\oplus\boldsymbol{e}_X \oplus \boldsymbol{e}'_X\rangle, \quad (\text{B23})$$

where for the last equality, we use variable changes $\boldsymbol{a}' \leftarrow \boldsymbol{a}' \oplus \boldsymbol{a}$, and $\boldsymbol{x}' \leftarrow \boldsymbol{x}' \oplus \boldsymbol{x}$. It can be seen that the error on the system $\mathcal{S}$ has propagated to the system $\mathcal{S}'$, and $|\theta\rangle_{\mathcal{S}\mathcal{S}'}$ is a product

state that can be rewritten as

$$|\theta\rangle_{\mathcal{S}\mathcal{S}'} = X^{e_X} Q_N(|u\rangle_{\mathcal{Z}} \otimes Z^{w'}|\phi\rangle_{\mathcal{I}} \otimes |\overline{v \oplus v'}\rangle_{\mathcal{X}})$$
$$\otimes X^{e_X \oplus e'_X} Q_N(|u' \oplus u\rangle_{\mathcal{Z}'} \otimes |\overline{w'}\rangle_{\mathcal{I}'} \otimes |\overline{v'}\rangle_{\mathcal{X}'}).$$
(B24)

Hence, the partial state of the system $\mathcal{S}$ is the same as in (B18). Further, measuring the qubits of the ancilla system in the Pauli Z basis, we get $m = P_N(u \oplus u', a', x') \oplus e_X \oplus e'_X \in \{0, 1\}^N$, for some random vectors $a' \in \{0, 1\}^{|\mathcal{I}|}$ and $x' \in \{0, 1\}^{|\mathcal{X}|}$.

Two observations are in place here.

First, from (B18), it follows that the frozen vector corresponding to $\mathcal{X} \subset \mathcal{S}$ (original system) has changed to $v \oplus v'$, after the Steane's procedure. Further, the logical Z operator corresponding to $Z^{w'}$ gets applied on $\mathcal{S}$. However, since we know w', we can reverse this logical operation using (B12). Hence, the logical information encoded in $\mathcal{S}$ has not been altered, due to the syndrome extraction.

The second observation concerns the SC decoding, which takes as input the measurement outcome $m = P_N(u \oplus u', a', x') \oplus e_X \oplus e'_X$, and the frozen vector $u \oplus u'$. It produces an estimate of the information vector (a', x'), from which we can produce an estimate of the total error $e_X \oplus e'_X$. The vector a' may be correctly estimated, owning to the fact that it corresponds to good virtual channels. Some of the x' positions may be incorrectly estimated, but this does not matter, as the induced logical error corresponds to an X-type stabilizer operator, acting trivially on the code space.

Hence, assuming the vector a' is decoded correctly, we also get the correct value of the total error $e_X \oplus e'_X$ (up to an X-type stabilizer operator). We then correct the $\mathcal{S}$ system by applying $X^{e_X \oplus e'_X}$, which will leave the error $X^{e'_X}$ (original error on $\mathcal{S}'$) on $\mathcal{S}$ after correction. This leftover error, may hopefully be corrected in the next round of correction, where we may similarly add another error from the ancilla system. However, note that the advantage of error correction is that it does not allow errors to accumulate and the only left error on the encoded state is due to the last round of error correction (which may be corrected, when the encoded logical state is eventually measured). Hence, we may stabilize logical qubits against noise, by doing error correction repeatedly.

It is worth noticing that for topological (or some families of quantum LDPC codes), fault tolerant error correction needs the decoding operation to be applied on a time window, composed of several consecutive syndrome extractions, e.g., [10]. For Steane's fault tolerant error correction, decoding is simply applied on each extracted "syndrome" (recall the "syndrome" in this case is actually a noisy codeword).

b. Z-error correction. The decoding of Z errors can be done similarly to the case of X errors as follows. To extract the syndrome for Z errors [see Fig. 7(b)], one needs an ancilla system $\mathcal{S}'$ prepared in a logical Z basis state,

$$|\widetilde{w'}\rangle_{\mathcal{S}'} = Q_N(|u'\rangle_{\mathcal{Z}'} \otimes |w'\rangle_{\mathcal{I}'} \otimes |\overline{v'}\rangle_{\mathcal{X}'}).$$
(B25)

After preparing the state $|\widetilde{w'}\rangle_{\mathcal{S}'}$ on ancilla system $\mathcal{S}'$, the transversal CNOT$_{\mathcal{S}' \to \mathcal{S}}$ gate is applied on corresponding qubits of systems $\mathcal{S}$ and $\mathcal{S}'$. Then each qubit in the ancilla system $\mathcal{S}'$ is measured in the Pauli X basis. The measurement
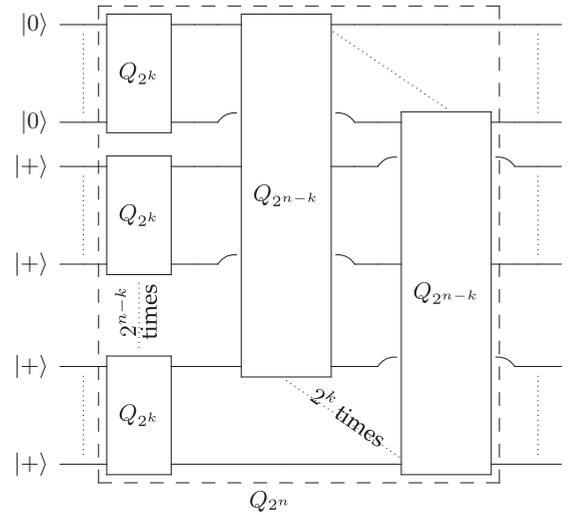
FIG. 8. Quantum polar transform decomposition, using $Q_{2^n} = (I_{2^k} \otimes Q_{2^{n-k}})(Q_{2^k} \otimes I_{2^{n-k}})$. Bent wires go under the blocks they cross. In the case input qubits are prepared as shown on the left, the encoded state is the logical $|0\rangle$ state of a Shor code.

output m is a noisy codeword of the classical polar code $\mathcal{P}(N, \pi(\mathcal{X}), \pi(v))$, induced in X basis [Fig. 6(b)].

Lemma 5. Let e_Z and e'_Z be preparation errors that has happened on systems $\mathcal{S}$ and $\mathcal{S}'$, respectively. Then, after the Steane's Z-error syndrome extraction, the state of the system $\mathcal{S}$ is given by

$$Z^{e_Z}|\widetilde{X^{w'}\phi}\rangle_{\mathcal{S}} = Z^{e_Z} Q_N(|u \oplus u'\rangle_{\mathcal{Z}} \otimes X^{w'}|\phi\rangle_{\mathcal{I}} \otimes |\overline{v}\rangle_{\mathcal{X}}). \quad (B26)$$

Further, the measurement outcome is a noisy codeword of the classical polar code $\mathcal{P}(N, \pi(\mathcal{X}), \pi(v))$, with frozen set $\mathcal{X}$ and frozen vector $\pi(v \oplus v')$, as follows:

$$m = P_N^\top(z', a', v \oplus v') \oplus e_Z \oplus e'_Z, \quad (B27)$$

where $a' \in \{0, 1\}^{|\mathcal{I}|}$ and $x' \in \{0, 1\}^{|\mathcal{X}|}$ are random vectors.

The proof of Lemma 5 is similar to that of Lemma 4, by expanding quantum states of systems $\mathcal{S}$ and $\mathcal{S}'$ in the Pauli X basis. Finally, based on the frozen vector $v \oplus v'$ and the noisy codeword m in (B27), the SC decoder generates an estimate of a', and in turn we can obtain an estimate of the error $e_Z \oplus e'_Z$ (up to a Z-type stabilizer operator).

APPENDIX C: $\mathcal{Q}_1$ CODES: QUANTUM POLAR CODES ENCODING ONE QUBIT

1. Shor $\mathcal{Q}_1$ codes (Proof of Theorem 1)

To prove Theorem 1, we will use the decomposition $Q_N = (I_{2^k} \otimes Q_{2^{n-k}})(Q_{2^k} \otimes I_{2^{n-k}})$, for $0 \leqslant k \leqslant n$. This decomposition is illustrated in Fig. 8, where we have 2^{n-k} parallel Q_{2^k} blocks, followed by 2^k parallel $Q_{2^{n-k}}$ blocks. If one considers the quantum system $\mathcal{S}$ as a vector of N qubits, the decomposition illustrated in Fig. 8 is equivalent to reshaping $\mathcal{S}$ as a $2^k \times 2^{n-k}$ matrix of qubits, with columns filled in by consecutive qubits from the original vector, then applying Q_{2^k} on each column, and $Q_{2^{n-k}}$ on each row.

For the logical state $|\widetilde{0}\rangle_{\mathcal{S}}$, the first $i = 2^k$ inputs of the quantum polar transform Q_N are equal to $|0\rangle$, while the remaining
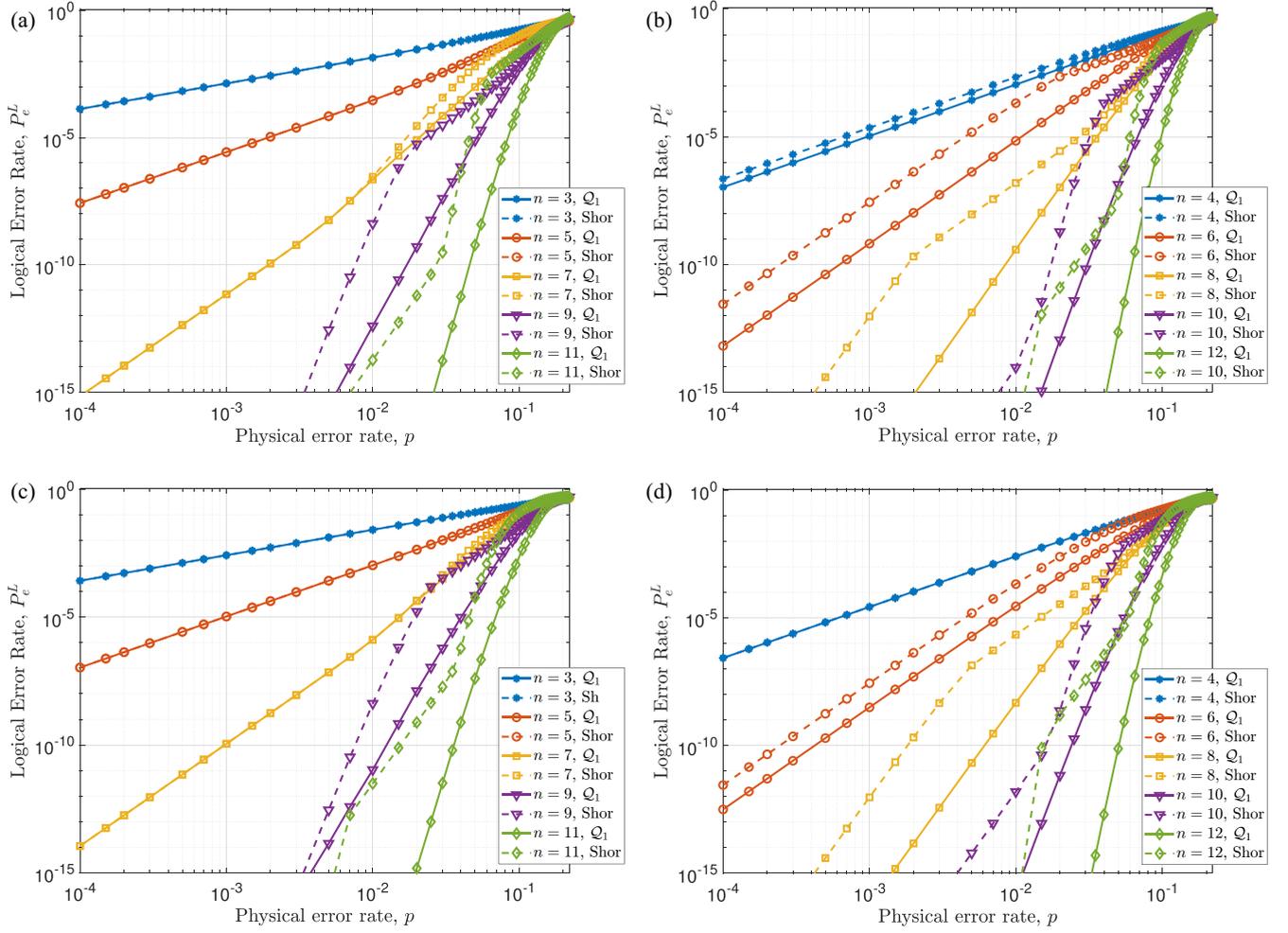
FIG. 9. Logical error rate of $\mathcal{Q}_1$ and Shor codes, for the depolarizing channel. (a), (b) Using correlations between X and Z errors. (a) n odd (for $n = 3, 5, 7$, $\mathcal{Q}_1$, and Shor curves virtually coincide). (b) n even. (c), (d) Ignoring correlations between X and Z errors. (c) n odd (for $n = 3, 5, 7$, $\mathcal{Q}_1$, and Shor curves virtually coincide). (d) n even (for $n = 4$, $\mathcal{Q}_1$, and Shor curves virtually coincide).

$2^n - 2^k$ inputs are equal to $|+\rangle$ (see Fig. 8). Hence, each of the 2^{n-k} parallel Q_{2^k} unitaries in Fig. 8 acts trivially on its input state. Therefore, the input of the rth $Q_{2^{n-k}}$ unitary, where $1 \leqslant r \leqslant 2^k$, is the quantum state $|0\rangle_{r,1} \otimes_{c=2}^{2^{n-k}} |+\rangle_{r,c}$. It follows that (omitting normalization factors)

$$
\begin{aligned}
|\widetilde{0}\rangle_{\mathcal{S}} &= \otimes_{r=1}^{2^k} Q_{2^{n-k}} \left(|0\rangle_{r,1} \otimes_{c=2}^{2^{n-k}} |+\rangle_{r,c} \right) \\
&= \otimes_{r=1}^{2^k} Q_{2^{n-k}} \left(\left(|+\rangle_{r,1} + |-\rangle_{r,1} \right) \otimes_{c=2}^{2^{n-k}} |+\rangle_{r,c} \right) \\
&= \otimes_{r=1}^{2^k} \left[Q_{2^{n-k}} \left(\otimes_{c=1}^{2^{n-k}} |+\rangle_{r,c} \right) \right. \\
&\qquad\quad \left. + Q_{2^{n-k}} \left(|-\rangle_{r,1} \otimes_{c=2}^{2^{n-k}} |+\rangle_{r,c} \right) \right] \\
&= \otimes_{r=1}^{2^k} \left(\otimes_{c=1}^{2^{n-k}} |+\rangle_{r,c} + \otimes_{c=1}^{2^{n-k}} |-\rangle_{r,c} \right). \quad (C1)
\end{aligned}
$$

For the logical state $|\widetilde{1}\rangle_{\mathcal{S}}$, the inputs of Q_N is $|1\rangle_{r,1} \otimes_{c=2}^{2^{n-k}} |+\rangle_{r,c}$. Hence, using $|1\rangle_{r,1} = |+\rangle_{r,1} - |-\rangle_{r,1}$, it follows similarly that $|\widetilde{1}\rangle_{\mathcal{S}} = \otimes_{r=1}^{2^k} (\otimes_{c=1}^{2^{n-k}} |+\rangle_{r,c} - \otimes_{c=1}^{2^{n-k}} |-\rangle_{r,c})$.

2. Construction of general $\mathcal{Q}_1$ codes

In this section we provide more details about the construction of $\mathcal{Q}_1$ codes, and further numerically estimate its performance on Pauli and erasure channels.

For $\mathcal{Q}_1$ codes, SC decoder only needs to decode the virtual channels corresponding to the information position i for both X and Z error channels W_Z and W_X, respectively. Let $P_e(W_Z^{(i)})$ and $P_e(W_X^{(\pi(i))})$ denote the error probability of the respective virtual channels, corresponding to the information position i. Recall that the error probability of a classical channel, is the probability of the maximum *a posteriori* estimate of the channel input, conditional on the observed channel output, not being equal to the actual input. Hence, the logical error rate of the $\mathcal{Q}_1$ code, with respect to the information position i, is given by

$$
P_e^L(i) = 1 - \left[1 - P_e(W_Z^{(i)}) \right]\left[1 - P_e(W_X^{(\pi(i))}) \right]. \quad (C2)
$$

The information position i should be chosen so as to minimize the corresponding logical error rate in (C2). Precisely, we have

$$
i = \arg\min_{j=1,\dots,N} P_e^L(j), \quad \text{for } \mathcal{Q}_1 \text{ codes}, \quad (C3)
$$

$$
i = \arg\min_{j=2^0,\dots,2^n} P_e^L(j), \quad \text{for Shor-}\mathcal{Q}_1 \text{ codes}. \quad (C4)
$$

3. Numerical results

Here we provide numerical results for the construction of $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes, for the quantum depolarizing and quantum erasure channels.

The quantum depolarizing channel with physical error probability p, is a Pauli channel as in (B13), with $P_I = 1 - p$, and $p_X = p_Y = p_Z = p/3$. We use density evolution [24] to estimate the error probability of virtual channels, i.e., $P_e(W_Z^{(j)})$ and $P_e(W_X^{(\pi(j))})$, $j = 1, \ldots, N$. The information positions for the $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes are then determined according to (C3) and (C4). Moreover, we consider the two constructions (or decoding strategies) given in Sec. 2, i.e., either using or ignoring the correlations between X and Z errors. Here ignoring correlations between X and Z errors may seem unfounded. We will later provide the rationale for this in Sec. 2, under the paragraph "Prepared Codes."

The quantum erasure channel erases the input qubit, with some probability ε, or transmits it perfectly, with probability $1 - \varepsilon$. When a qubit is erased, it is replaced by a totally mixed state. Further, the channel also outputs a classical flag, which indicates whether the qubit has been erased ($|1\rangle_E$) or not ($|0\rangle_E$). Hence, it can be represented as a quantum operation as follows:

$$\mathcal{W}_E(\rho) = (1 - \varepsilon)|0\rangle\langle0|_E \otimes \rho + \varepsilon|1\rangle\langle1|_E \otimes \tfrac{1}{2}. \quad \text{(C5)}$$

It is easily seen that $\mathcal{W}_E$ acts as a classical erasure channel with erasure probability ε in both Pauli Z and Pauli X basis. Hence, the induced channels W_X and W_Z are classical erasure channels, with erasure probability ε. The erasure probability of virtual channels ($P_e(W_Z^{(j)})$ and $P_e(W_X^{(\pi(j))})$, $j = 1, \ldots, N$) can be computed analytically [3]. The information positions for the $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes are then determined according to (C3) and (C4). For this channel, the two construction strategies (using or ignoring correlations) are easily seen to be equivalent.

Considering the quantum depolarizing channel, Fig. 9 shows the logical error rate $P_e^L(i)$ vs the physical error probability p, for the $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes, with information position determined according to to (C3) and (C4). Note that for fixed code length $N = 2^n$, the information position may vary depending on the physical error probability value. We consider the two decoding strategies mentioned above, namely, either using or ignoring the correlations between X and Z errors. It can be observed that using correlations yield (slightly) better decoding performance. Moreover, in both cases, we observe that the logical error rate of the $\mathcal{Q}_1$ code is in general lower than that of the Shor code, and the gap is increasing with increasing code length (i.e., number of polarization steps n). We emphasize that the gap in the decoding performance is due to the channel polarization phenomenon and not to the minimum distance ($\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes have actually the same minimum distance, see below).

As just mentioned, the information position i may vary, depending on the physical error probability p. However, numerical results suggests that as p goes to zero, the information position i reaches a stable (constant) value. These values are reported in Table II for both decoding strategies (either using or ignoring correlations), and different values of n. We also report in Table II similar results for the quantum erasure channel
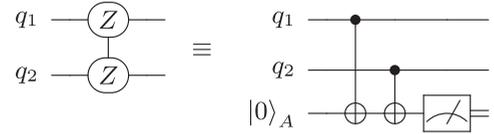
(a) Pauli $Z \otimes Z$ measurement: shorthand notation (left) and quantum circuit implementing the Pauli $Z \otimes Z$ measurement (right).
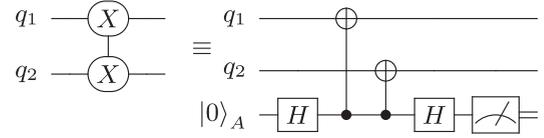
(b) Pauli $X \otimes X$ measurement: shorthand notation (left) and quantum circuit implementing the Pauli $X \otimes X$ measurement (right).

FIG. 10. Two-qubit Pauli measurements: shorthand notation and quantum circuits implementing the measurements.

(we omit the logical error rate curves for the quantum erasure channel, since they are of the same nature as the logical error rate curves in Fig. 9). It can be observed that for $\mathcal{Q}_1$ codes, the information position values reported in Table II depend on the noise model (depolarizing or erasure channel), as well as the decoding strategy (using or ignoring correlations).

Finally, we note that for a given n value, all $\mathcal{Q}_1$ and Shor codes with information positions given in Table II have the same minimum distance, which is reported on the last column of the table. The reported minimum distance is the minimum weight of logical X and Z operators, and can be computed by using (B11) and (B12).

APPENDIX D: MEASUREMENT-BASED PREPARATION OF LOGICAL $\mathcal{Q}_1$ CODE STATES

1. Measurement-based preparation without noise (Proof of Lemma 1)

We consider the standard "phase kickback trick" implementation of Pauli $X \otimes X$ and $Z \otimes Z$ measurements, using ancilla qubits as in Fig. 10.

Case 1: Preparation using Pauli $Z \otimes Z$ measurements

In this case, our procedure consists of performing transversal Pauli $Z \otimes Z$ measurements on corresponding qubits of systems $\mathcal{S}_1 = \{1, \ldots, K/2\}$, and $\mathcal{S}_2 = \{K/2 + 1, \ldots, K\}$, prepared in $\mathcal{Q}_1$ code states $|q_{\frac{K}{2}}^1\rangle_{\mathcal{S}_1} := Q_{\frac{K}{2}}|\boldsymbol{u_1}, \overline{\boldsymbol{v}}_1\rangle_{\mathcal{S}_1}$ and $|q_{\frac{K}{2}}^2\rangle_{\mathcal{S}_2} := Q_{\frac{K}{2}}|\boldsymbol{u_2}, \overline{\boldsymbol{v}}_2\rangle_{\mathcal{S}_2}$, respectively, as illustrated in Fig. 11.

Expanding the quantum state $|\overline{\boldsymbol{v}}_1\rangle_{\mathcal{X}(n-1)}$ in the Pauli Z basis, and using (B1), we get, up to a normalization factor,

$$\left|q_{\frac{K}{2}}^1\right\rangle_{\mathcal{S}_1} = \sum_{\boldsymbol{x_1} \in \{0,1\}^{\frac{K}{2} - i(k-1)}} (-1)^{\boldsymbol{v_1} \cdot \boldsymbol{x_1}} |P_{\frac{K}{2}}(\boldsymbol{u_1}, \boldsymbol{x_1})\rangle_{\mathcal{S}_1}. \quad \text{(D1)}$$

Similarly, we may also expand the quantum state $|q_{K/2}^2\rangle_{\mathcal{S}_2}$ in the Pauli Z basis. Further, we consider the circuit in Fig. 10(a) to perform transversal Pauli $Z \otimes Z$ measurements, which are done in the following two steps [below, we denote by $\mathcal{S}_3$ the ancilla system A from Fig. 10(a)].

TABLE II. Best information positions for low error probabilities.[a]

Levels of recursion (n)	Depolarizing channel using correlations		Depolarizing channel ignoring correlations		Erasure channel		Min dist.
	Information position i for best $\mathcal{Q}_1$ and Shor-$\mathcal{Q}_1$ codes						
	$\mathcal{Q}_1$	Shor	$\mathcal{Q}_1$	Shor	$\mathcal{Q}_1$	Shor	
3	4 (6.8×10^{-2})	4 (2.0×10^{-1})	4 (1.0×10^{-3})	4 (1.0×10^{-3})	2 (5.0×10^{-1})	2 (5.0×10^{-1})	2
4	13 (2.0×10^{-1})	4 (2.0×10^{-1})	7 (9.0×10^{-4})	4 (2.0×10^{-1})	7 (5.0×10^{-1})	4 (5.0×10^{-1})	4
5	8 (2.0×10^{-1})	8 (2.0×10^{-1})	8 (2.0×10^{-1})	8 (2.0×10^{-1})	4 (2.0×10^{-1})	4 (5.0×10^{-1})	4
6	50 (1.6×10^{-1})	8 (1.8×10^{-2})	23 (1.4×10^{-1})	8 (8.8×10^{-2})	23 (5.0×10^{-1})	8 (4.0×10^{-2})	8
7	16 (8.0×10^{-3})	16 (2.0×10^{-1})	16 (1.8×10^{-2})	16 (2.0×10^{-1})	8 (2.6×10^{-2})	8 (1.9×10^{-1})	8
8	199 (1.4×10^{-2})	16 (2.0×10^{-3})	91 (6.2×10^{-2})	16 (4.0×10^{-3})	87 (2.6×10^{-1})	16 (6.0×10^{-3})	16
9	32 (1.0×10^{-3})	32 (1.6×10^{-2})	32 (2.0×10^{-3})	32 (2.4×10^{-2})	16 (5.0×10^{-3})	16 (4.4×10^{-2})	16
10	806 (6.0×10^{-5})	32 (3.0×10^{-4})	363 (6.2×10^{-2})	32 (6.0×10^{-4})	343 (9.0×10^{-2})	32 (1.0×10^{-3})	32
11	96 (3.0×10^{-4})	64 (4.0×10^{-3})	96 (6.4×10^{-4})	64 (6.3×10^{-3})	32 (1.0×10^{-3})	32 (1.4×10^{-2})	32
12	3222 (6.0×10^{-5})	64 (6.0×10^{-5})	1451 (6.6×10^{-2})	64 (1.0×10^{-4})	1367 (4.4×10^{-2})	64 (2.4×10^{-4})	64

[a]For the depolarizing channel, we consider physical error rates $p \in [10^{-5}, 2\times10^{-1}]$ (note that the coherent information of the channel vanishes for $p \approx 0.1893$). Reported information position values are constant for physical error rates $p \in [10^{-5}, p_0]$. The value of p_0 is reported in parentheses, under the value of i (small font). Similarly, for the quantum erasure channel, we consider channel erasure probability values $\varepsilon \in [10^{-5}, 5\times10^{-1}]$. Reported information position values are constant for channel erasure probabilities $\varepsilon \in [10^{-5}, \varepsilon_0]$, where the value of ε_0 is reported in parentheses, under the value of i.

(1) We first take an $(K/2)$-qubit ancilla state $|\mathbf{0}\rangle_{\mathcal{S}_3}$, and then apply transversal CNOT gates, $\text{CNOT}_{\mathcal{S}_1 \to \mathcal{S}_3}$ and $\text{CNOT}_{\mathcal{S}_2 \to \mathcal{S}_3}$. This gives the following joint quantum state on $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$:

$$|\eta\rangle_{\mathcal{S}_1\mathcal{S}_2\mathcal{S}_3} = \sum_{\mathbf{x}_1,\mathbf{x}_2}(-1)^{\mathbf{v}_1\cdot\mathbf{x}_1+\mathbf{v}_2\cdot\mathbf{x}_2}|P_{\frac{K}{2}}(\mathbf{u}_1,\mathbf{x}_1)\rangle_{\mathcal{S}_1}|P_{\frac{K}{2}}(\mathbf{u}_2,\mathbf{x}_2)\rangle_{\mathcal{S}_2}$$
$$\times |P_{\frac{K}{2}}(\mathbf{u}_1\oplus\mathbf{u}_2,\mathbf{x}_1\oplus\mathbf{x}_2)\rangle_{\mathcal{S}_3}. \quad (D2)$$
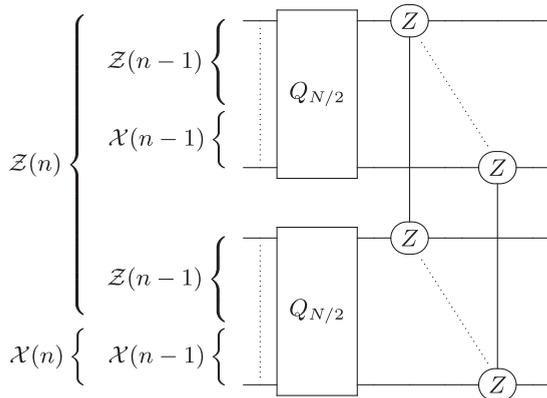
FIG. 11. Preparation using Pauli $Z\otimes Z$ measurements ($i(k) = i(k-1)+\frac{K}{2}\in\{\frac{K}{2}+1,\dots,K\}$).

(2) Then we measure each qubit in the ancilla system $\mathcal{S}_3$ in the Pauli Z basis. From (D2), the measurement outcome gives a binary vector of length $K/2$ as follows:

$$\mathbf{m} = P_{\frac{K}{2}}(\mathbf{u}',\mathbf{x}) \in \{0,1\}^{\frac{K}{2}}, \quad (D3)$$

where $\mathbf{u}' = \mathbf{u}_1\oplus\mathbf{u}_2 \in \{0,1\}^{i(k)}$, and $\mathbf{x} \in \{0,1\}^{\frac{K}{2}-i(k)}$ is a random vector. Further, from (D2) and (D3), the state of the joint system $\mathcal{S}_1 \cup \mathcal{S}_2$ after the measurements is as follows:

$$|\eta'\rangle_{\mathcal{S}_1\mathcal{S}_2} = \sum_{\substack{\mathbf{x}_1,\mathbf{x}_2\\\mathbf{x}_1\oplus\mathbf{x}_2=\mathbf{x}}}(-1)^{\mathbf{v}_1\cdot\mathbf{x}_1+\mathbf{v}_2\cdot\mathbf{x}_2}|P_{\frac{K}{2}}(\mathbf{u}_1,\mathbf{x}_1)\rangle_{\mathcal{S}_1}|P_{\frac{K}{2}}(\mathbf{u}_2,\mathbf{x}_2)\rangle_{\mathcal{S}_2}. \quad (D4)$$

It can be seen as follows that the quantum state $|\eta'\rangle_{\mathcal{S}_1\mathcal{S}_2}$ is the $\mathcal{Q}_1$ code state $|q_K\rangle_{\mathcal{S}_1\mathcal{S}_2}$ as in Case 1 of Lemma 1:

$$|\eta'\rangle_{\mathcal{S}_1\mathcal{S}_2} = \sum_{\substack{\mathbf{x}_1,\mathbf{x}_2\\\mathbf{x}_1\oplus\mathbf{x}_2=\mathbf{x}}}(-1)^{\mathbf{v}_1\cdot\mathbf{x}_1+\mathbf{v}_2\cdot\mathbf{x}_2}|P_{\frac{K}{2}}(\mathbf{u}_1,\mathbf{x}_1)\rangle_{\mathcal{S}_1}|P_{\frac{K}{2}}(\mathbf{u}_2,\mathbf{x}_2)\rangle_{\mathcal{S}_2}$$

$$= \sum_{\mathbf{x}_2}(-1)^{\mathbf{v}_1\cdot(\mathbf{x}+\mathbf{x}_2)+\mathbf{v}_2\cdot\mathbf{x}_2}|P_{\frac{K}{2}}(\mathbf{u}'\oplus\mathbf{u}_2,\mathbf{x}\oplus\mathbf{x}_2)\rangle_{\mathcal{S}_1}$$

$$\times |P_{\frac{K}{2}}(\mathbf{u}_2,\mathbf{x}_2)\rangle_{\mathcal{S}_2}$$

$$= (-1)^{\mathbf{v}_1\cdot\mathbf{x}}\sum_{\mathbf{x}_2}(-1)^{(\mathbf{v}_1+\mathbf{v}_2)\cdot\mathbf{x}_2}|P_K(\mathbf{u}',\mathbf{x},\mathbf{u}_2,\mathbf{x}_2)\rangle_{\mathcal{S}_1\mathcal{S}_2}$$

$$= Q_K|\mathbf{u}',\mathbf{x},\mathbf{u}_2,\overline{\mathbf{v}_1\oplus\mathbf{v}_2}\rangle_{\mathcal{S}_1\mathcal{S}_2},$$
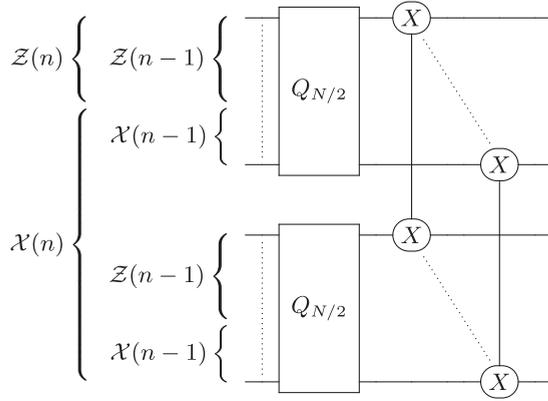
FIG. 12. Preparation using Pauli $X \otimes X$ measurements ($i(k) = i(k-1) \in \{1, \ldots, \frac{K}{2}\}$).

where in the second equality, we have used $\boldsymbol{u_1} = \boldsymbol{u'} \oplus \boldsymbol{u_2}$ and $\boldsymbol{x_1} = \boldsymbol{x} \oplus \boldsymbol{x_2}$, and in the third equality, we have used $P_K(\boldsymbol{a}, \boldsymbol{b}) = (P_{\frac{K}{2}}(\boldsymbol{a} \oplus \boldsymbol{b}), P_{\frac{K}{2}}(\boldsymbol{b})), \boldsymbol{a}, \boldsymbol{b} \in \{0, 1\}^{\frac{K}{2}}$, using the recursion of the classical polar transform given in Fig. 5(a).

Hence, after the Pauli $Z \otimes Z$ measurements, we have prepared the $\mathcal{Q}_1$ code state on the joint system $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$,

$$|q_K\rangle_{\mathcal{S}} = Q_K |\boldsymbol{u'}, \boldsymbol{x}, \boldsymbol{u_2}, \overline{\boldsymbol{v_1} \oplus \boldsymbol{v_2}}\rangle_{\mathcal{S}}. \tag{D5}$$

Finally, from (D3), we have that $P_{\frac{K}{2}}(\boldsymbol{m}) = (\boldsymbol{u'}, \boldsymbol{x}) \in \{0, 1\}^{\frac{K}{2}}$ (using $P_K^2 = I$). Hence, $\boldsymbol{x}$ is determined by, $\boldsymbol{x} = P_{\frac{K}{2}}(\boldsymbol{m})|_{\mathcal{X}(n-1)}$, as desired.

Case 2: Preparation using Pauli $X \otimes X$ measurements

In this case, our procedure consists in performing transversal Pauli $X \otimes X$ measurements on corresponding qubits of systems $\mathcal{S}_1$ and $\mathcal{S}_2$, prepared in $\mathcal{Q}_1$ code states $|q_{\frac{K}{2}}^1\rangle_{\mathcal{S}_1} := Q_{\frac{K}{2}} |\boldsymbol{u_1}, \overline{\boldsymbol{v_1}}\rangle_{\mathcal{S}_1}$ and $|q_{\frac{K}{2}}^2\rangle_{\mathcal{S}_2} := Q_{\frac{K}{2}} |\boldsymbol{u_2}, \overline{\boldsymbol{v_2}}\rangle_{\mathcal{S}_2}$, as illustrated in Fig. 12.

We skip the proof here as it is similar to Case 1. By expanding $|q_{\frac{K}{2}}^1\rangle_{\mathcal{S}_1}$ and $|q_{\frac{K}{2}}^2\rangle_{\mathcal{S}_2}$, in the Pauli X basis instead and using (B2) it can be seen that the measurement outcome of Pauli $X \otimes X$ measurements is given by

$$\boldsymbol{m} = P_{\frac{K}{2}}^{\top}(\boldsymbol{z}, \boldsymbol{v'}) \in \{0, 1\}^{\frac{K}{2}}, \tag{D6}$$

where $\boldsymbol{z} \in \{0, 1\}^{i(k-1)}$ is a random vector, and $\boldsymbol{v'} = \boldsymbol{v_1} \oplus \boldsymbol{v_2} \in \{0, 1\}^{\frac{K}{2} - i(k-1)}$. Further, after measurements, the state on $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$ is a $\mathcal{Q}_1$ state is given by

$$|q_K\rangle_{\mathcal{S}} = |\boldsymbol{u_1} \oplus \boldsymbol{u_2}, \overline{(\boldsymbol{v_1}, \boldsymbol{z}, \boldsymbol{v'})}\rangle, \tag{D7}$$

where $\boldsymbol{z}$ can be determined from (D6) as, $\boldsymbol{z} = P_{\frac{K}{2}}^{\top}(\boldsymbol{m})|_{\mathcal{Z}(k-1)}$.

2. Fault-tolerant measurement-based preparation with noise

In this section, supposing a circuit-level noise model with Pauli errors, we detail the measurement-based preparation with the error detection from Procedure 2, for both Cases 1 and 2. Then, we provide a proof of fault tolerance according to Theorem 3.
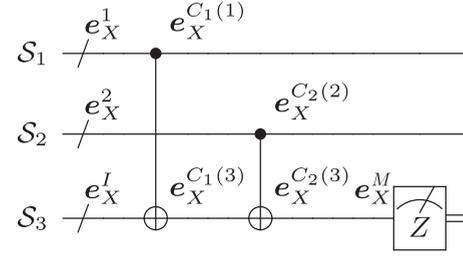
(a) X errors.
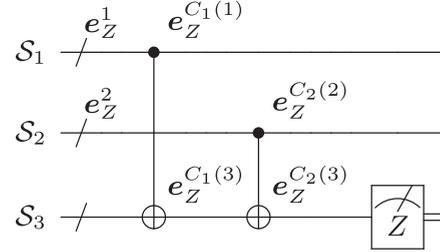
(b) Z errors.

FIG. 13. Representation of errors during the preparation with Pauli $Z \otimes Z$ measurements. The crossed wires represent $K/2$-qubit systems $\mathcal{S}_1$, $\mathcal{S}_2$ and $\mathcal{S}_3$, respectively. The CNOT gate between two systems represents the transversal CNOT gates between the systems. The errors are represented where they happen. For example, in Fig. 13(a), $\boldsymbol{e}_X^1, \boldsymbol{e}_X^2$, and $\boldsymbol{e}_X^I$ represent the initial errors on systems $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{S}_3$, respectively. Further, $\boldsymbol{e}_X^{C_1(1)}$ and $\boldsymbol{e}_X^{C_1(3)}$ represent the errors caused by the first CNOT, applied between $\mathcal{S}_1$ and $\mathcal{S}_3$, respectively. Similarly, the errors due to the second CNOT are represented on systems $\mathcal{S}_2$ and $\mathcal{S}_3$. Finally, $\boldsymbol{e}_X^M$ represents the X error due to the measurement on system $\mathcal{S}_3$.

We suppose that we are given noisy versions of $\mathcal{Q}_1$ code states of length $K/2$ on $\mathcal{S}_1 = \{1, \ldots, K/2\}$ and $\mathcal{S}_2 = \{K/2 + 1, \ldots, K\}$, as follows:

$$|q_{\frac{K}{2}}^1\rangle_{\mathcal{S}_1} = X^{\boldsymbol{e}_X^1} Z^{\boldsymbol{e}_Z^1} Q_{\frac{K}{2}} |\boldsymbol{u_1}, \overline{\boldsymbol{v_1}}\rangle_{\mathcal{S}_1}, \tag{D8}$$

$$|q_{\frac{K}{2}}^2\rangle_{\mathcal{S}_2} = X^{\boldsymbol{e}_X^2} Z^{\boldsymbol{e}_Z^2} Q_{\frac{K}{2}} |\boldsymbol{u_2}, \overline{\boldsymbol{v_2}}\rangle_{\mathcal{S}_2}, \tag{D9}$$

where $\boldsymbol{u_1}, \boldsymbol{u_2} \in \{0, 1\}^{i(k-1)}$, $\boldsymbol{v_1}, \boldsymbol{v_2} \in \{0, 1\}^{\frac{K}{2} - i(k-1)}$, and the errors $\boldsymbol{e}_X^1, \boldsymbol{e}_Z^1, \boldsymbol{e}_X^2, \boldsymbol{e}_Z^2 \in \{0, 1\}^{\frac{K}{2}}$ are unknown.

Case 1: Preparation using noisy Pauli $Z \otimes Z$ measurements

We suppose that the following errors happen due to the component failures during transversal Pauli $Z \otimes Z$ measurements [see also Fig. 13, where all errors are given; also recall from the previous section, that $\mathcal{S}_3$ denotes the ancilla system needed for the "phase kickback trick" implementation of $Z \otimes Z$ measurements, i.e., system A in Fig. 10(a)].

(1) Suppose failures during the intialization of $\mathcal{S}_3$ in the Pauli Z basis cause an X error $\boldsymbol{e}_X^I \in \{0, 1\}^{K/2}$ on $\mathcal{S}_3$.

(2) Suppose CNOT failures in $\text{CNOT}_{\mathcal{S}_1 \to \mathcal{S}_3}$ cause X, Z type errors $\boldsymbol{e}_X^{C_1(1)}, \boldsymbol{e}_Z^{C_1(1)} \in \{0, 1\}^{K/2}$, respectively, on $\mathcal{S}_1$, and X, Z type errors $\boldsymbol{e}_X^{C_1(3)}, \boldsymbol{e}_Z^{C_1(3)} \in \{0, 1\}^{K/2}$, respectively, on $\mathcal{S}_3$.

TABLE III. Total errors on systems $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{S}_3$.

System	Total X error	Total Z error
$\mathcal{S}_1$	$e_X^1 \oplus e_X^{C_1(1)}$	$e_Z^1 \oplus e_Z^{C_1(1)}$
$\mathcal{S}_2$	$e_X^2 \oplus e_X^{C_2(2)}$	$e_Z^2 \oplus e_Z^{C_1(3)} \oplus e_Z^{C_2(2)}$
$\mathcal{S}_3$	$e_X^I \oplus e_X^1 \oplus e_X^{C_1(3)} \oplus e_X^2 \oplus e_X^{C_2(3)} \oplus e_X^M$	$e_Z^{C_1(3)} \oplus e_Z^{C_2(3)}$

(3) Suppose CNOT failures in $\text{CNOT}_{\mathcal{S}_2 \to \mathcal{S}_3}$ cause X, Z type errors $e_X^{C_2(2)}, e_Z^{C_2(2)} \in \{0, 1\}^{K/2}$, respectively, on $\mathcal{S}_2$, and X, Z type errors $e_X^{C_2(3)}, e_Z^{C_2(3)} \in \{0, 1\}^{K/2}$, respectively, on $\mathcal{S}_3$.

(4) Suppose failures during the measurement of $\mathcal{S}_3$ in the Pauli Z basis cause an X error $e_X^M \in \{0, 1\}^{K/2}$ on $\mathcal{S}_3$.

The measurement outcome of the transversal Pauli $Z \otimes Z$ measurements and the state of the joint system $\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2$ after measurements is given in Lemma 6.

Lemma 6. The measurement outcome of noisy transversal Pauli $Z \otimes Z$ measurements on systems $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively in (D8) and (D9), is equal to

$$\boldsymbol{m}' = \boldsymbol{m} \oplus \boldsymbol{e}_X \in \{0, 1\}^{\frac{K}{2}}, \qquad (D10)$$

where $\boldsymbol{m}$ is the measurement outcome corresponding to the preparation without noise from (D3) and $\boldsymbol{e}_X = e_X^I \oplus e_X^1 \oplus e_X^{C_1(3)} \oplus e_X^2 \oplus e_X^{C_2(3)} \oplus e_X^M$. Further, after the measurement, we get

$$|q_K'\rangle_{\mathcal{S}} = X^{\tilde{e}_X} Z^{\tilde{e}_Z} |q_K\rangle_{\mathcal{S}}, \qquad (D11)$$

where $|q_K\rangle_{\mathcal{S}}$ is the prepared state without noise from (D5) and the errors are as follows:

$$\tilde{\boldsymbol{e}}_X = \left(e_X^1 \oplus e_X^{C_1(1)}, e_X^2 \oplus e_X^{C_2(2)}\right) \in \{0, 1\}^K, \qquad (D12)$$

$$\tilde{\boldsymbol{e}}_Z = \left(e_Z^1 \oplus e_Z^{C_1(1)}, e_Z^2 \oplus e_Z^{C_1(3)} \oplus e_Z^{C_2(2)}\right) \in \{0, 1\}^K. \qquad (D13)$$

Proof. Note that X errors in Fig. 13(a), and Z errors in Fig. 13(b) can be propagated from the l.h.s. to r.h.s., using the following rules.

(1) An X error simply passes through the target of a CNOT gate, and it propagates from the control of the CNOT gate to its target.

(2) An Z error simply passes through the control of a CNOT gate, and it propagates from the target of the CNOT gate to its control.

The X and Z errors on the r.h.s. for $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{S}_3$ are given in Table III.

It follows that the noisy measurement outcome $\boldsymbol{m}'$ is equal to the binary sum of the measurement outcome $\boldsymbol{m}$ in the noiseless case and the X error on system $\mathcal{S}_3$, therefore, from Table III, we get (D10). Further, the prepared state $|q_K'\rangle_{\mathcal{S}}$ is equal to the noiseless state $|q_K\rangle_{\mathcal{S}}$, with some X and Z errors on it. The X (or Z) error on $\mathcal{S}$ is simply the concatenation of the total X (or Z) errors on systems $\mathcal{S}_1$ and $\mathcal{S}_2$. Therefore, from Table III we get (D12), and (D13), for X and Z errors in $|q_K'\rangle_{\mathcal{S}}$, respectively. ∎

We now combine the noisy preparation in Lemma 6 with the error detection gadget according to Procedure 2. We recall here how the error detection gadget works. Consider the error $\boldsymbol{e}_X$ in the measurement outcome $\boldsymbol{m}'$ in (D10) so that its

syndrome is a zero vector:

$$P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{Z}(k-1)} = \boldsymbol{0}. \qquad (D14)$$

Then the prepared state is accepted and the random vector $\boldsymbol{x}$ in (D11) is estimated as

$$\hat{\boldsymbol{x}} = P_{\frac{K}{2}}(\boldsymbol{m}')|_{\mathcal{X}(k-1)}. \qquad (D15)$$

The total error in the prepared state, with respect to the estimate $\hat{\boldsymbol{x}}$, is given in Lemma 7.

Lemma 7. Consider the error $\boldsymbol{e}_X$ in the measurement outcome $\boldsymbol{m}$ from (D10), so that it satisfies (D14), and let $\hat{\boldsymbol{x}}$ be defined according to (D15). Then, the state of the joint system $\mathcal{S}$ in (D11) can be written as follows, with respect to $\hat{\boldsymbol{x}}$:

$$|q_K'\rangle_{\mathcal{S}} = X^{\boldsymbol{e}_X^f} Z^{\boldsymbol{e}_Z^f} Q_K |(\boldsymbol{u}', \hat{\boldsymbol{x}}, \boldsymbol{u_2}, \overline{\boldsymbol{v_1} \oplus \boldsymbol{v_2}})\rangle_{\mathcal{S}}, \qquad (D16)$$

where $\boldsymbol{e}_X^f = \tilde{\boldsymbol{e}}_X + (\boldsymbol{e}_X, \boldsymbol{0})$ and $\boldsymbol{e}_Z^f = \tilde{\boldsymbol{e}}_Z$, so that $\tilde{\boldsymbol{e}}_X$ and $\tilde{\boldsymbol{e}}_Z$ are according to (D12) and (D13), respectively.

Proof. From (D3), (D10), and (D15), we have that

$$\hat{\boldsymbol{x}} = \boldsymbol{x} \oplus P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)}. \qquad (D17)$$

We may write $|q_K'\rangle_{\mathcal{S}}$ in (D11), with respect to $\hat{\boldsymbol{x}}$ as follows:

$$\begin{aligned}
|q_K'\rangle_{\mathcal{S}} &= X^{\tilde{e}_X} Z^{\tilde{e}_Z} Q_K |(\boldsymbol{u}', \boldsymbol{x}, \boldsymbol{u_2}, \overline{\boldsymbol{v_1} \oplus \boldsymbol{v_2}})\rangle \\
&= X^{\tilde{e}_X} Z^{\tilde{e}_Z} \sum_{\boldsymbol{x_2}} (-1)^{(\boldsymbol{v_1} \oplus \boldsymbol{v_2}) \cdot \boldsymbol{x_2}} \\
&\quad |P_K(\boldsymbol{u}', \hat{\boldsymbol{x}} \oplus P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)}, \boldsymbol{u_2}, \boldsymbol{x_2})\rangle \\
&= X^{\tilde{e}_X} Z^{\tilde{e}_Z} \sum_{\boldsymbol{x_2}} (-1)^{(\boldsymbol{v_1} \oplus \boldsymbol{v_2}) \cdot \boldsymbol{x_2}} X^{(\boldsymbol{e}_X, \boldsymbol{0})} |P_K(\boldsymbol{u}', \hat{\boldsymbol{x}}, \boldsymbol{u_2}, \boldsymbol{x_2})\rangle \\
&= X^{\tilde{e}_X \oplus (\boldsymbol{e}_X, \boldsymbol{0})} Z^{\tilde{e}_Z} Q_K |(\boldsymbol{u}', \hat{\boldsymbol{x}}, \boldsymbol{u_2}, \overline{\boldsymbol{v_1} \oplus \boldsymbol{v_2}})\rangle, \qquad (D18)
\end{aligned}$$

where in the second equality, we have expanded the quantum state in the Pauli Z basis and used (D17), and the third equality follows from the second equality, by using $\boldsymbol{e}_X = P_{\frac{K}{2}}(P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{Z}(n-1)}, P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)}) = P_{\frac{K}{2}}(\boldsymbol{0}, P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)})$. ∎

Case 2: Preparation using noisy Pauli $X \otimes X$ measurements

The errors during the preparation with Pauli $X \otimes X$ measurements are given in Fig. 14. Note that we have Z type initialization and measurement errors on the ancilla system $\mathcal{S}_3$, which are denoted by $e_Z^I, e_Z^M \in \{0, 1\}^{K/2}$, respectively. For the errors caused by the CNOT gates, $\text{CNOT}_{\mathcal{S}_3 \to \mathcal{S}_1}$ and $\text{CNOT}_{\mathcal{S}_3 \to \mathcal{S}_2}$, we have used the same notation as in the case of Pauli $Z \otimes Z$ measurements.

Here we provide Lemmas 8 and 9, which are analogous to Lemmas 6 and 7, respectively, and thus their proofs have been omitted.

Lemma 8. The measurement outcome of transversal Pauli $X \otimes X$ measurements on systems $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively in (D8) and (D9), is equal to

$$\boldsymbol{m}' = \boldsymbol{m} \oplus \boldsymbol{e}_Z \in \{0, 1\}^{\frac{K}{2}}, \qquad (D19)$$

where $\boldsymbol{m}$ is the measurement outcome corresponding to the preparation without noise, as in (D6), and $\boldsymbol{e}_Z = e_Z^I \oplus e_Z^1 \oplus e_Z^{C_1(3)} \oplus e_Z^2 \oplus e_Z^{C_2(3)} \oplus e_Z^M$. Further, after the measurement, we
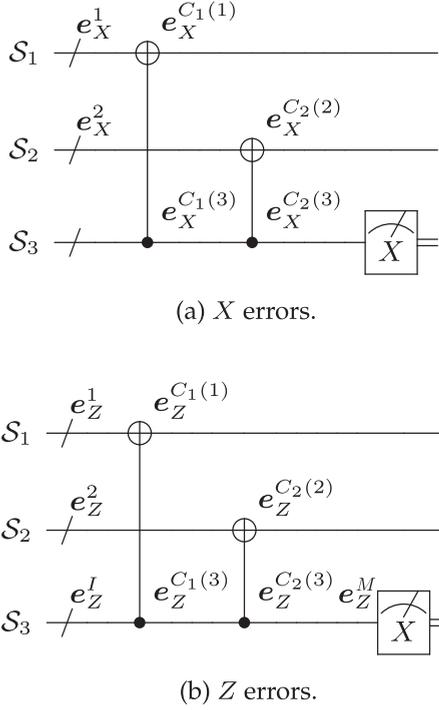
(a) X errors.

(b) Z errors.

FIG. 14. Errors during preparation with Pauli $X \otimes X$ measurements.

get

$$|q'_K\rangle_S = X^{\tilde{e}_X} Z^{\tilde{e}_Z} |q_K\rangle_S, \tag{D20}$$

where $|q_K\rangle_S$ is the prepared state without noise, as in (D7), and the errors are as follows:

$$\tilde{e}_X = \left(e_X^1 \oplus e_X^{C_1(1)}, e_X^2 \oplus e_X^{C_1(3)} \oplus e_X^{C_2(2)}\right) \in \{0, 1\}^K, \tag{D21}$$

$$\tilde{e}_Z = \left(e_Z^1 \oplus e_Z^{C_1(1)}, e_Z^2 \oplus e_Z^{C_2(2)}\right) \in \{0, 1\}^K. \tag{D22}$$

We now combine the noisy preparation in Lemma 8 with the error detection gadget according to Procedure 2. Recall that when no error is detected, the prepared state is accepted and the z in (D20) is estimated as

$$\hat{z} = P_{\frac{K}{2}}^{\top}(m')|_{\mathcal{Z}(k-1)}. \tag{D23}$$

Lemma 9. Consider the error e_Z in the measurement outcome m from (D19), so that its syndrome is a zero vector, *i.e.*, $P_{\frac{N}{2}}^{\top}(e_Z)|_{\mathcal{X}(n-1)} = 0$, and let $\hat{z}$ be defined as in (D23). Then, the state of the joint system S in (D20) can be written as follows, with respect to $\hat{z}$:

$$|q'_K\rangle_S = X^{e_X^f} Z^{e_Z^f} Q_K |u_1 \oplus u_2, \overline{v_1, \hat{z}, v'}\rangle_S, \tag{D24}$$

where $e_X^f = \tilde{e}_X$ and $e_Z^f = \tilde{e}_Z \oplus (\mathbf{0}, e_Z)$, so that $\tilde{e}_X$ and $\tilde{e}_Z$ are according to (D21) and (D22), respectively, and e_Z is the measurement error in (D19).

Proof of Theorem 3

We provide a proof of Theorem 3, using the mathematical induction. The base case, i.e., the zeroth level of recursion, corresponds to the initialization of N qubits in a Pauli Z basis state. Let T_0 be the number of failures in initialization. As a

failure in initialization produces only a single-qubit X error, therefore, we have that $\text{wt}(e_X^f) = T_0$, for the error $e_X^f \in \{0, 1\}^N$ after the zeroth level of recursion. Hence, Theorem 3 holds for the zeroth level of recursion.

We show in Lemma 11 below that if Theorem 3 is true for the $(k-1)$th, $1 \leqslant k \leqslant n$, level of recursion, it remains true for the kth level of recursion, therefore, implying that Theorem 3 holds for any $1 \leqslant k \leqslant n$.

Recall that at the kth level of recursion, we prepare 2^{n-k} copies of $|q_K\rangle$, where each copy is prepared by applying transversal two-qubit Pauli measurements on two copies of $|q_{K/2}\rangle$. It is enough to show that Theorem 3 holds for a given preparation instance of $|q_K\rangle$. Hence, we consider $|q_{K/2}\rangle_{S_1}$ and $|q_{K/2}\rangle_{S_2}$ from (D8) and (D9), and for the sake of brevity, we suppose that Pauli $Z \otimes Z$ measurements are applied at the kth level of recursion. Similar results to the ones that will be proven here can be obtained for the case of Pauli $X \otimes X$ measurements.

We suppose that t_k component failures happen during the implementation of transversal Pauli $Z \otimes Z$ measurements on S_1 and S_2, using an ancilla system S_3 (see also Fig. 13). We decompose t_k as follows:

$$t_k = t_k^I + t_k^{C_1} + t_k^{C_2} + t_k^M, \tag{D25}$$

where t_k^I is the number of failures during the initialization of S_3 in the Pauli Z basis, $t_k^{C_i}$ for $i \in \{1, 2\}$ is the number of CNOT failures in $\text{CNOT}_{S_i \to S_3}$, and t_k^M is the number of failures during the Pauli Z measurement on S_3. To relate with Fig. 13, note that the errors e_X^I and e_X^M are produced by t_k^I and t_k^M faults, respectively. Further, the errors $e_X^{C_1(1)}, e_X^{C_1(3)}, e_Z^{C_1(1)}, e_Z^{C_1(3)}$ are produced by $t_k^{C_1}$ faults, and finally the errors $e_X^{C_2(2)}, e_X^{C_2(3)}, e_Z^{C_2(2)}, e_Z^{C_2(3)}$ are produced by $t_k^{C_2}$ faults.

We will also need the following notation:

(i) For $i \in \{1, 2\}$, let $t_k^{C_i}(X)$ be the number of CNOT failures in $\text{CNOT}_{S_i \to S_3}$ that produce a single-qubit X error on the corresponding outputs, i.e., the number of CNOT failures, where one of the following errors $X \otimes I, X \otimes Z, I \otimes X, Z \otimes X, Y \otimes I, Y \otimes Z, I \otimes Y, Z \otimes Y$ is produced. Similarly, let $t_k^{C_i}(Z)$ be the number of CNOT failures in $\text{CNOT}_{S_i \to S_3}$ that produce a single-qubit Z error.

(ii) For $i \in \{1, 2\}$, let $t_k^{C_i}(XX)$ be the number of CNOT failures in $\text{CNOT}_{S_i \to S_3}$ that produce a two-qubit X error, i.e., the number of CNOT failures, where one of the errors $X \otimes X, X \otimes Y, Y \otimes X, Y \otimes Y$ is produced. Similarly, let $t_k^{C_i}(ZZ)$ be the number of CNOT failures in $\text{CNOT}_{S_i \to S_3}$ that produce a two-qubit Z error.

Note that the following inequalities hold trivially for $i \in \{1, 2\}$:

$$t_k^{C_i}(X) + t_k^{C_i}(XX) \leqslant t_k^{C_i}, \tag{D26}$$

$$t_k^{C_i}(Z) + t_k^{C_i}(ZZ) \leqslant t_k^{C_i}. \tag{D27}$$

In Lemma 10, we provide several inequalities, connecting the number of faults with the weight of the produced errors (see Fig. 13). We will use these equalities later in the proof of Lemma 11.

Lemma 10. The following inequalities hold at the kth level of recursion:

$$\mathrm{wt}\big(\boldsymbol{e}_X^I\big) = t_k^I, \tag{D28}$$

$$\mathrm{wt}\big(\boldsymbol{e}_X^M\big) = t_k^M, \tag{D29}$$

$$\mathrm{wt}\big(\boldsymbol{e}_X^{C_i(i)} \oplus \boldsymbol{e}_X^{C_i(3)}\big) = t_k^{C_i}(X), i \in \{1, 2\}, \tag{D30}$$

$$\mathrm{wt}\big(\boldsymbol{e}_X^{C_i(i)}\big) + \mathrm{wt}\big(\boldsymbol{e}_X^{C_i(3)}\big) = t_k^{C_i}(X) + 2t_k^{C_i}(XX), i \in \{1, 2\}, \tag{D31}$$

$$\mathrm{wt}\big(\boldsymbol{e}_Z^{C_i(i)} \oplus \boldsymbol{e}_Z^{C_i(3)}\big) = t_k^{C_i}(Z), i \in \{1, 2\}, \tag{D32}$$

$$\mathrm{wt}\big(\boldsymbol{e}_Z^{C_i(i)}\big) + \mathrm{wt}\big(\boldsymbol{e}_Z^{C_i(3)}\big) = t_k^{C_i}(Z) + 2t_k^{C_i}(ZZ), i \in \{1, 2\}. \tag{D33}$$

Proof. The equalities in (D28) and (D29) simply follow from the fact a failure in Pauli Z basis initialization or measurement produces a single-qubit X error on the output.

Suppose the jth, $j \in \{1, \ldots, K/2\}$-CNOT gate in $\mathrm{CNOT}_{\mathcal{S}_i \to \mathcal{S}_3}$ failed. If it produces a single-qubit X error on the output, the jth component of either $\boldsymbol{e}_X^{C_i(i)}$ or $\boldsymbol{e}_X^{C_i(3)}$ is equal to 1. If it produces a two-qubit X error on the output, the jth component of both $\boldsymbol{e}_X^{C_i(i)}$ and $\boldsymbol{e}_X^{C_i(3)}$ is equal to 1. This observation directly implies (D30) and (D31). Similarly, it can be seen that (D32) and (D33) hold. ∎

Lemma 11. Suppose that T_{k-1}^1 faults occur during the (successful) preparation of $|q_{K/2}\rangle_{\mathcal{S}_1}$ in (D8) and T_{k-2}^2 faults occur during the preparation of $|q_{K/2}\rangle_{\mathcal{S}_2}$ in (D9), using the measurement-based procedure incorporated with the error detection. Further, suppose that the following holds for $i \in \{1, 2\}$:

$$\mathrm{wt}\big(\boldsymbol{e}_X^i\big) \leqslant T_{k-1}^i, \tag{D34}$$

$$\mathrm{wt}\big(\boldsymbol{e}_Z^i\big) \leqslant T_{k-1}^i. \tag{D35}$$

Consider the prepared state $|q_K'\rangle$ according to (D16). Then there exist equivalent errors $\boldsymbol{e}_X'^f \equiv \boldsymbol{e}_X^f, \boldsymbol{e}_Z'^f \equiv \boldsymbol{e}_Z^f$, satisfying

$$\mathrm{wt}\big(\boldsymbol{e}_X'^f\big) \leqslant T_k, \tag{D36}$$

$$\mathrm{wt}\big(\boldsymbol{e}_Z'^f\big) \leqslant T_k, \tag{D37}$$

where $T_k = T_{k-1}^1 + T_{k-1}^2 + t_k$, where t_k is from (D25), is the total number of failures after the kth level of recursion.

Proof. We first prove (D36). Let $\boldsymbol{e}_X$ be the measurement error in (D10), so that its syndrome is zero according to (D14). Then the syndrome of $(\boldsymbol{e}_X, \boldsymbol{e}_X)$ is also zero, i.e., $P_N(\boldsymbol{e}_X, \boldsymbol{e}_X)|_{\mathcal{Z}(k)} = \boldsymbol{0}$. It can be seen as follows. We have that

$$(\boldsymbol{e}_X, \boldsymbol{e}_X) = (P_{K/2}(\boldsymbol{0}, P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)}), \ P_{K/2}(\boldsymbol{0}, P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)}))$$

$$= P_K(\boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}, P_{\frac{K}{2}}(\boldsymbol{e}_X)|_{\mathcal{X}(n-1)}). \tag{D38}$$

Using $|\mathcal{X}(n-1)| = |\mathcal{X}(n)|$ and (D38), it follows that $P_N(\boldsymbol{e}_X, \boldsymbol{e}_X)|_{\mathcal{Z}(k)} = \boldsymbol{0}$. Therefore, $(\boldsymbol{e}_X, \boldsymbol{e}_X)$ gives a stabilizer (up to a sign factor) of the quantum state $|q_K'\rangle$ in (D16), implying that $\boldsymbol{e}_X'^f := \widetilde{\boldsymbol{e}}_X + (\boldsymbol{0}, \boldsymbol{e}_X)$ is an equivalent error to $\boldsymbol{e}_X^f = \widetilde{\boldsymbol{e}}_X + (\boldsymbol{e}_X, \boldsymbol{0})$ in (D16).

We now provide upper bounds on $\mathrm{wt}(\boldsymbol{e}_X^f)$ and $\mathrm{wt}(\boldsymbol{e}_X'^f)$.

From (D10) and (D12), we have that

$$\boldsymbol{e}_X^f = \big(\boldsymbol{e}_X^2 \oplus \boldsymbol{e}_X^I \oplus \boldsymbol{e}_X^{C_1(1)} \oplus \boldsymbol{e}_X^{C_1(3)} \oplus \boldsymbol{e}_X^{C_2(3)} \oplus \boldsymbol{e}_X^M, \ \boldsymbol{e}_X^2 \oplus \boldsymbol{e}_X^{C_2(2)}\big). \tag{D39}$$

Further,

$$\mathrm{wt}\big(\boldsymbol{e}_X^f\big) \leqslant 2\mathrm{wt}\big(\boldsymbol{e}_X^2\big) + \mathrm{wt}\big(\boldsymbol{e}_X^I\big) + \mathrm{wt}\big(\boldsymbol{e}_X^{C_1(1)} \oplus \boldsymbol{e}_X^{C_1(3)}\big)$$

$$+ \mathrm{wt}\big(\boldsymbol{e}_X^{C_2(2)}\big) \oplus \mathrm{wt}\big(\boldsymbol{e}_X^{C_2(3)}\big) + \mathrm{wt}\big(\boldsymbol{e}_X^M\big)$$

$$\leqslant 2\big(\mathrm{wt}\big(\boldsymbol{e}_X^2\big) + t_k^{C_2}(XX)\big) + t_k^I + t_k^{C_1}(X)$$

$$+ t_k^{C_2}(X) + t_k^M, \tag{D40}$$

where the first inequality follows from (D39) and using $\mathrm{wt}(\sum_i \boldsymbol{u}_i) \leqslant \sum_i \mathrm{wt}(\boldsymbol{u})_i$, and the second inequality follows from (D28)–(D31). Similarly, it can be shown that

$$\mathrm{wt}\big(\boldsymbol{e}_X'^f\big) \leqslant 2\big(\mathrm{wt}\big(\boldsymbol{e}_X^1\big) + t_k^{C_1}(XX)\big)$$

$$+ t_k^I + t_k^{C_1}(X) + t_k^{C_2}(X) + t_k^M. \tag{D41}$$

Without loss of generality, we may assume that $\mathrm{wt}(\boldsymbol{e}_X^1) + t_k^{C_1}(XX) \leqslant \mathrm{wt}(\boldsymbol{e}_X^2) + t_k^{C_2}(XX)$. Therefore, we have that

$$\mathrm{wt}\big(\boldsymbol{e}_X'^f\big) \leqslant \mathrm{wt}\big(\boldsymbol{e}_X^1\big) + t_k^{C_1}(XX) + \mathrm{wt}\big(\boldsymbol{e}_X^2\big) + t_k^{C_2}(XX)$$

$$+ t_k^I + t_k^{C_1}(X) + t_k^{C_2}(X) + t_k^M$$

$$\leqslant \mathrm{wt}\big(\boldsymbol{e}_X^1\big) + \mathrm{wt}\big(\boldsymbol{e}_X^2\big) + t_k^I + \big(t_k^{C_1}(X) + t_k^{C_1}(XX)\big)$$

$$+ \big(t_k^{C_2}(X) + t_k^{C_2}(XX)\big) + t_k^M$$

$$\leqslant T_{k-1}^1 + T_{k-1}^2 + t_k^I + t_k^{C_1} + t_k^{C_2} + t_k^M$$

$$\leqslant T_{k-1}^1 + T_{k-1}^2 + t_k, \tag{D42}$$

where the third inequality follows from (D34) and (D26), and the fourth inequality follows from (D25).

We now prove (D37). Using (D13), we get for $\boldsymbol{e}_Z^f$ in (D16),

$$\boldsymbol{e}_Z^f = \big(\boldsymbol{e}_Z^1 \oplus \boldsymbol{e}_Z^{C_1(1)}, \ \boldsymbol{e}_Z^2 \oplus \boldsymbol{e}_Z^{C_1(3)} \oplus \boldsymbol{e}_Z^{C_2(2)}\big). \tag{D43}$$

As $Z \otimes Z$ on the corresponding qubits of $\mathcal{S}_1$ and $\mathcal{S}_2$ is a stabilizer generator, it follows that the following error is equivalent to $\boldsymbol{e}_Z^f$ in (D43):

$$\boldsymbol{e}_Z'^f = \boldsymbol{e}_Z^f \oplus \big(\boldsymbol{e}_Z^{C_1(3)}, \boldsymbol{e}_Z^{C_1(3)}\big)$$

$$= \big(\boldsymbol{e}_Z^1 \oplus \boldsymbol{e}_Z^{C_1(1)} \oplus \boldsymbol{e}_Z^{C_1(3)}, \ \boldsymbol{e}_Z^2 \oplus \boldsymbol{e}_Z^{C_2(2)}\big). \tag{D44}$$

We have

$$\mathrm{wt}\big(\boldsymbol{e}_Z'^f\big) \leqslant \mathrm{wt}\big(\boldsymbol{e}_Z^1\big) + \mathrm{wt}\big(\boldsymbol{e}_Z^2\big) + \mathrm{wt}\big(\boldsymbol{e}_Z^{C_1(1)} \oplus \boldsymbol{e}_Z^{C_1(3)}\big) + \mathrm{wt}\big(\boldsymbol{e}_Z^{C_2(2)}\big)$$

$$\leqslant T_{k-1}^1 + T_{k-1}^2 + t_k^{C_1}(Z) + t_k^{C_2}(Z) + 2t_k^{C_2}(ZZ)$$

$$\leqslant T_{k-1}^1 + T_{k-1}^2 + t_k^{C_1} + t_k^{C_2}$$

$$\leqslant T_{k-1}^1 + T_{k-1}^2 + t_k, \tag{D45}$$

where the first inequality follows from (D44) and using $\mathrm{wt}(\sum_i \boldsymbol{u}_i) \leqslant \sum_i \mathrm{wt}(\boldsymbol{u})_i$, the second inequality follows from (D35) and (D32) and (D33), the third inequality follows from (D27), and finally the fourth inequality follows from (D25). ∎

APPENDIX E: NUMERICAL RESULTS ON FAULT TOLERANT ERROR CORRECTION

In this section we provide details about the methods used to generate numerical results regarding the logical error rates of $\mathcal{Q}_1$ codes, under Steane error correction in conjunction with the proposed measurement-based preparation with error detection. In this context, we also provide simulation results on the rate of successful preparation of $\mathcal{Q}_1$ code states, for the measurement-based preparation with error detection.

We start by presenting first the noise model used to produce errors during the simulation of the measurement-based preparation procedure and the Steane error-correction scheme. Note that we consider the implementation of Pauli $Z \otimes Z$ and Pauli $X \otimes X$ measurements according to circuits in Fig. 10(a) and Fig. 10(b), respectively. However, for the Pauli $X \otimes X$ measurement in Fig. 10(b), we consider the initialization in Pauli Z basis followed by the Hadamard gate as one operation, corresponding to the initialization in Pauli X basis, and similarly, we consider the last Hadamard gate followed by the Pauli X measurement as one operation, corresponding to a Pauli X measurement.

1. Noise model

We need noise models only for the basic components of the procedure, i.e., initialization operations and single-qubit measurements, in either Z or X basis and CNOT gates. We consider the following types of errors, corresponding to the circuit-based depolarizing noise model from [10]. The probability parameter p below, is referred to as the *physical error rate*.

(1) The noisy initialization in Pauli Z basis is equal to perfectly initializing a qubit in a Pauli Z basis state, then applying a Pauli X error on the qubit, with probability p. Similarly, the noisy initialization in Pauli X basis is equal to perfectly initializing a qubit in a Pauli X basis state, then applying a Pauli Z error on the qubit, with probability p.

(2) The noisy Pauli Z measurement is equal to first applying a Pauli X error, with probability p, on the qubit we want to measure, and then applying the perfect Pauli Z measurement. Similarly, the noisy Pauli X measurement is equal to first applying a Pauli Z error, with probability p, and then applying the perfect Pauli X measurement.

(3) The noisy CNOT gate is equal to the perfect CNOT followed by a two-qubit depolarizing channel, with error probability p. Precisely, after the perfect CNOT, any one of the 15 two-qubit Pauli errors $I \otimes X, I \otimes Y, I \otimes Z, X \otimes I, X \otimes X, X \otimes Y, X \otimes Z, Y \otimes I, Y \otimes X, Y \otimes Y, Y \otimes Z, Z \otimes I, Z \otimes X, Z \otimes Y, Z \otimes Z$, may occur with probability $\frac{p}{15}$.

2. Simulation of the preparation procedure

Consider the $\mathcal{Q}_1$ code state $|q_N\rangle_\mathcal{S}$ on the $N = 2^n$ qubit system $\mathcal{S} = \{1, \ldots, N\}$. To prepare $|q_N\rangle_\mathcal{S}$, we first initialize the N qubits in a Pauli Z basis state (using the noisy initialization defined above), and then follow the recursive preparation procedure based on two-qubit Pauli measurements. During the recursive procedure, initialization operations, CNOT gates, and single-qubit measurements are replaced by their noisy versions, and errors generated at some point by noisy operations are propagated throughout the rest of the procedure. If an error
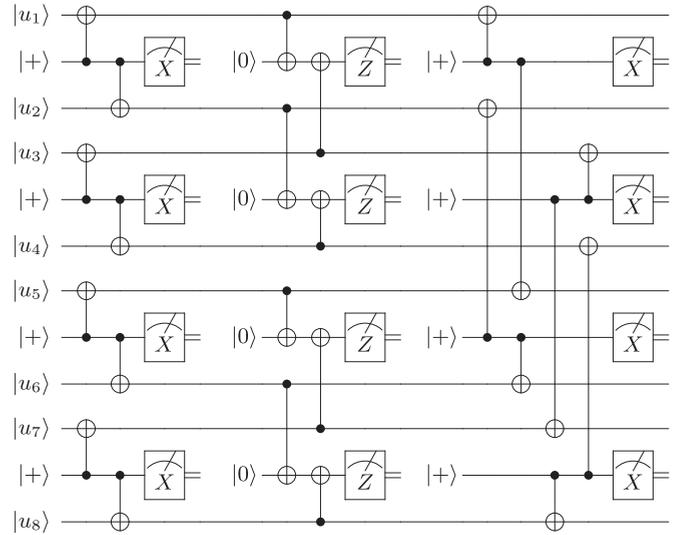
FIG. 15. Measurement-based preparation for the $\mathcal{Q}_1[N = 8, i(n) = 3]$, with Pauli $Z \otimes Z$ and Pauli $X \otimes X$ measurements implemented according to Figs. 10(a) and 10(b). Initialization operations are shown as ket states. For single-qubit measurement operations, the Pauli basis is also indicated. Initialization operations, measurements, and CNOT gates are noisy, according to the assumed circuit-level depolarizing noise model. Note that errors are generated only by the above noisy operations (we do not consider errors that might occur while the qubits are idle). Error detection is performed after each recursion level (one round of measurements of the four ancilla qubits), and the procedure is restarted from the beginning if an error is detected. Error detection after the first level of recursion is useless, hence it is not performed.

is detected at any recursion level (according to the error detection method from Procedure 2), then we discard the whole procedure and restart from the beginning, by initializing the N qubits in a Pauli Z basis state. See also the example in Fig. 15.

As qubits are initialized in Pauli Z basis, we may ignore the first $k, 1 \leqslant k \leqslant n$ levels of recursion in case Pauli $Z \otimes Z$ measurements are needed to be applied consecutively for the first k levels of recursion correspond to applying Pauli $Z \otimes Z$ measurements. This reduces the number of component in the preparation circuit, hence improving the probability that the preparation succeeds.

At the end of recursion, we have the knowledge of the $|\boldsymbol{u}\rangle_{\mathcal{Z}(n)}$ and $|\boldsymbol{v}\rangle_{\mathcal{X}(n)}$, hence the knowledge of prepared $\mathcal{Q}_1$ code state. Further, we also know the total X and Z type errors on the prepared state, which we will use for simulating Steane's error correction in the next sections.

Further, we determine the preparation rate of the measurement-based procedure as follows. We run the preparation procedure $R > 0$ times, and denote by t the number of times the preparation completed (i.e., no error has been detected during the preparation procedure). Then, the preparation rate, denoted by p_{prep}, is defined as follows:

$$p_{\text{prep}} = \lim_{R \to \infty} \frac{t}{R}. \tag{E1}$$

Prepared codes. We consider $\mathcal{Q}_1$ codes of length $N = 16$ and $N = 64$ qubits. We choose the information position i according to the results in Table II (best positions of the
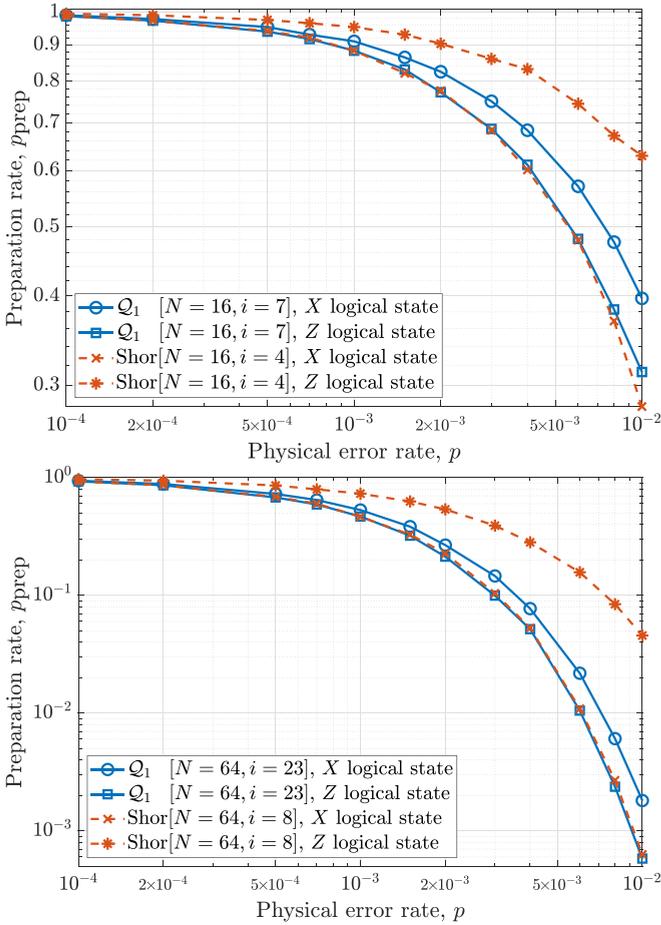
FIG. 16. Preparation rate for the logical X and logical Z code states of $\mathcal{Q}_1$ codes ($N = 16$, $i = 7$) and ($N = 64$, $i = 23$).

corresponding lengths, for sufficiently low error rate), assuming a depolarizing noise model and ignoring correlations between X and Z errors. Thus, for $N = 16$, we take the information position $i = 7$, and for $N = 64$, we take $i = 23$.

The fact that the $\mathcal{Q}_1$ code construction ignores correlations between between X and Z errors is due to the Steane error correction. Indeed, X and Z errors are corrected independently, considering ancilla states prepared in either a logical X basis state $|\widetilde{\boldsymbol{w}'}\rangle_{\mathcal{S}'}$, or a logical Z basis state $|\widetilde{\boldsymbol{w}'}\rangle_{\mathcal{S}'}$, respectively. During the X-error correction step [Fig. 7(a)], Z errors that happened on the ancilla system $\mathcal{S}'$ while preparing $|\widetilde{\boldsymbol{w}'}\rangle_{\mathcal{S}'}$, are copied to the original system $\mathcal{S}$. Similarly, during the Z-error correction step [Fig. 7(b)], X errors that happened on the ancilla system $\mathcal{S}'$ while preparing $|\widetilde{\boldsymbol{w}'}\rangle_{\mathcal{S}'}$, are copied to $\mathcal{S}$. Clearly, these X and Z errors are decorrelated, since they happened during the preparation of different logical states.

Figure 16 shows the preparation rate p_{prep}, for the logical Z and logical X code states of Q_1 and Shor codes of length $N = 16, 64$, with respect to the physical error rate p. Here the total number of runs is $R = 10^5$. We observe that p_{prep} is nonzero for sufficiently low p and it approaches to 1 as p goes to zero, for all the $\mathcal{Q}_1$ code states. Further, for p close to zero, p_{prep} is symmetric, in the sense that it is virtually the same for all code states for a given N. For bigger values of p, the difference in p_{prep} for different code states of the same length is

explained by the fact that for some code states, we have Pauli $Z \otimes Z$ measurements at the first levels of recursion, which may be ignored, hence, reducing the number of components in the preparation circuit, as explained before. For example, for Z logical states of Shor codes $N = 16$, $i = 4$ and $N = 64$, $i = 23$, we may ignore the first two and three levels of recursions, respectively, explaining their higher p_{prep} compared to other code states of the same length. Furthermore, p_{prep} is much lower for codes states of length $N = 64$, compared to that of length $N = 16$, especially at higher values of p. This is also explained by the fact that the preparation circuit, in general, consists of much larger number of components for $N = 64$ than $N = 16$.

3. Monte Carlo-based estimates of the logical error rates

In this section, we provide a practical method to estimate logical error rates of $\mathcal{Q}_1$ codes (given in Fig. 4 and see also Fig. 17), under the Steane's error correction. We consider a $\mathcal{Q}_1$ code of length N, with information position i, and consider the following notation $\mathcal{I} = \{i\}$, $\mathcal{Z} = \{1, \dots, i - 1\}$, $\mathcal{X} = \{i + 1, \dots, N\}$, and $\mathcal{S} = \mathcal{Z} \cup \mathcal{I} \cup \mathcal{X}$.

Logical X error rate. To determine the logical X error rate, we prepare a logical Pauli Z basis code state $|\widetilde{w}\rangle_{\mathcal{S}} = Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |w\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$, $w \in \{0, 1\}$, that we want to protect against X errors. Further, we prepare a logical Pauli X basis code state $|\widetilde{w'}\rangle_{\mathcal{S}'} = Q_N(|\boldsymbol{u'}\rangle_{\mathcal{Z}'} \otimes |\overline{w'}\rangle_{\mathcal{I}'} \otimes |\overline{\boldsymbol{v'}}\rangle_{\mathcal{X}'})$, $w' \in \{0, 1\}$, to be used as the ancilla system for syndrome extraction [see Fig. 7(a)].

The logical X error rate is determined as follows.

(1) *Preparing $\mathcal{Q}_1$ code states:* We first simulate the measurement-based preparation of $|\widetilde{w}\rangle_{\mathcal{S}}$ and $|\widetilde{w'}\rangle_{\mathcal{S}'}$ states, as described before (in case of error detection, we restart the preparation procedure until it completes). After the preparation completes, we know the frozen vectors $\boldsymbol{u}, \boldsymbol{u'} \in \{0, 1\}^{i-1}$, corresponding to the frozen sets $\mathcal{Z}$ and $\mathcal{Z}'$, and the frozen vectors $\boldsymbol{v}, \boldsymbol{v'} \in \{0, 1\}^{N-i}$ corresponding to the frozen sets $\mathcal{X}$ and $\mathcal{X}'$. Further, for $|\widetilde{w}\rangle_{\mathcal{S}}$, we know the logical Z value w, and for $|\widetilde{w'}\rangle_{\mathcal{S}'}$ we know the logical X value w'. Moreover, we also have the final errors $\boldsymbol{e}_X$ and $\boldsymbol{e}'_X$ on systems $\mathcal{S}$ and $\mathcal{S}'$, respectively.

(2) *Generating the syndrome* We generate the syndrome according to Steane's procedure [Fig. 7(a)]. According to Lemma 4, the syndrome $\boldsymbol{m}$ consists of a noisy version of a random codeword of the classical polar code $P(N, \mathcal{Z}, \boldsymbol{u} \oplus \boldsymbol{u'})$. We generate $\boldsymbol{m}$ as the sum of the random codeword from (2.1) and the three error terms from (2.2), below.

(2.1) First, we generate a *random codeword* $P_N(\boldsymbol{u} \oplus \boldsymbol{u'}, a', \boldsymbol{x'})$, by taking random values $a' \in \{0, 1\}$ and $\boldsymbol{x'} \in \{0, 1\}^{N-i}$.

(2.2) We then add to the generated codeword, the following:

The first error term is $\boldsymbol{e}_X \oplus \boldsymbol{e}'_X$, where $\boldsymbol{e}_X$ and $\boldsymbol{e}'_X$ are given in step (1) [see also (B19)].

The second term corresponds to the X error generated on the system $\mathcal{S}'$ during the implementation of the qubitwise CNOT$_{\mathcal{S} \to \mathcal{S}'}$.

The third error term is due to Pauli Z measurements on the system $\mathcal{S}'$.

(a)

(b)
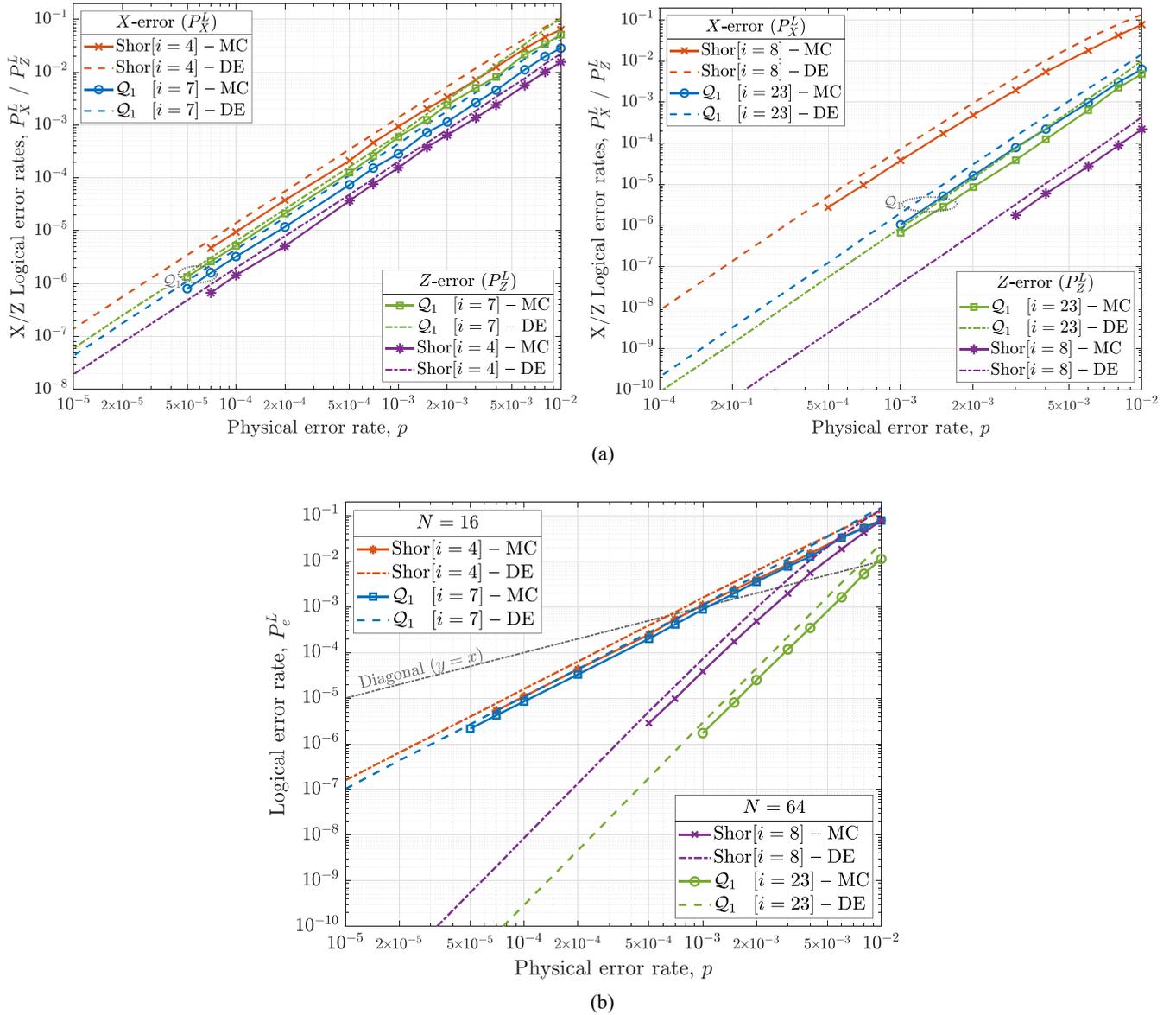
FIG. 17. Numerical results for $\mathcal{Q}_1$ and Shor codes of length $N = 16$ and $N = 64$. (a) Monte-Carlo (MC) and Density-evolution (DE) based estimates of the X/Z logical error rates of $\mathcal{Q}1$ and Shor codes of length $N = 16$ and $N = 64$. (b) Monte-Carlo (MC) and Density-evolution (DE) based estimates of the logical error rate of $\mathcal{Q}1$ and Shor codes of length $N = 16$ and $N = 64$ (here, the logical error rate $P_e^L = P_X^L + P_Z^L - P_X^L P_Z^L$, where P_X^L and P_Z^L are given in (a) above).

Let $\boldsymbol{e}_X^C$ and $\boldsymbol{e}_X^{C'}$ be the error produced by $\text{CNOT}_{\mathcal{S} \to \mathcal{S}'}$ on $\mathcal{S}$ and $\mathcal{S}'$, respectively. Further, let $\boldsymbol{e}_X^{M'}$ is the error produced by Pauli Z measurements on $\mathcal{S}'$. Then we have that

$$\boldsymbol{m} = P_N(\boldsymbol{u} \oplus \boldsymbol{u}', a', \boldsymbol{x}') \oplus \boldsymbol{e}_X^{\text{tot}}, \quad \text{(E2)}$$

where $\boldsymbol{e}_X^{\text{tot}} := \boldsymbol{e}_X \oplus \boldsymbol{e}_X' \oplus \boldsymbol{e}_X^C \oplus \boldsymbol{e}_X^{M'}$ is the total X error that happened on the system $\mathcal{S}'$.

Further, we also update the error on system $\mathcal{S}$, by adding $\boldsymbol{e}_X^C$ to $\boldsymbol{e}_X$, i.e., adding the X error that happened on system $\mathcal{S}$ during the implementation of the qubitwise $\text{CNOT}_{\mathcal{S} \to \mathcal{S}'}$.

(3) *Error correction* Given the frozen value $\boldsymbol{u} \oplus \boldsymbol{u}'$ from step (1), and the extracted syndrome $\boldsymbol{m}$ from step (2), we use

SC decoding [42] to get an estimate $\hat{a}' \in \{0, 1\}$ of a', and then generate an estimate of the total error $\boldsymbol{e}_X^{\text{tot}}$ in (E2), as follows:

$$\hat{\boldsymbol{e}}_X^{\text{tot}} = \boldsymbol{m} \oplus P_N(\boldsymbol{u} \oplus \boldsymbol{u}', \hat{a}', \boldsymbol{0}). \quad \text{(E3)}$$

Note that we do not need to estimate $\boldsymbol{x}'$ here, since the induced logical error corresponds to an X-type stabilizer operator, acting trivially on the code space (see also the discussion after Lemma 4).

We then perform error correction on the state of the system $\mathcal{S}$, and update the X error on $\mathcal{S}$, by adding the estimated total error $\hat{\boldsymbol{e}}_X^{\text{tot}}$. Let $\boldsymbol{e}_X^{\text{corc}}$ be the the error on system $\mathcal{S}$ after correction. From (E2) and (E3), it follows that $\boldsymbol{e}_X^{\text{corc}}$ is equivalent to the following error:

$$\boldsymbol{e}_X^{\text{corc}} \equiv \boldsymbol{e}_X' \oplus \boldsymbol{e}_X^C \oplus \boldsymbol{e}_X^{C'} \oplus \boldsymbol{e}_X^{M'} \oplus P_N(\boldsymbol{0}, a' \oplus \hat{a}', \boldsymbol{0}, \boldsymbol{0}). \quad \text{(E4)}$$

(4) *Guessing the logical value* The error correction is successful if we can successfully recover the logical Z value from the state of the system $\mathcal{S}$, after error correction.

To get the logical Z value, we need to perform single-qubit Pauli Z measurements on system $\mathcal{S}$, and then estimate the logical value from the measurement outcome.

It can be seen that the measurement outcome of Pauli Z measurements gives a noisy version of a random codeword of the classical polar code $P(N, \mathcal{Z}, \boldsymbol{u} \oplus \boldsymbol{u}')$, as follows:

$$\boldsymbol{m} = P_N(\boldsymbol{u} \oplus \boldsymbol{u}', w, \boldsymbol{x}) \oplus \boldsymbol{e}_X^{\text{corc}} \oplus \boldsymbol{e}_X^M, \qquad \text{(E5)}$$

where w is the logical Z value corresponding to the initial state on the system $\mathcal{S}$, $\boldsymbol{x}$ is a random vector, $\boldsymbol{e}_X^{\text{corc}}$ is the X error on the system $\mathcal{S}$ after the error correction from (E4), and $\boldsymbol{e}_X^M$ is the error caused by the single-qubit Pauli Z measurements on system $\mathcal{S}$.

From the frozen vector $\boldsymbol{u} \oplus \boldsymbol{u}'$ and the noisy codeword $\boldsymbol{m}$ in (E5), we generate an estimate $\hat{w}$ of w, using the SC decoding. If $\hat{w} \neq w$, we report a decoding failure, otherwise the decoding succeeds.

We run the above steps (1)–(4), until we report $f > 0$ decoding failures. Let R be the number of runs for f decoding failures, then the logical X error rate, denoted by P_X^L, is computed as follows:

$$P_X^L = \frac{f}{R}. \qquad \text{(E6)}$$

For our numerical simulations, the value of f varies between 50 to 200, depending on the physical error rate p of our noise model.

Logical Z error rate. To determine the logical Z error rate, we consider a logical Pauli X basis code state $|\widetilde{w}\rangle_{\mathcal{S}} = Q_N(|\boldsymbol{u}\rangle_{\mathcal{Z}} \otimes |\overline{w}\rangle_{\mathcal{I}} \otimes |\overline{\boldsymbol{v}}\rangle_{\mathcal{X}})$, $w \in \{0, 1\}$, that we want to protect against Z errors. Further, we consider a logical Pauli Z basis code state $|\widetilde{w'}\rangle_{\mathcal{S}'} = Q_N(|\boldsymbol{u}'\rangle_{\mathcal{Z}'} \otimes |w'\rangle_{\mathcal{I}'} \otimes |\overline{\boldsymbol{v}'}\rangle_{\mathcal{X}'})$, $w' \in \{0, 1\}$, to be used as the ancilla system for syndrome extraction [Fig. 7(a)]. The logical Z error rate is then determined similarly to the above description for logical X error rate, while inverting X and Z bases, and using Lemma 5 instead of Lemma 4. The logical Z error rate is denoted by P_Z^L.

Finally, the logical error rate (accounting for both X and Z errors), denoted by P_e^L, is given as follows:

$$P_e^L = P_X^L + P_Z^L - P_X^L P_Z^L. \qquad \text{(E7)}$$

4. Density-evolution-based estimates of the logical error rates

To reliably estimate the logical error rate value, the Monte Carlo method described in Sec. 3 requires an increasingly large number of simulations as the logical error rate decreases. Hence, as p decreases, this requires increasingly more computational time (or resources) and becomes practically unfeasible for small values of p. In this section we provide a theoretical method to estimate the logical error rate, based on density evolution [24] (see also Fig. 17).

Consider the Steane's error correction for X errors from Sec. 3. Note that it involves two steps of decoding; the first during Step 3 for error correction and the second during Step 4 for guessing the logical value. Each failure in decoding introduces a logical X error, hence, the logical value is incorrectly determined if and only if one of the two decoders fail.

For a given realization of errors [i.e., e_X^{tot} in (E2), or $\boldsymbol{e}_X^{\text{corc}} \oplus \boldsymbol{e}_X^M$ in (E5)], the SC decoding works by propagating the corresponding log-likelihood ratio (LLR) values throughout the polar encoding graph (from the right-hand side of the graph, corresponding to the encoded information, to the left-hand side of the graph, corresponding to the uncoded information; see also footnote [42]). Rather than propagating LLR values for a given sample (realization of errors), the density evolution method propagates their probability density functions, thus averaging over all the sample space. To determine the probability distribution of the input LLRs, one needs to estimate the input error probability of the decoder [i.e., $P(e_X^{\text{tot}}(i) = 1]$ for the SC decoding in Step 3, or $P(\boldsymbol{e}_X^{\text{corc}}(i) \oplus \boldsymbol{e}_X^M(i) = 1)$ for the SC decoding in Step 4.

Accordingly, we determine the logical X error rate in the following two steps:

(1) *Input error probabilities of decoders* To determine the input error probabilities of the decoders in Steps 3 and 4, we need to generate statistics for the error terms e_X^{tot} in (E2) and $\boldsymbol{e}_X^{\text{corc}} \oplus \boldsymbol{e}_X^M$ in (E5). In particular, we need to estimate the output X error probabilities of the Z and X logical states, by numerical simulation. This is done as follows.

For a given physical error rate p, we run the measurement-based preparation with the error detection for logical Z and X states until we have R successful preparations for each one of them [43]. Let $\boldsymbol{e}_X^r, \boldsymbol{e}_X'^r \in \{0, 1\}^N$, $1 \leqslant r \leqslant R$, be the X errors corresponding to the rth successful preparation of the logical Z and X states, respectively. Then, the average output X error rate for Z and X logical states are estimated as follows:

$$p_X^{\text{prep}} = \frac{1}{RN} \sum_{r=1}^R \text{wt}(\boldsymbol{e}_X^r), \qquad \text{(E8)}$$

$$p_X'^{\text{prep}} = \frac{1}{RN} \sum_{r=1}^R \text{wt}(\boldsymbol{e}_X'^r). \qquad \text{(E9)}$$

Let $p_X^{\text{in}_1}$ and $p_X^{\text{in}_2}$ be the input error rate of the first and second decoders, respectively. From (E2), we have that

$$p_X^{\text{in}_1} = 1 - \left(1 - p_X^{\text{prep}}\right)\left(1 - p_X'^{\text{prep}}\right)\left(1 - \frac{8p}{15}\right)(1 - p). \quad \text{(E10)}$$

Further, for the sake of simplicity, we compute the input error rate of the second decoder, assuming that the first decoder has succeeded. Then, from (E4) and (E5), we have that

$$p_X^{\text{in}_2} = 1 - \left(1 - p_X'^{\text{prep}}\right)\left(1 - \frac{8p}{15}\right)(1 - p)^2. \qquad \text{(E11)}$$

Note that as long as the first decoder succeeds with a probability close to one, (E11) approximates well the input error rate of the second decoder.

(2) *X logical error rate* After obtaining the input error probabilities $p_X^{\text{in}_1}$ and $p_X^{\text{in}_2}$, we compute output error rates of the decoders [44], using density evolution. Let $P_X^{\text{out}_1}$ and $P_X^{\text{out}_2}$ be the output error probabilities of the first and second decoders, respectively. Then, we determine the X logical error rate of the Steane's error correction as follows:

$$P_X^L = 1 - \left(\left(1 - p_X^{\text{out}_1}\right)\left(1 - p_X^{\text{out}_2}\right) + p_X^{\text{out}_1} p_X^{\text{out}_2}\right). \qquad \text{(E12)}$$

We may similarly determine the Z input error probabilites for the first and second decoder, estimate their output

probabilities using density evolution, and then determine P_Z^L, i.e., the Z logical error rate of the Steane's error correction. Finally, using P_X^L and P_Z^L, we may determine the logical error rate P_e^L as in (E7).

Numerical results for the logical error rates of $\mathcal{Q}_1(N = 16, i = 7)$ and $\mathcal{Q}_1(N = 64, i = 23)$ codes, based on either Monte Carlo simulation or density evolution, are provided in Fig. 17.

---

[1] J. Preskill, Fault-tolerant quantum computation, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, T. Spiller, and S. Popescu (World Scientific, Bristol, UK, 1998), pp. 213–269.

[2] D. Gottesman, An introduction to quantum error correction and fault-tolerant quantum computation, in *Proceedings of the Symposia in Applied Mathematics of Quantum Information Science and Its Contributions to Mathematics*, edited by S. J. Lomonaco, Jr. (American Mathematical Society, Washington, DC, 2010), Vol. 68, pp. 13–58.

[3] E. Arikan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, IEEE Trans. Inf. Theory **55**, 3051 (2009).

[4] J. M. Renes, F. Dupuis, and R. Renner, Efficient polar coding of quantum information, Phys. Rev. Lett. **109**, 050504 (2012).

[5] M. M. Wilde and S. Guha, Polar codes for degradable quantum channels, IEEE Trans. Inf. Theory **59**, 4718 (2013).

[6] J. M. Renes and M. M. Wilde, Polar codes for private and quantum communication over arbitrary channels, IEEE Trans. Inf. Theory **60**, 3090 (2014).

[7] F. Dupuis, A. Goswami, M. Mhalla, and V. Savin, Polarization of quantum channels using Clifford-based channel combining, IEEE Trans. Inf. Theory **67**, 2857 (2021).

[8] A. Holmes, M. R. Jokar, G. Pasandi, Y. Ding, M. Pedram, and F. T. Chong, NISQ+: Boosting quantum computing power by approximating quantum error correction, in *Proceedings of the 2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (IEEE, Piscataway, NJ, 2020), pp. 556–569.

[9] A. Yu. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. **303**, 2 (2003).

[10] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation, Phys. Rev. A **86**, 032324 (2012).

[11] A. J. Landahl, J. T. Anderson, and P. R. Rice, Fault-tolerant quantum computing with color codes, arXiv:1108.5738.

[12] J.-P. Tillich and G. Zémor, Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength, IEEE Trans. Inf. Theory **60**, 1193 (2013).

[13] D. Gottesman, Fault-tolerant quantum computation with constant overhead, Quantum Inf. Comput. **14**, 1338 (2014).

[14] P. Panteleev and G. Kalachev, Asymptotically good quantum and locally testable classical LDPC codes, in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing* (ACM Press, New York, NY, 2022), pp. 375–388.

[15] A. Leverrier and G. Zémor, Quantum Tanner codes, in *Proceedings of the 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Washington, DC, 2022), pp. 872–883.

[16] A. Krishna and J.-P. Tillich, Magic state distillation with punctured polar codes, arXiv:1811.03112.

[17] Measurement repetition can be avoided by using codes with the single-shot error correction property [45,46], which allows

correcting physical errors using only a single round of noisy measurements, e.g., 3D/4D toric codes, 3D/4D hypergraph product codes, 4D hyperbolic codes, and quantum expander codes.

[18] Note that the error detection gadget is a built-in feature of the proposed preparation procedure, with errors being detected on a block of measurement outcomes, as opposed to an external gadget detecting errors on individual measurement outcomes, e.g., the flag-qubit approach [47].

[19] A. M. Steane, Active stabilization, quantum computation, and quantum state synthesis, Phys. Rev. Lett. **78**, 2252 (1997).

[20] A. M. Steane, Fast fault-tolerant filtering of quantum codewords, arXiv:quant-ph/0202036.

[21] Virtual channels are part of polar code construction, as explained in Appendixes A and B.

[22] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A **52**, R2493(R) (1995).

[23] D. Bacon, Operator quantum error-correcting subsystems for self-correcting quantum memories, Phys. Rev. A **73**, 012340 (2006).

[24] I. Tal and A. Vardy, How to construct polar codes, IEEE Trans. Inf. Theory **59**, 6562 (2013).

[25] K. M. Svore, A. W. Cross, I. L. Chuang, and A. V. Aho, A flow-map model for analyzing pseudothresholds in fault-tolerant quantum computing, Quantum Inf. Comput. **6**, 193 (2006).

[26] Yu Tomita and K. M. Svore, Low-distance surface codes under realistic quantum noise, Phys. Rev. A **90**, 062320 (2014).

[27] T. Tansuwannont, B. Pato, and K. R. Brown, Adaptive syndrome measurements for Shor-style error correction, Quantum **7**, 1075 (2023).

[28] C. Chamberland, A. Kubica, T. J. Yoder, and G. Zhu, Triangular color codes on trivalent graphs with flag qubits, New J. Phys. **22**, 023019 (2020).

[29] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error, in *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing* (ACM Press, New York, NY, 1997), pp. 176–188.

[30] P. Aliferis, D. Gottesman, and J. Preskill, Quantum accuracy threshold for concatenated distance-3 codes, Quantum Inf. Comput. **6**, 97 (2006).

[31] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, Elucidating reaction mechanisms on quantum computers, Proc. Natl. Acad. Sci. USA **114**, 7555 (2017).

[32] J. O'Gorman and E. T. Campbell, Quantum computation with realistic magic-state factories, Phys. Rev. A **95**, 032338 (2017).

[33] D. Litinski, Magic state distillation: Not as costly as you think, Quantum **3**, 205 (2019).

[34] C. Ryan-Anderson, J. G. Bohnet, K. Lee, D. Gresh, A. Hankin, J. P. Gaebler, D. Francois, A. Chernoguzov, D. Lucchetti, N. C. Brown *et al.*, Realization of real-time fault-tolerant quantum error correction, Phys. Rev. X **11**, 041058 (2021).

[35] P. Murali, D. M. Debroy, K. R. Brown, and M. Martonosi, Architecting noisy intermediate-scale trapped ion quantum computers, in *Proceedings of the 2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (IEEE, Piscataway, NJ, 2020), pp. 529–542.

[36] A. J. Sigillito, M. J. Gullans, L. F. Edge, M. Borselli, and J. R. Petta, Coherent transfer of quantum information in a silicon double quantum dot using resonant swap gates, npj Quantum Inf. **5**, 110 (2019).

[37] H. Asai, S. Iizuka, T. Mogami, J. Hattori, K. Fukuda, T. Ikegami, K. Kato, H. Oka, and T. Mori, Device structure and fabrication process for silicon spin qubit realizing process-variation-robust swap gate operation, Jpn. J. Appl. Phys. **62**, SC1088 (2023).

[38] B. Jadot, P.-A. Mortemousque, E. Chanrion, V. Thiney, A. Ludwig, A. D. Wieck, M. Urdampilleta, C. Bäuerle, and T. Meunier, Distant spin entanglement via fast and coherent electron shuttling, Nat. Nanotechnol. **16**, 570 (2021).

[39] I. Seidler, T. Struck, R. Xue, N. Focke, S. Trellenkamp, H. Bluhm, and L. R. Schreiber, Conveyor-mode single-electron shuttling in Si/SiGe for a scalable quantum computing architecture, npj Quantum Inf. **8**, 100 (2022).

[40] J. M. Boter, J. P. Dehollain, J. P. G. Van Dijk, Y. Xu, T. Hensgens, R. Versluis, H. W. L. Naus, J. S. Clarke, M. Veldhorst, F. Sebastiano *et al.*, Spiderweb array: A sparse spin-qubit array, Phys. Rev. Appl. **18**, 024053 (2022).

[41] Strictly speaking, the classical information obtained at step (3) is not an error syndrome, but an error corrupted version of a random codeword (of course, if needed, one may classically compute the corresponding error syndrome).

[42] The SC decoding assumes that e_X^{tot} is a vector of independent and identically distributed Bernoulli variables, i.e., $P(e_X^{\text{tot}}(i) = 1) = p_X^{\text{in}}$, for all $i = 1, \ldots, N$, and for some probability value $p_X^{\text{in}} \in (0, 1)$, which is referred to as the *input error probability of the decoder*. While the "belief-propagation" variant of the SC decoding needs an estimate of p_X^{in} (in order to calculate the input log-likelihood ratios of the decoder, $\text{LLR}(i) := (-1)^{m(i)} \log((1 - p_X^{\text{in}})/p_X^{\text{in}}), \forall i = 1, \ldots, N$), here we use the so-called "min-sum" approximation of the SC decoding, which does not need such an estimate (in this case, the input log-likelihood ratio values of the decoder may be simply set to $\text{LLR}(i) := (-1)^{m(i)}, \forall i = 1, \ldots, N$).

[43] In our numerical simulation, we have taken $R = 100/p$.

[44] Precisely, we determine the probability distributions of the input LLRs of the decoder, propagate these probability distributions numerically throughout the polar encoding graph, then take the corresponding output error rates.

[45] H. Bombín, Single-shot fault-tolerant quantum error correction, Phys. Rev. X **5**, 031043 (2015).

[46] E. T. Campbell, A theory of single-shot error correction for adversarial noise, Quantum Sci. Technol. **4**, 025006 (2019).

[47] R. Chao and B. W. Reichardt, Quantum error correction with only two extra qubits, Phys. Rev. Lett. **121**, 050502 (2018).

Correction: Minor errors in text in the second and fourth sentences in the penultimate paragraph of Sec. III have been fixed.