GHZ Distillation using Quantum LDPC Codes

Narayanan Rengaswamy
Department of Electrical and Computer Engineering
University of Arizona
Tucson, Arizona 85721, USA
E-mail: narayananr@arizona.edu

Ankur Raina
Department of Electrical Engineering and Computer Science
Indian Institute of Science Education and Research
Bhopal, Madhya Pradesh 462066, India
E-mail: ankur@iiserb.ac.in

Nithin Raveendran
Department of Electrical and Computer Engineering
University of Arizona
Tucson, Arizona 85721, USA
E-mail: nithin@email.arizona.edu

Bane Vasić
Department of Electrical and Computer Engineering
University of Arizona
Tucson, Arizona 85721, USA
E-mail: vasic@ece.arizona.edu

2023 12th International Symposium on Topics in Coding (ISTC) | 979-8-3503-2611-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISTC57237.2023.10273456

***Abstract*—Entanglement distribution is a critical task in quantum networks. Since the distributed entanglement can suffer from noise in the channel, it is necessary to develop methods that distill higher quality entanglement from the shared noisy entangled states. In this work, we propose a protocol to distill multi-qubit Greenberger-Horne-Zeilinger (GHZ) states among the nodes of a network using quantum error correcting codes. The method builds upon a Bell state distillation protocol by Wilde *et al.* (2007) that we recently generalized to 3-qubit GHZ states. The key technical result that enables our protocol shows how measuring a Pauli operator, or in general a set of code stabilizers, on one subsystem of a multipartite GHZ state affects the other subsystems. The design and analysis of the protocol is driven by the stabilizer formalism for measurements, and we provide discussions to elucidate the steps of the protocol. A similar approach can be applied to distill other multipartite entangled states as long as they are stabilizer states.**

***Index Terms*—Quantum networks, stabilizer codes, GHZ states, stabilizer formalism, entanglement distillation**

I. Introduction

QUANTUM networks are envisaged to interconnect multiple quantum-enabled nodes that are physically far apart. Compared to classical networks, a key advantage in quantum networks is the possibility of entangling different subsets of nodes and using this preshared entanglement as a resource in network protocols. Since nodes can be very far from each other, quantum repeaters will have to be inserted into the network for mitigating the severe losses in direct node-to-node channels [1], [2]. Moreover, each of these nodes could be built using different quantum technologies, such as trapped-ions or superconducting qubits, but they must be able to interface with the network. Hence, we need to develop methods for distributing high-quality entanglement between nodes through repeaters, and these methods should in principle be technology-agnostic. Typical entanglement distribution schemes are heralded and hence inefficient. Since long-term repeater architectures are designed to include quantum error correction (QEC) capabilities [3], it is pertinent to investigate entanglement distribution schemes that leverage QEC.

The idea of using quantum error correcting codes (QECCs) to distill entangled states was first proposed by Bennett *et al.* in their seminal paper on mixed state entanglement and QEC [4]. In their approach, Alice locally produces k perfect Bell pairs and then uses a QECC to protect the k halves from all pairs that are to be transmitted to Bob. The transmission happens through multiple uses of quantum teleportation, where the preshared entangled resources between Alice and Bob are noisy. Hence, the k halves are explicitly encoded by Alice using an $[\![n, k]\!]$ QECC, then transmitted via quantum teleportation, and finally error corrected and decoded by Bob.

In 2007, Wilde *et al.* [5] used a different approach to distill Bell pairs via QEC (see Fig. 1). Here, Alice generates n perfect Bell pairs and sends one half of each pair to Bob through a noisy channel. Then, she picks an $[\![n, k]\!]$ stabilizer code [6], [7] and measures the $(n-k)$ stabilizers on her n qubits (from all pairs). Due to a well-known "matrix transpose" property of Bell states (3), besides projecting her qubits onto the code subspace (modulo some Pauli corrections), her measurements *simultaneously* project Bob's qubits to an equivalent code's subspace. Alice classically communicates her syndrome to Bob, which he combines with his own syndrome to correct errors on his qubits. If Bob's error correction succeeds, then Alice's and Bob's qubits hold k perfect Bell pairs in the k pairs of logical qubits, which can be transformed into physical Bell pairs by inversion of the encoding unitary on both parties. Therefore, this protocol does not have an explicit encoding step as in the Bennett *et al.* protocol, and Alice's measurement induces the encoding. Note that there are no errors on her qubits that the syndrome measurement is supposed to correct.

While the protocol is clear, it is not obvious why the k logical qubits form logical Bell pairs just before the decoding

This work is funded by the NSF Center for Quantum Networks (CQN) under the grant NSF-ERC 1941583, partly by NASA through the Jet Propulsion Laboratory's SURP program, and also by the NSF grants CIF-1855879, CIF-2106189, CCF-2100013 and ECCS/CCSS-2027844. Bane Vasić has disclosed an outside interest in his startup company Codelucida to the University of Arizona. Conflicts of interest resulting from this interest are being managed by The University of Arizona in accordance with its policies.

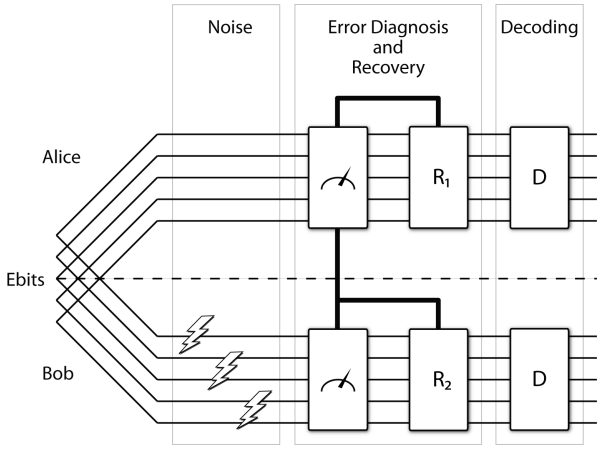

Fig. 1: The QEC based protocol by Wilde *et al.* [5] to distill Bell pairs between Alice and Bob. Figure taken from [5].

(unencoding) step. After introducing some background and notation in Section II, we use the stabilizer formalism for measurements [8] to briefly clarify the reason for this phenomenon. We refer the interested reader to [9] for a detailed discussion using an explicit example. Then, we extend the protocol beyond Bell states, where we distill ℓ-qubit GHZ states using stabilizer codes. In order to develop this protocol, we establish a technical result that shows how stabilizer measurements on one subsystem of a GHZ state produces a joint code on all the other subsystems. We had proven this result and developed the protocol for $\ell = 3$ in [9], and here we generalize to any ℓ.

Our work is well compatible with recent work on quantum repeaters that exploit QEC. In [3], the authors considered a hybrid repeater scheme where the physical qubits actually belong to the subspace of the Gottesman-Kitaev-Preskill (GKP) code, and there is an outer stabilizer code imposed on these GKP qubits. Using the $[\![4,2,2]\!]$ code and the $[\![7,1,3]\!]$ Steane code as examples, they showed that the GKP analog information from the inner round of error correction can help correct more errors than these outer codes can normally correct. Thus, our QEC based entanglement distillation protocol can be implemented in such repeater architectures. Recently, quantum low-density parity-check (QLDPC) codes with linearly scaling rate and distance have been constructed [10]–[12], and the advantages of concatenating the GKP code with QLDPC codes has been demonstrated [13]. Hence, employing concatenated QLDPC-GKP codes in our protocol could lead to high-rate high-output-fidelity entanglement distillation in quantum networks.

II. Background and Notation

Let n denote the number of qubits in a quantum system. Given binary (row) vectors $a, b \in \mathbb{F}_2^n$, we will denote an n-qubit Hermitian Pauli matrix by $E(a,b)$, where $a_i = 1$ (resp. $b_i = 1$) indicates Pauli X (resp. Z) on qubit i, $a_i = b_i = 1$ indicates Pauli Y on qubit i, and $a_i = b_i = 0$ indicates identity on qubit i. The *weight* of a Pauli is the number of qubits on which it acts non-trivially. For example, for $n = 3$ qubits, $E([1,0,1],[0,1,1]) = X \otimes Z \otimes Y$ and its weight is 3. Since $E(a,b)$ is Hermitian and unitary, it has eigenvalues ± 1 and $E(a,b)^2 = I_N$, where $N \coloneqq 2^n$. The n-qubit Pauli group is

$$\mathcal{P}_n \coloneqq \{\imath^\kappa E(a,b),\ a,b \in \mathbb{F}_2^n,\ \kappa \in \mathbb{Z}_4 = \{0,1,2,3\}\}, \quad (1)$$

where $\imath \coloneqq \sqrt{-1}$. Two Paulis $E(a,b)$ and $E(c,d)$ commute or anticommute depending on the *symplectic inner product* $\langle [a,b],[c,d]\rangle_{\mathrm{s}} \coloneqq ad^T + bc^T \pmod 2$: if the inner product is 0 then they commute, if it is 1 then they anticommute.

An r-dimensional *stabilizer group* $\mathcal{S}$ is a commutative subgroup of $\mathcal{P}_n$ that is generated by r commuting Hermitian Paulis such that $-I_N \notin \mathcal{S}$. The common $+1$ eigenspace of (the elements of) $\mathcal{S}$ is called an $[\![n,k,d]\!]$ *stabilizer code* $\mathcal{Q}(\mathcal{S})$, where $k \coloneqq n - r$ and d is the minimum weight of any Pauli $E(a,b) \notin \mathcal{S}$ that commutes with every element of $\mathcal{S}$ [6], [7]. If the generators of $\mathcal{S}$ are $\{\varepsilon_i E(a_i,b_i),\ i = 1,2,\ldots,r\}$, where $\varepsilon_i \in \{\pm 1\}$, then the projector onto the subspace $\mathcal{Q}(\mathcal{S})$ is

$$\Pi_{\mathcal{S}} = \prod_{i=1}^{r} \frac{(I_N + \varepsilon_i E(a_i,b_i))}{2}. \quad (2)$$

When $r = n$, $\mathcal{S}$ is said to be a *maximal* stabilizer group where $\mathcal{Q}(\mathcal{S})$ is a unique state $|\psi(\mathcal{S})\rangle$ up to an unimportant global phase. Such a state is called a *stabilizer state*. Given a stabilizer state, the *stabilizer formalism* [8] provides a recipe to update $\mathcal{S}$ when a Pauli measurement is performed on the state. Let $\nu E(c,d)$ be measured on the state to obtain a result $\mu \in \{\pm 1\}$. Then, one of the following is applicable:

1) If $\langle [a_i,b_i],[c,d]\rangle_{\mathrm{s}} = 0$ for all $i \in \{1,\ldots,r\}$, then $\mathcal{S}$ remains unchanged because $\mu\nu E(c,d) \in \mathcal{S}$ already.
2) If $\langle [a_i,b_i],[c,d]\rangle_{\mathrm{s}} = 1$ for exactly one $i \in \{1,\ldots,r\}$, then replace $\varepsilon_i E(a_i,b_i)$ with $\mu\nu E(c,d)$.
3) If $\langle [a_i,b_i],[c,d]\rangle_{\mathrm{s}} = 1$ for $i \in A \subseteq \{1,\ldots,r\}$, then replace $\varepsilon_j E(a_j,b_j)$ with $\mu\nu E(c,d)$ for one $j \in A$, and for every other $i \in A$, replace the stabilizer with $\varepsilon_i E(a_i,b_i)\cdot\varepsilon_j E(a_j,b_j)$ (which commutes with $E(c,d)$). See [9] for details on binary arithmetic for Paulis.

Let $|\Phi_n^+\rangle_{\mathrm{AB}} \coloneqq \left(\frac{|00\rangle_{\mathrm{AB}} + |11\rangle_{\mathrm{AB}}}{\sqrt{2}}\right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle_{\mathrm{A}} |x\rangle_{\mathrm{B}}$. It is well-known that this state is stabilized by $\mathcal{S}(|\Phi_n^+\rangle_{\mathrm{AB}}) = \langle X_{\mathrm{A}} X_{\mathrm{B}}, Z_{\mathrm{A}} Z_{\mathrm{B}}\rangle^{\otimes n}$. It is also known that $|\Phi_n^+\rangle_{\mathrm{AB}}$ satisfies the following matrix identity for any matrix M [4], [5]:

$$(M_{\mathrm{A}} \otimes I_{\mathrm{B}}) \left|\Phi_n^+\right\rangle_{\mathrm{AB}} = (I_{\mathrm{A}} \otimes M_{\mathrm{B}}^T) \left|\Phi^+\right\rangle_{\mathrm{AB}}. \quad (3)$$

When M is a projector, one can replace M by M^2 and apply this property to only one M to see that the operator on the right hand side becomes $M_{\mathrm{A}} \otimes M_{\mathrm{B}}^T$. Thus, projecting Alice's qubits by M induces a *simultaneous* projection of Bob's qubits by M^T. In particular, when $M = \Pi_{\mathcal{S}}$, which is induced by measuring the stabilizer generators of $\mathcal{S}$ on Alice's qubits, Bob's qubits are projected onto the subspace of the "transpose" code whose projector is $\Pi_{\mathcal{S}}^T$. By transposing (2), it is clear that the stabilizer generators for this transpose code are $\{\varepsilon_i E(a_i,b_i)^T\}$, where $E(a_i,b_i)^T = (-1)^{a_i b_i^T} E(a_i,b_i)$ because $Y^T = -Y$ but X and Z are symmetric.

III. Code based Entanglement Distillation

A. Bell Pair Distillation using Stabilizer Codes

We begin by using the stabilizer formalism to explain why, before the decoding step, the logical qubits of Alice and Bob form k Bell pairs in the distillation protocol by Wilde *et al.* [5] that we discussed in the Introduction.

Initially, Alice generates the $2n$-qubit stabilizer state $|\Phi_n^+\rangle_{\mathrm{AB}}$, which can be simulated by creating the stabilizer group $\mathcal{S}(|\Phi_n^+\rangle_{\mathrm{AB}})$. This group has $2n$ commuting generators, two for each Bell pair. Now, Alice chooses some $[\![n, k, d]\!]$ stabilizer code $\mathcal{Q}(\mathcal{S})$ and measures the $r = n - k$ stabilizer generators of $\mathcal{S}$ on qubits marked 'A'. We can use the stabilizer formalism in Section II to evolve the stabilizer group through each measurement. Crucially, the rules of the stabilizer formalism guarantee that after each step the new set of generators still mutually commute. Hence, after r steps, we will have Alice's code stabilizers belonging in the evolved group. Due to the Bell matrix identity in (3) (for projector $\Pi_{\mathcal{S}}$), we know that Bob's qubits would have been simultaneously projected onto the subspace of the "transpose" code. Thus, Bob's code stabilizers must also belong to the evolved group, and we have $2r = 2(n - k)$ code stabilizer generators in total.

The Pauli error from the channel can only affect the signs of these stabilizers, which are assumed to be fixed later by Bob's decoder. The remaining $2k$ generators of the evolved group mutually commute and also commute with all these code stabilizers. Each of these $2k$ operators must act both on Alice's and Bob's qubits, and since they are not themselves stabilizers of the code, the Alice (resp. Bob) component of each operator must be a logical operator for Alice's (resp. Bob's) code. With some thought, one can appropriately define logical X and logical Z operators for the codes of Alice and Bob to conclude that these $2k$ operators correspond to logical $X_{\mathrm{A}}X_{\mathrm{B}}$ and logical $Z_{\mathrm{A}}Z_{\mathrm{B}}$ for the k pairs of logical qubits. Hence, in the Wilde *et al.* protocol, this is why the logical qubits of Alice and Bob form logical Bell pairs just before the decoding step. When the encoding unitaries are inverted on both parties, these logical Bell pairs are converted into physical Bell pairs that are of higher quality than the n noisy Bell pairs initially shared between Alice and Bob. For a more detailed discussion of this phenomenon, see [9].

B. Multi-Qubit GHZ Distillation

Given this understanding of the Bell pair distillation protocol, it is natural to extend it to distill ℓ-qubit GHZ states, $\left|\mathrm{GHZ}^{\ell}\right\rangle = \frac{(|00\cdots0\rangle+|11\cdots1\rangle)}{\sqrt{2}}$. The case of $\ell = 3$, the standard GHZ state, was recently solved in [9]. Here, we extend the protocol to any $\ell > 3$ and use $\ell = 4$ for simplicity. Unless we include the superscript ℓ, $|\mathrm{GHZ}\rangle$ denotes the 4-qubit state.

Consider n copies of the 4-qubit GHZ state where the 4 qubits of each copy are marked 'A', 'B', 'C', and 'D'. Similar to the case of the standard Bell state, the qubits can be rearranged to rewrite the joint state as

$$|\mathrm{GHZ}_n\rangle_{\mathrm{ABCD}} = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathbb{F}_2^n} |x\rangle_{\mathrm{A}} |x\rangle_{\mathrm{B}} |x\rangle_{\mathrm{C}} |x\rangle_{\mathrm{D}} . \tag{4}$$

Each GHZ state has the following associated stabilizer group:

$$\mathcal{S}_{\mathrm{GHZ}} = \langle Z_{\mathrm{A}}Z_{\mathrm{B}}I_{\mathrm{C}}I_{\mathrm{D}},\ I_{\mathrm{A}}Z_{\mathrm{B}}Z_{\mathrm{C}}I_{\mathrm{D}},\ I_{\mathrm{A}}I_{\mathrm{B}}Z_{\mathrm{C}}Z_{\mathrm{D}},\ X_{\mathrm{A}}X_{\mathrm{B}}X_{\mathrm{C}}X_{\mathrm{D}}\rangle.$$

Hence, the stabilizers for $|\mathrm{GHZ}_n\rangle_{\mathrm{ABCD}}$ are $\mathcal{S}_{\mathrm{GHZ}}^{\otimes n}$. Next, we need to generalize the Bell matrix identity (3) to the GHZ case and identify how Pauli measurements on one subsystem affect the other subsystems. We begin with a simple lemma.

Lemma 1. *Let $M = \sum_{x,y \in \mathbb{F}_2^n} M_{xy} |x\rangle \langle y| \in \mathbb{C}^{2^n \times 2^n}$ be any matrix acting on qubits 'A'. Then,*

$$(M_{A_1} \otimes I) \left|GHZ_n^{\ell}\right\rangle_{A_1 \cdots A_\ell} = \left(I_{A_1} \otimes \left(\widehat{M^T}\right)\right) \left|GHZ_n^{\ell}\right\rangle_{A_1 \cdots A_\ell} ;$$

$$\textit{'GHZ-map'}\colon M \mapsto \widehat{M} \coloneqq \sum_{x,y \in \mathbb{F}_2^n} M_{xy} |x\rangle \langle y|^{\otimes(\ell-1)} .$$

Proof: Similar to the Bell state case, we calculate

$$\begin{aligned} M_{\mathrm{A}_1} \left|\mathrm{GHZ}_n^{\ell}\right\rangle_{\mathrm{A}_1 \cdots \mathrm{A}_\ell} &= \frac{1}{\sqrt{2^n}} \sum_{x,y \in \mathbb{F}_2^n} M_{xy} |x\rangle_{\mathrm{A}_1} |y\rangle_{\mathrm{A}_2} \cdots |y\rangle_{\mathrm{A}_\ell} \\ &= \frac{1}{\sqrt{2^n}} \sum_{x,y} |x\rangle_{\mathrm{A}_1} (M^T)_{yx} |y\rangle_{\mathrm{A}_2} \cdots |y\rangle_{\mathrm{A}_\ell} \\ &= \left(I_{\mathrm{A}_1} \otimes \left(\widehat{M^T}\right)_{\mathrm{A}_2 \cdots \mathrm{A}_\ell}\right) \left|\mathrm{GHZ}_n^{\ell}\right\rangle_{\mathrm{A}_1 \cdots \mathrm{A}_\ell} \end{aligned}$$

This completes the proof and establishes the identity. ∎

Next, we establish some properties of the GHZ-map, which are straightforward to prove (see [9] for proof of $\ell = 3$).

Lemma 2. *The GHZ-map $M \in \mathbb{C}^{2^n \times 2^n} \mapsto \widehat{M} \in \mathbb{C}^{2^{(\ell-1)n} \times 2^{(\ell-1)n}}$ is an algebra homomorphism [14]:*

(a) *Linear: If $M = \alpha A + \beta B$, where $\alpha, \beta \in \mathbb{C}$, then $\widehat{M} = \alpha\widehat{A} + \beta\widehat{B}$.*
(b) *Multiplicative: If $M = AB$, then $\widehat{M} = \widehat{A}\widehat{B}$.*
(c) *Projector-preserving: If $M^2 = M$, then $\widehat{M}^2 = \widehat{M}$.*

Consider performing stabilizer measurements on Alice's qubits. This corresponds to the case where $M = \Pi_{\mathcal{S}}$ for some stabilizer group $\mathcal{S}$. The third property above clarifies that this also induces a projection on the remaining qubits. However, we want to understand whether it projects onto a *stabilizer* code and, if so, then we also want to know the structure of this induced code. The above lemma greatly simplifies this pursuit since the code projector (2) is a product of sums. Note that we seek to expand $\widehat{\Pi_{\mathcal{S}}^T}$, and that the transpose map commutes with the GHZ-map. Due to the multiplicativity of the GHZ-map, it is sufficient to consider only the case $r = 1$ in $\Pi_{\mathcal{S}}$, where there is a single stabilizer generator $\varepsilon E(a, b)$. Now, due to the linearity of the GHZ-map, we only need to determine $\widehat{I_N}$ and $\widehat{E(a,b)}$, since $E(a,b)^T = (-1)^{ab^T} E(a,b)$. Using this approach, we arrive at the following main technical result.

Theorem 3. *Given n copies of the ℓ-qubit GHZ state with subsystems $A_1, A_2, \ldots, A_\ell$, measuring $E(a, b)$ on the n qubits of subsystem A_1 and obtaining the result $\varepsilon \in \{\pm 1\}$ is equivalent to measuring the following with results $+1$ on the qubits of the remaining $(\ell - 1)$ subsystems:*

$$\varepsilon(-1)^{\left(\sum_{i=1}^{\ell-2} \sum_{j>i}^{\ell-1} b_i * b_j\right) a^T} \bigotimes_{t=2}^{\ell} E(a, b_{t-1})_{A_t}^T$$

$$= \varepsilon(-1)^{\left(b+\sum_{i=1}^{\ell-2}\sum_{j>i}^{\ell-1} b_i * b_j\right)a^T} \bigotimes_{t=2}^{\ell} E(a, b_{t-1})_{A_t} \quad \textit{and}$$

$$\{Z_{A_2,i}Z_{A_3,i} = E(0,e_i)_{A_2} \otimes E(0,e_i)_{A_3}\ ,$$
$$Z_{A_3,i}Z_{A_4,i} = E(0,e_i)_{A_3} \otimes E(0,e_i)_{A_4}\ ,\ \dots\ ,$$
$$Z_{A_{\ell-1},i}Z_{A_\ell,i} = E(0,e_i)_{A_{\ell-1}} \otimes E(0,e_i)_{A_\ell}\ ;\ i = 1,2,\dots,n\},$$

where $b_1, b_2, \dots, b_{\ell-1} \in \mathbb{F}_2^n$ *satisfy* $b_1 \oplus b_2 \oplus \cdots \oplus b_{\ell-1} = b$, $x * y$ *denotes the element-wise product of two vectors,* $Z_{A_t,i}$ *refers to* Z *on* i*-th qubit of subsystem* A_t*, and* e_i *is the standard basis vector with the* 1 *in the* i*-th position.*

Proof: The proof is a direct generalization of the $\ell = 3$ case. See [9] for the details. ∎

Example 1. Consider $\ell = 3, n = 1$ and the case when $M = \frac{I+Z}{2} = \frac{I+E(0,1)}{2}$, with $a = 0, b = 1 = b_1, b_2 = 0$. Then, $\widehat{I} = \frac{I\otimes I+Z\otimes Z}{2}$ and $\widehat{E(0,1)^T} = (E(0,1)^T \otimes E(0,0)) \cdot \widehat{I} = (Z\otimes I)\cdot\widehat{I}$. Therefore, the stabilizers for BC are $\langle Z\otimes I, Z\otimes Z\rangle$.

If we had an X-measurement for 'A', where $a = 1, b = 0$, then $E(a,b)^T \otimes E(a,0) = X \otimes X$. Combined with the $Z \otimes Z$ from $\widehat{I}$, the qubits on BC are projected to the Bell state.

More interestingly, if we consider a Y-measurement for 'A', where $a = b = 1$, then $E(a,b)^T \otimes E(a,0) = Y^T \otimes X = -Y \otimes X$. Thus, assuming the measurement result is $+1$, the new BC stabilizers are $\langle -Y\otimes X, Z\otimes Z\rangle$. It can be verified that the post-measurement state for this case will be $\frac{(|0\rangle+i|1\rangle)}{\sqrt{2}} \otimes \frac{(|00\rangle-i|11\rangle)}{\sqrt{2}}$, which is stabilized by the above stabilizer. ∎

Remark 4. There are two special cases that eliminate the sign in the new joint stabilizer. One can set $b_1 = b$ and $b_2 = b_3 = \cdots = b_{\ell-1} = 0$ [9], like in Example 1, in which case $b_i * b_j = 0$ always. More generally, one can define $\{b_i \colon b_i \neq 0\}$ such that $b_i * b_j = 0$ while $b_1 \oplus b_2 \oplus \cdots \oplus b_{\ell-1} = b$ still holds, i.e., splitting the entries of b into $(\ell-1)$ disjoint groups.

As we desired, the above result shows how a Pauli measurement on one subsystem, A_1, of (multiple copies of) the GHZ state affects the remaining subsystems. All the GHZ stabilizers involving subsystems $\mathrm{A}_2, \mathrm{A}_3, \dots, \mathrm{A}_\ell$ are retained. Hence, the post-measurement state is "GHZ-like" on these $(\ell-1)$ subsystems but with an additional globally entangling stabilizer. This is akin to the globally entangling all-X stabilizer for the standard GHZ state, but it depends on the Pauli operator being measured on A_1. Note that, since the Pauli measurement randomly projects onto a subspace, the induced stabilizers given by the theorem do not uniquely determine the post-measurement state on the $(\ell-1)$ subsystems. The degrees of freedom for the state will be quantified shortly in a more general setting. One might argue that this theorem can be obtained by directly applying the stabilizer formalism to $\mathcal{S}_{\mathrm{GHZ}}$. However, some thought clarifies that arriving at the conclusions rigorously takes at least an equal amount of effort.

In the context of measuring a set of $(n-k)$ stabilizer generators of a code (on qubits A_1), the above result confirms that this induces a joint *stabilizer* code on the remaining $(\ell-1)$ subsystems. There are $n(\ell-1)$ qubits on these subsystems and each code stabilizer generator contributes a stabilizer generator for this induced code. Besides, as stated in the theorem, there are $n(\ell-2)$ GHZ stabilizers on all pairs of adjacent subsystems, $\{\mathrm{A}_j\mathrm{A}_{j+1}\,;\, j = 2,\dots,\ell-1\}$, independent of the code stabilizers being measured. Hence, the induced code has $(n-k)+n(\ell-2)$ stabilizer generators, which means it is an $[\![n(\ell-1), k]\!]$ code and the post-measurement state has k logical degrees of freedom. The minimum distance of the induced code will depend on the minimum distance of the A_1-code as well as the new GHZ stabilizers and the choice of $\{b_i\}$. In [15], for $\ell = 3$, only the special case of Theorem 3 with $b_1 = b, b_2 = b_3 = \cdots = b_{\ell-1} = 0$ was considered. Since this leads to purely X-type stabilizers for the remaining subsystems, a local diagonal Clifford operation was prescribed to fix the stabilizers. Such techniques can also be applied in the more general Theorem 3 based on the choices of b_i.

We will now complete this paper with the overall description of the protocol. More details can be found in [9].

C. The Distillation Protocol

The protocol is showed on the left side of Fig. 2 for $\ell = 3$. We will restrict ourselves to CSS codes here, since most good codes found in the literature are of this type. However, if necessary, the protocol can be generalized to arbitrary stabilizer codes using some additional details from [15], where that initial protocol turned out to be less scalable.

For any $\ell \geq 3$, A_1 generates n ideal copies of the ℓ-qubit GHZ state, names the qubits of each copy A_1 through A_ℓ, chooses some $[\![n,k]\!]$ code $\mathcal{Q}(\mathcal{S})$ defined by a stabilizer $\mathcal{S}$, and measures the $(n-k)$ generators of $\mathcal{S}$ on qubits A_1. Then, A_1 applies Theorem 3 to determine the induced code $\mathcal{Q}\left(\mathcal{S}^{(\ell-1)}\right)$ on the remaining subsystems. Let us again set $\ell = 4$ for simplicity. For tracking the protocol, we can initially create a table whose rows are the binary representations of the generators of $\mathcal{S}_{\mathrm{GHZ}}^{\otimes n}$ (similar to [9]). Group the n $Z_{\mathrm{A}_i}Z_{\mathrm{B}_i}I_{\mathrm{C}_i}I_{\mathrm{D}_i}$ generators in the first part of the table, the n $I_{\mathrm{A}_i}Z_{\mathrm{B}_i}Z_{\mathrm{C}_i}I_{\mathrm{D}_i}$ generators in the second part, the n $I_{\mathrm{A}_i}I_{\mathrm{B}_i}Z_{\mathrm{C}_i}Z_{\mathrm{D}_i}$ in the third part, and finally the n $X_{\mathrm{A}_i}X_{\mathrm{B}_i}X_{\mathrm{C}_i}X_{\mathrm{D}_i}$ in the fourth part. If there is a purely Z-type generator, $E(0,b)_{\mathrm{A}}$, for $\mathcal{S}$, then it will commute with the first three parts and only affect the last part based on the stabilizer formalism. Moreover, by an appropriate linear combination of the rows of the first part, one can produce the element $E(0,b)_{\mathrm{A}} \otimes E(0,b)_{\mathrm{B}}$, which when multiplied by the new code stabilizer produces the stabilizer $E(0,b)_{\mathrm{B}}$ on purely subsystem B. By a similar trick in the second part and subsequently in the third part, one can produce single-subsystem stabilizers $E(0,b)_{\mathrm{C}}$ and $E(0,b)_{\mathrm{D}}$ as well. Hence, it suffices to only consider stabilizers $E(a,b)_{\mathrm{A}}, a \neq 0$.

Such stabilizers transform into the multiple-subsystem stabilizers described by Theorem 3. Now, qubits of B, C, and D need to be transmitted over a noisy channel to the respective nodes, based on the network topology. For those nodes to be able to correct errors, a code needs to be imposed purely on each subsystem *before* transmission of the respective qubits. Let A be connected to B. Then, based on the choice of b_1, b_2, b_3 in Theorem 3, A measures code stabilizers $E(a,b_1)_{\mathrm{B}}$

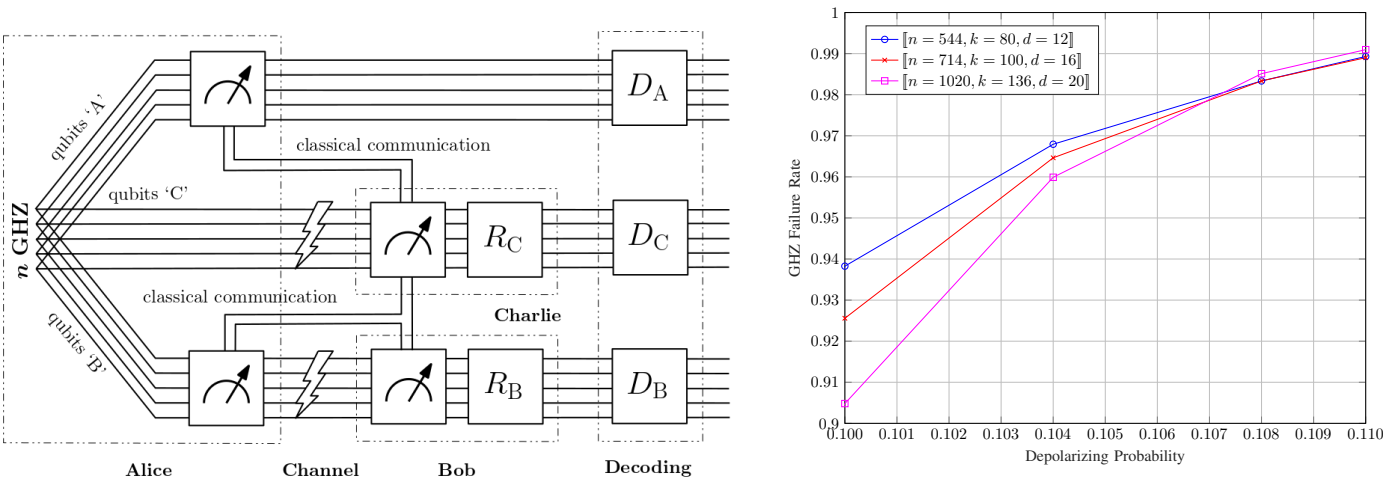

Fig. 2: (left) QEC-based distillation protocol for GHZ states. (right) Threshold of the protocol on a lifted product code family.

on qubits B. With some thought, one sees that these stabilizers only affect the second part of the table. Now, since $\pm E(a, b_1)_{\mathrm{B}} \otimes E(a, b_2)_{\mathrm{C}} \otimes E(a, b_3)_{\mathrm{D}}$ is already a stabilizer, by multiplying with $E(a, b_1)_{\mathrm{B}}$ we obtain a code on B and a residual code jointly on C and D. The qubits of B can be transmitted to node B (along with necessary classical sign information of stabilizers), which can perform error correction.

If A is not connected to C and D, then A has to send those qubits to B. Thus, it appears that A has to perform stabilizer measurements as above not only on B but on C and D as well. However, this can be relegated to subsequent nodes to reduce the burden on A. Let A also send qubits C and D to node B along with qubits B. There is some joint Pauli error on B, C, and D, and the error correction of B only fixes the error part on B. If B measures code stabilizers on C, then the preexisting Pauli error can be transformed into an effective Pauli error *after* the code was imposed on C. This enables node C to correct this error as well as any error encountered while B sends qubits C. A similar statement holds for D as well. Thus, the protocol can be stated as follows: for every edge connected to a node, the node performs stabilizer measurements on the respective subsystem to impose a code on the qubits of the recipient on that edge. The correctness of the protocol relies on carefully tracking signs of stabilizers based on such measurements at each node. Once all qubits are distributed, each node uses the logical Paulis of their respective codes [9] to determine and invert the encoding unitary. This converts the k logical GHZ states into k perfect physical GHZ states, provided all error corrections were successful.

In Fig. 2 (right), we plot the threshold of the protocol for $\ell = 3$ on a family of lifted product codes under iterative min-sum decoding. A more detailed discussion can be found in [9].

References

[1] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, p. 5932, 1998.

[2] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A*, vol. 59, no. 1, p. 169, 1999. [Online]. Available: https://arxiv.org/abs/quant-ph/9808065

[3] F. Rozpędek, T. Schiet, D. Elkouss, A. C. Doherty, S. Wehner *et al.*, "Optimizing practical entanglement distillation," *Physical Review A*, vol. 97, no. 6, p. 062333, 2018. [Online]. Available: https://arxiv.org/abs/1803.10111

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996. [Online]. Available: https://arxiv.org/abs/quant-ph/9604024

[5] M. M. Wilde, H. Krovi, and T. A. Brun, "Convolutional entanglement distillation," *Proc. IEEE Intl. Symp. Inf. Theory*, pp. 2657–2661, June 2010. [Online]. Available: https://arxiv.org/abs/0708.3699

[6] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, 1997. [Online]. Available: https://arxiv.org/abs/quant-ph/9705052

[7] R. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1369–1387, Jul 1998. [Online]. Available: https://arxiv.org/abs/quant-ph/9608006

[8] D. Gottesman, "The Heisenberg representation of quantum computers," in *Intl. Conf. on Group Theor. Meth. Phys.* International Press, Cambridge, MA, 1998, pp. 32–43. [Online]. Available: https://arxiv.org/abs/quant-ph/9807006

[9] N. Rengaswamy, N. Raveendran, A. Raina, and B. Vasić, "Entanglement Purification with Quantum LDPC Codes and Iterative Decoding," *arXiv preprint arXiv:2210.14143*, 2022. [Online]. Available: https://arxiv.org/abs/2210.14143

[10] N. P. Breuckmann and J. N. Eberhardt, "Balanced product quantum codes," *IEEE Transactions on Information Theory*, vol. 67, no. 10, pp. 6653–6674, 2021. [Online]. Available: https://arxiv.org/abs/2012.09271

[11] P. Panteleev and G. Kalachev, "Asymptotically good quantum and locally testable classical LDPC codes," in *Proc. 54th Annual ACM SIGACT Symposium on Theory of Computing*, 2022, pp. 375–388. [Online]. Available: https://arxiv.org/abs/2111.03654v1

[12] I. Dinur, M.-H. Hsieh, T.-C. Lin, and T. Vidick, "Good quantum LDPC codes with linear time decoders," *arXiv preprint arXiv:2206.07750*, 2022. [Online]. Available: https://arxiv.org/abs/2206.07750

[13] N. Raveendran, N. Rengaswamy, F. Rozpędek, A. Raina, L. Jiang, and B. Vasić, "Finite rate QLDPC-GKP coding scheme that surpasses the CSS Hamming bound," *Quantum*, vol. 6, p. 767, Jul. 2022. [Online]. Available: https://arxiv.org/abs/2111.07029

[14] D. S. Dummit and R. M. Foote, *Abstract algebra*. Wiley Hoboken, 2004, vol. 3.

[15] N. Rengaswamy, A. Raina, N. Raveendran, and B. Vasić, "Distilling GHZ States using Stabilizer Codes," *arXiv preprint arXiv:2109.06248*, 2021. [Online]. Available: https://arxiv.org/abs/2109.06248