# $\sqrt{n} \mapsto \Theta(n)$ Magic States 'Distillation' Using Quantum LDPC Codes.

David Ponarovsky

August 21, 2024

## 1 Introduction.

In this work, we consider quantum circuits under the Clifford-free noise model. In this model, it is assumed that any of the Clifford gates, such as $S$, $H$, and $CZ$, can be applied perfectly. Additionally, the circuits have access to noisy magic states at an error rate of $p$, formulated as the mixed state $(1-p)\left|T\right\rangle + pZ\left|T\right\rangle$, where $p \in (0,1)$ is the probability that a given state is actually a faulty one and $\left|T\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + e^{i\frac{\pi}{4}}\left|1\right\rangle)$ is a Magic State. Finally, the model allows for intermediate measurements and the application of Clifford gates controlled by the classical outcomes of the measurements. It has been shown that this model is quantum universal.

The Magic State Distillation Protocol is a quantum circuit in the Clifford-free noise model that consumes $n$ noisy magic states at an error rate of $p$ and outputs $k$ independent magic states at an error rate of $\varepsilon$. The previews constructions usually used self- Triorthogonal codes (Definition 2.1) [BH12], in which the logical $T^k$ gate can be computed transversally. Depending on how good the code is in terms of rate and distance, it can give a better gain in the reduction of the error rate and lower consumption of Magic states. This was shown in **[COMMENT]** cite it. The standard approach of computing $T^k$ transversally gives a $\log^{\gamma}(\frac{1}{\varepsilon})$-overhead distillation protocol, where $\gamma = \log(\frac{n}{k})/\log(d)$. **[COMMENT]** mention known $\gamma$ values and provide citations. For many years, the major focus was on giving a distillation protocol for which $\gamma \to 0$. Recently, [WHY24] succeeded in achieving this. This achievement raises the question of whether $\gamma = 0$ specifies the limit or if there exists a distillation protocol that consumes a sublinear amount of Magic states. We answer this question in the affirmative. Here, we show the existence and construction of protocols that consume $\sqrt{n}$ Magic States and produce, almost surely, $\Theta(n)$ perfect Magic States. We emphasize that the protocols output dependent states, i.e., if the protocol fails, then any of the $\Theta(n)$ outcomes is a faulty Magic state. This is why we put the phrase "Distillation" in quotation marks in the title.

**Theorem 1.1** ($\sqrt{n} \to n$ 'Distillation' (unformal)). *There exists an efficient falut tolerance circuit, with respect to Clifford-free noise model, that with high probability produce asymptotically more Magic States than what it consumes.*

## 2 Notations, Definitions and Construction.

The notation used in this paper follows standard conventions for coding theory. We use $n$ to represent the length of the code, $k$ for the code's dimension, and $\rho$ for its rate. The minimum distance of the code will be denoted as $d$, and the relative distance, i.e., $d/n$, as $\delta$. In this paper, $n$ and $k$ will sometimes refer to the number of physical and logical bits. Codes will be denoted by a capital $C$ followed by either a subscript or superscript. When referring to multiple codes, we will use the above parameters as functions. For example, $\rho(C_1)$ represents the rate of the code $C_1$. Square brackets are used to present all these parameters compactly, and we use them as follows: $C = [n,k,d]$ to declare a code with the specified length, dimension, and distance. Any theorem, lemma, or claim that states a statement that is true in the asymptotic sense refers to a family of codes. The parity check matrix of the code will be denoted as $H$, with the rows of $H$ representing the parity check equations. The generator matrix of the code will be denoted as $G$, with the rows of $G$

representing the basis of codewords. The syndrome of a received word will be denoted as $s$, which is the result of multiplying $r$ by the transpose of $H$. We use $C^{\perp}$ to denote the dual code of $C$, which is defined such that any codeword of it $z \in C^{\perp}$ is orthogonal to any $x \in C$, meaning $z \cdot x = 0$, where the product is defined as $x \cdot z = \sum_i x_i z_i$. $C^{\top}$ stands for the code obtained by taking the parity check matrix of $C$ and transposing it.

In this paper, we define the triple product $\mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{Z}$ as $|x \cdot y \cdot z| = \sum_i^n x_i y_i z_i$. Similarly, we define the binary product $|x \cdot y|$, noting that this product differs from the standard product by mapping into $\mathbb{Z}$ rather than $\mathbb{F}_2$. For $w \in \mathbb{F}_2^n$, we use the super operator $\cdot|_w$ to map an operator originally defined in an $n$-dimensional space to an operator that only acts on coordinates restricted to $w$. For example, $x|_w$ is the vector in $\mathbb{F}_2^{|w|}$ obtained by taking the values of $x$ on coordinates where $w$ is not zero. $|x \cdot y|_w = \sum_{i: w_i \neq 0} x_i y_i$ and $C|_w$ is the code obtained by taking the codewords of $C$ restricted to $w$.

**Definition 2.1.** *Let $C$, $\tilde{C}$ be linear binary codes at the same length, We will say that $\tilde{C}$ is a Triorthogonal with respect to $C$ if:*

1. *$\tilde{C} \subset C$*
2. *$|x \cdot y \cdot z|$ is even for $x, y, z \in C$ such that at least one of $x, y, z$ belongs to $\tilde{C}$.*
3. *$|x \cdot y|$ is even for $x, y \in C$ such that at least one of $x, y$ belongs to $\tilde{C}$.*

*If a code $C$ is Triorthogonal with respect to itself then we will say that $C$ is a self Triorthogonal code.*

For example, the empty code, that contains only the zero code word, i.e $C = \{0\}$, is a Triorthogonal with respect to any code. In fact for proving Theorem 2.1 taking the empty code is sufficient. For other example, the Triorthogonal codes defined in [BH12] are Triorthogonal with respect to themself.

A quantum code over $n$ qubits is an embedding of $\mathcal{H}_2^{\otimes k}$ as a subspace of $\mathcal{H}_2^{\otimes n}$. Similar to classical codes, we will call $n$ and $k$ the physical and logical qubits. The embeddings of states in $\mathcal{H}_2^{\otimes k}$ are called codewords or encoded states. In addition, we will use the term "logical operator" (i.e. logical $X_i$) to describe an operator that acts on the code space exactly as it would act on the logical space $\mathcal{H}_2^{\otimes k}$ (in our example, turning on and off the encoded state corresponds to the $i$th qubit exactly as $X_i$ acts as Pauli $X$ on the $i$th qubit in $\mathcal{H}_2^{\otimes k}$). We will denote by $X$ and $Z$ the single $X$ and $Z$ Pauli operators, by $X_i$ the application of $X$ on the $i$th qubit and nothing else (identity) on the rest of the qubits. By $X^{(v)}$ for some $v \in \mathbb{F}_2^n$, we mean the operator composed by applying $X$ on each of the qubits whose index is a non-trivial coordinate of $v$ and identity elsewhere. In a similar fashion, we define $Z^{(v)}$. When the context is clear, we will allow ourselves to omit the brackets, i.e. $Z^v$. The weight of a Pauli operator is the number of coordinates on which the operator acts non-trivially. Recall that the set of Pauli $+I$ spans all the Hermitian matrices. We say that the Pauli weight of an operator is the maximal weight of a Pauli in its Pauli decomposition. For example, consider the operator $A = IXX + ZII$, the weight of $A$ is 2. The distance of a quantum code is the minimal weight of an operator that takes one codeword to another. We use the standard bracket notation to describe quantum states and in addition, we define for a vector space $A \subset \mathbb{F}_2^n$ the notation $|A\rangle$ to represent the uniform superposition of all the vectors belonging to that space, namely:

$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle$$

We define in the same way the notation to hold for affine spaces, $|x + A\rangle$. We will use $\propto$ to denote a quantum states up to normalization factor, for example $|\psi\rangle \propto |0\rangle + |1\rangle$ means that $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. A CSS code is a quantum code defined by a pair of classical codes $C_X$ and $C_Z$, satisfying $C_Z^{\perp} \subset C_X$, such that any codeword of it has the form $|x + C_Z^{\perp}\rangle$, where $x \in C_X$. We will use $Q$ to refer to a CSS code in general and use $C_X/C_Z^{\perp}$ to refer to the vectors associated with the $X$-generators or the encoded states in the computational basis. In the same way, $C_Z/C_X^{\perp}$ refers to the $Q$ in the phase basis. We will say that a CSS code $Q$ is a LDPC if $C_X$ and $C_Z$ are both LDPC codes. Our construction uses the classical Tanner code [Tan81], the expander codes [SS96], and Hyperproduct product (quantum expanders) [LTZ15], [TZ14], [BFS23]. We will not describe these constructions and refer the reader to those papers for further information.

**Theorem 2.1** ($\sqrt{n} \to n$ 'Distillation'). *There exists is $p_0 \in (0,1)$ such that for the Clifford-free noise model with an error rate $p < p_0$, there is a family of circuits that, for sufficiently large $n$, consume $\sqrt{n}$ noisy Magic States and with probability greater than $1 - e^{-n^{1/8}}$ output $\Theta(n)$ perfect Magic States. Furthermore, both the width and depth of the circuits are linear in $n$.*

Compared to the previous approaches, our construction does not use a self Triorthogonal code. Instead, we build a CSS code $Q$ for which there exists a subcode $\mathcal{X}' \subset C_X/C_Z^{\perp}$ with linear dimension, and non non-trivial distance, such that the restriction of $\mathcal{X}'$ to a vector $w \in C_Z/C_X^{\perp}$ is 'almost' Triorthogonal with respect to $(C_X)|_w$. This condition 'almost' allows us to compute the logical $T^{\rho(\mathcal{X}')n}$ by applying physical $T$ gates 'almost' only on the restricted bits. To overcome this 'almost' issue, we show that by choosing the code $Q$ to be an LDPC code, and such that there exists a vector $w \in C_Z/C_X^{\perp}$ with weight $|w| = \Theta(n^{\frac{1}{4}})$, Then the number of $T$ gates that need to be applied in a non-transversal fashion is sublinear. We then apply one of the previous distillation protocols to ensure that we have fresh magic states, which can effectively be thought of as perfect, to compute the non-transversal $T$ gates.

## 2.1 The Protocol's Description.

We are about to describe the circuit. Definition 2.2 defines a quantum code $Q$, in which the main computation occurs. Definition 2.3 defines a subspace $\mathcal{X}' \subset C_X/C_Z^{\perp}$ and a $Z$-generator $w$ such $\mathcal{X}'|_w$ is Triorthogonal with respect to $(C_X)|_w$. Lastly, Definition 2.4 defines the quantum gates $\mathcal{C}$, $\mathcal{E}$ and $\mathcal{D}$ stand for low-$T$ gate, encoder and decoder respectively, In Section 2.1 an hypotactic valid scheme of main routine is shown, for capture the full figure it's left to chain the drawn circuit constant number of time.

Before presenting the code we need to prove the following claim:

**Claim 2.1.** *Let $C_{Tanner}$ be a Tanner code defined by a graph with algebraic expansion $\lambda\Delta$, Suppose that both $C_0$ and $C_0^{\perp}$ have realtive distance greater than $\delta > \lambda$. Then $C_{Tanner}^{\top}$ has a linear distance.*

The proof is simplified version of Lemma 3 proof in [PK21].

*Proof.* Denote by $H^{\top}$ the parity check matrix of $C^{\top}_{\text{Tanner}}$. Observes that $H^{\top}$ can obtained by transposing any of the local parity check matrices of $C_0$, hence the action of $H^{\top}$ on $\mathbb{F}_2^{n-k}$ is multiplying $C_0^{\perp}$ generator matrices by given vectors according to some mapping from the vertices $(1-\rho)\Delta$-size local view to indices at $[n-k]$ and back. Denote that mapping by $\pi : V \times [(1-\rho_0)\Delta] \to [n-k]$. can be thought as multiplying $(n-k)$-size local view of the vertices of Let $y \in \mathbb{F}_2^{n-k}$, and let $S \subset V$, where $V$ denotes the vertices in the graph, be the $H^{\top}y$. □

**Definition 2.2.** *Let $\Delta$ be a constant integer, $C_0$ and $\tilde{C}_0$ be codes over $\Delta$ bits such that $\tilde{C}_0$ is Triorthogonal with respect to $C_0^{\perp}$. $C_0$ has parameters $\Delta[1, \delta_0, \rho_0]$, and $C_0^{\top}$ has relative distance greater than $\delta_0$. Let $C_{Tanner}$ be a Tanner code, defined by taking an expander graph with good expansion and $C_0$ as the small code. Let $C_{initial}$ be the dual-tensor code obtained by taking $(C_{Tanner}^{\perp} \otimes C_{Tanner}^{\perp})^{\perp}$. Note that first, this code has a positive rate and $\Theta(\sqrt{n})$ distance. Second, this code is an LDPC code as well. Also, notice that $C_{initial}^{\top}$ is obtained by transporting the parity check matrix, and therefore equals to $(C_{Tanner}^{\top,\perp} \otimes C_{Tanner}^{\top,\perp})^{\perp}$. Hence, $C_{initial}^{\top}$ has a square root distance as well.*

*Let $Q$ be the CSS code obtained by taking the Hyperproduct of $C_{initial}$ with itself. So, $Q$ is a quantum qLDPC code with parameters $[n, \Theta(n^{\frac{1}{4}}), \Theta(n)]$. The notations $Q, C_{Tanner}, C_{initial}, \tilde{C}_0, C_0$ will keep these definitions for the rest of the paper.*

For further explanation on dual-tensor, please refer to [LZ22], [Din+22], and [PK21]. We rely on the main theorem in [TZ14] for the Hyperproduct code distance and rate.

The main advantage of using the dual-tensor and Hyperproduct is that their bases can be easily understood in terms of the codes being multiplied to obtain them. For the dual-tensor $(C^{\perp} \otimes C^{\perp})^{\perp} = C \otimes \mathbb{F}_2^n \oplus \mathbb{F}_2^n \otimes C$, one can think of the codewords as $n \times n$ binary matrices and take the collection of imposing single generators of $C$ on the rows or columns as the code base. In the Hyperproduct , the code words can be thought of as assignments of bits on two matrices: the first at size $n(C) \times n(C)$, while the

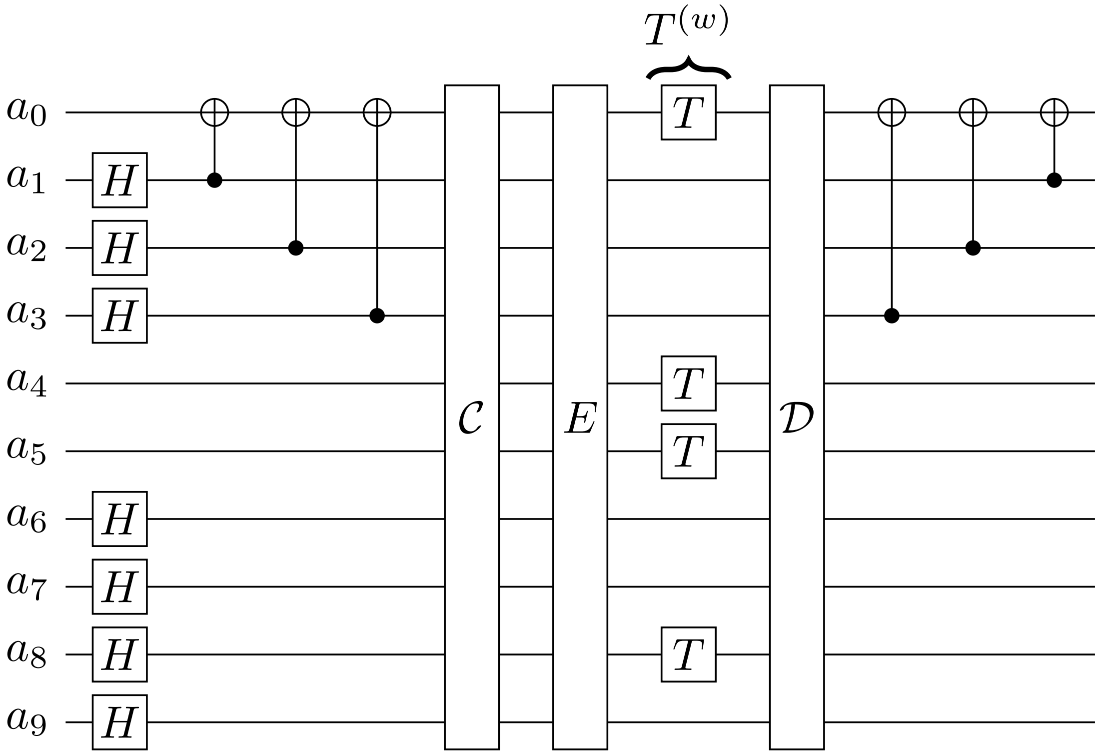

Figure 1: The circuit.

second is at size $n(C^\top) \times n(C^\top)$. Any generator of $C_X$ either imposes a $C$ generator on one of the rows of the first matrix or imposes a $C^\top$ generator on one of the columns of the second matrix. In our case, we can imagine that both the $X$ and $Z$ generators of $Q$ correspond to setting a generator of $C_{\text{Tanner}}$, $C_{\text{Tanner}}^\top$ on a 'row' of the 4D cube.

**Definition 2.3.** *Consider the code $Q$, defined in definition 2.2 in the computation base $C_X/C_Z^\perp$. Let $x_0$ be a codeword of $C_X/C_Z^\perp$. Denote by $w \in \mathbb{F}_2^n$ the binary string that represents the $Z$-generator that anti-commutes with the $X$-generator corresponding to $x_0$. Let $\mathcal{X} = \{x_0, x_1, ..x_{k'}\} \in \mathbb{F}_2^n$ be a subset of a basis for the code $C_X/C_Z^\perp$. Such $(\text{span}\ \mathcal{X}/x_0\ )|_w$ is a Triorthogonal code with respect to $C_X|_w$. Let us denote by $\mathcal{X}'$ the basis $\{y_1, y_2, .., y_{k'}\} \in \mathbb{F}_2^n$ defined as follows: $y_i = x_j + x_0$.*

Claim 3.1 states that $\mathcal{X}'$ is not empty and even has linear size at $n$.

**Definition 2.4.** *Denote by $E$ the circuit that encodes the $i$th logical bit into $|y_i + C_Z^\perp\rangle$, By $T^{(w)}$ the application of $T$ gates on the qubits for which $w$ acts non-trivially, meaning $T^{(w)}$ is a tensor product of $T$'s and $I$'s where on the $i$th qubit $T^{(w)}$ applies $T$ if $w_i$ equals 1, and identity otherwise. By $D$ denote the gate that decodes binary strings in $\mathbb{F}_2^n$ back into the logical space, $D$ is also responsible to correct errors. Finally, denote by $\mathcal{C}$ a non Clifford gate, which contains at most $o(n^{\frac{1}{4}})$ Magic States, and by $\mathcal{D}$ an $n^2$-overhead Magic Distillation Protocol, that consume $\Theta(\sqrt{n})$ magic and produce $O(n^{\frac{1}{4}})$ Magic States, with error rate less than $2^{-\alpha n}$.*

## 3 Proof of Theorem 1.

**Claim 3.1.** *There exists family of non-trivial distance quantum LDPC codes $Q$ such the subcode $\mathcal{X}'$ chosen respect to them has a positive rate. Furthermore, the rate of $\mathcal{X}'$ is a asymptotically converges to $Q$ rate:*

$$|\rho(Q) - \rho(\mathcal{X}')| = o(1)$$

*Proof.* Pick $x_0$ and $w \in \mathbb{F}_2^n$ , which correspond to the supports of anti commute $X$ and $Z$ generators, such that $w$ can be obtains by setting a codeword of $C_{\text{Tanner}}$ on the first $n^{\frac{1}{4}}$ bits and padding by zeros the rest. Clearly, $|w| = \Theta(n^{\frac{1}{4}})$. Denote by $\Gamma(w)$ vertices supports $w$ in the graph used to define $C_{\text{Tanner}}$.

Now for defying span $\mathcal{X}$, we are going to consider the parity checks matrix obtained by adding restrictions to $C_X$'s restrictions as follows: For any $\Delta$-bits correspond to a local view of vertex $v \in \Gamma(w)$ add restrictions of $\tilde{C}_0$. Then span $\mathcal{X}$ is the subspace of $C_X/C_Z^{\perp}$ satisfying $\tilde{C}_0$. Hence, the dimension of $\mathcal{X}$ is bounded by below by:

$$\rho(C_X) \cdot n - |\Gamma(w)| \cdot (1 - \rho(\tilde{C}_0))\Delta \geq \rho(C_X) \cdot n - \Delta \cdot n^{\frac{1}{4}}$$

And by the fact that the dimension of $C_Z^{\perp}$'s codewords satisfying $\tilde{C}_0$ on $\Gamma(w)$ local views is strictly lower then $\dim C_Z^{\perp}$, we get the following lower bound:

$$\begin{aligned}\dim \operatorname{span} \mathcal{X} &\geq \rho(C_X) \cdot n - \Delta \cdot n^{\frac{1}{4}} + \rho(C_Z) \cdot n - n \\ &\geq \rho(Q) - \Delta \cdot n^{\frac{1}{4}}\end{aligned}$$

□

**Remark 3.1.** *We emphasise that if one is only interest in having large $\mathcal{X}$ subset of $C_X/C_Z^{\perp}$ that is only $Triorthogonal$ to itself, then instead of setting more restrictions on the vertices in $\Gamma(w)$ one could just divides the non non-trivial bits of $w$ into $\Delta$-size buckets, and then considering the codewords which their restrictions to a bucket is a codeword of $\tilde{C}_0$. Then the above proof can be easily adapted to result the following for general CSS codes: There exists $\mathcal{X} \subset C_X/C_Z^{\perp}$ such:*

$$|\rho(Q) - \rho(\mathcal{X})| = d(Q)(1 - \rho(\tilde{C}_0))$$

*In general, this technique does not yield a $Triorthogonal$ code for a $C_X/C_Z^{\perp}$, but there are several cases in which it does. For example let's consider the quantum Tanner code. Since the distance of the quantum Tanner codes is $\sim n/\Delta$, where $\Delta^2$ is the degree of the square complex graph, (obtained by taking a codeword for which each local view of it is supported only on rows corresponding to a specific single left generator), we get that for any $\rho \in (0, \frac{1}{2})$ there is a good qLDPC such that the dimension of $\mathcal{X}'$ obtained respecting to it is $\geq (1-2\rho)^2 n - n/\Delta \cdot (1 - \rho(\tilde{C}_0))$.*

**Claim 3.2.** *There is a family of quantum circuits $\mathcal{C}$ consists of Clifford gates and at most $O(n^{3/4})$ number of $T$ gates such that:*

$$T^{(w)} |\mathcal{X}' + C_Z^{\perp}\rangle \propto E\, \mathcal{C}\ (TH)^{\rho(\mathcal{X}')n} |0\rangle$$

*Proof.* Let $\tau \in \mathcal{X}' + C_Z^{\perp}$, applying $T^{(w)}$ on $|\tau\rangle$ add a phase of $i\frac{\pi}{4} |\tau|_w$. Notice that $\tau$ can decompose to the sum of $X_{x_0} x_0 + \sum_{y_i \in \mathcal{X}} X_{y_i} y_i + \sum_{z_i \in \text{ base } C_Z^{\perp}} X_{z_i} z_i$ when $X_g$ is the indicator that equals 1 if the generator $g$ supports $\tau$. Let us denote by $\Lambda$ the union of the generators. So:

$$\begin{aligned}|\tau|_w &= \left| \sum_{g \in \Lambda} X_g g \right|_w \\ &= \sum_{g \in \Lambda} X_g |g|_w - 2 \sum_{g,h \in \Lambda \times \Lambda} X_g X_h |g \cdot h|_w + 4 \sum_{g,h,k \in \Lambda \times \Lambda \times \Lambda} X_g X_h X_k |g \cdot h \cdot k|_w\end{aligned}$$

Since $\mathcal{X}|_w$ is Triorthogonal with respect to $C_X|_w$ all the terms above that involve multiplication of at least one element in $\mathcal{X}$ is even, and therefore those terms add a phases that can be computed by Clifford gate:

1. $i\frac{\pi}{4} |y_i|_w \to c \cdot i\frac{\pi}{2}$ and therefore can computed by applying logical $S_{y_i}$.
2. $i\frac{\pi}{4} 2|y_i \cdot g|_w \to c \cdot i\pi$ and therefore can computed by applying logical $CZ_{y_i,g}$.

3. $i\frac{\pi}{4}4|y_i \cdot g \cdot h|_w \to c \cdot i2\pi$ and therefore such terms don't add phase at all.

So, only multiplications of generators which are either the $x_0$ generator or $C_Z^\perp$ generators might contribute a non-Clifford phase. Notice that since $x_0$ and $w$ anti-commute, we have that $|x|_w = 1$. Hence, $i\frac{\pi}{4}|x_w|$ contributes the phase of the logical $T_{x_0}$ up to logical $S_{x_0}, S_{x_0}^\dagger$. Additionally, observe that any singleton $i\frac{\pi}{4}|z_i|_w$ contributes a phase of a gate composed of at most a single logical $T_{z_i}$, and any pair $i\frac{\pi}{4}2|'z_j \text{ OR } x_0' \cdot z_i|_w$ and triple $i\frac{\pi}{4}4|'z_j \text{ OR } x_0' \cdot z_i \cdot z_k|_w$ contribute the phase of logical $CS, CCZ$, respectively. Therefore, each of them can be computed by at most $O(1)$ logical $T$ gates. Overall, we can get a rough upper bound on the number of logical $T$ gates required to uncompute the phase:

$$i\frac{\pi}{4}\left(|X_{x_0}x_0 + \sum_{z_i \in \text{ base } C_Z^\perp} X_{z_i}|_w - |X_{x_0}x_0|_w\right)$$

by at most:

$$\leq c\left(1 + \left|\{z_i \in \text{ base } C_Z^\perp : z_i|_w \neq 0\}\right|\right)^3$$

Since $Q$ is LDPC code, any bit of it, participate in a constant number of checks, therefore:

$$\begin{aligned}\left|\{z_i \in \text{ base } C_Z^\perp : z_i|_w \neq 0\}\right| = O(|w|)\\ \to c\left(1 + \left|\{z_i \in \text{ base } C_Z^\perp : z_i|_w \neq 0\}\right|\right)^3 \leq O(n^{3/4})\end{aligned}$$

Let $\mathcal{C}$ the gate which compute those phases in the logical space. □

**Claim 3.3.** *There is a family of quantum circuits $\mathcal{C}$ consists of Clifford gates and at most $o(\sqrt{n})$ number of $T$ gates, and produce $\Theta(n)$ $|T\rangle$ states.*

*Proof.* Chain recursively the protocol in Claim 3.2 for $1 + \lceil \log_{(1+\frac{1}{3})} 2 \rceil$ times. □

***Proof of Theorem 2.1.*** Outline:

1. Denote by $\mathcal{N}_1, \mathcal{N}_2$ the noise channels of $p$-Pauli noise, and Clifford-free $p$-noise models. Consider the indicator $X$ that indicate that a decoder $\mathcal{D}$ succeed to decode the sampled error. We can assume that $\mathbf{Pr}_{\mathcal{N}_2}[X] \geq \mathbf{Pr}_{\mathcal{N}_1}[X]$, Otherwise we can apply random Pauli on $[n]/[w]$ qubits with error rate $p$ so the error will be sampled according to $\mathcal{N}_1$.
2. We know that $\mathcal{D}$ decode errors drawn from $\mathcal{N}_1$ with high probability. ( In fact with: $1 - e^{-\Theta(d)}$ where $d$ is the code distance.)
3. Using the union bound:

$$\mathbf{Pr}[\mathcal{D} \text{ fails }] \leq \sum_{i=0}^{1+\lceil \log_{\frac{4}{3}} 2 \rceil} \exp\left(-n^{\frac{1}{4}\cdot\left(\frac{4}{3}\right)^i \cdot \frac{1}{2}}\right)$$

□

[LZ22] [MN98] [TZ14] [MEK12] [BH12]

# References


[Tan81] R. Tanner. "A recursive approach to low complexity codes". In: *IEEE Transactions on Information Theory* 27.5 (1981), pp. 533–547. DOI: 10.1109/TIT.1981.1056404.

[SS96] M. Sipser and D.A. Spielman. "Expander codes". In: *IEEE Transactions on Information Theory* 42.6 (1996), pp. 1710–1722. DOI: 10.1109/18.556667.

[MN98] Cristopher Moore and Martin Nilsson. *Parallel Quantum Computation and Quantum Codes.* 1998. arXiv: quant-ph/9808027 [quant-ph].

[BH12] Sergey Bravyi and Jeongwan Haah. "Magic-state distillation with low overhead". In: *Physical Review A* 86.5 (2012), p. 052329.

[MEK12] Adam M. Meier, Bryan Eastin, and Emanuel Knill. *Magic-state distillation with the four-qubit code.* 2012. arXiv: 1204.4221 [quant-ph].

[TZ14] Jean-Pierre Tillich and Gilles Zemor. "Quantum LDPC Codes With Positive Rate and Minimum Distance Proportional to the Square Root of the Blocklength". In: *IEEE Transactions on Information Theory* 60.2 (Feb. 2014), pp. 1193–1202. DOI: 10.1109/tit.2013.2292061. URL: https://doi.org/10.1109%2Ftit.2013.2292061.

[LTZ15] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zemor. "Quantum Expander Codes". In: *2015 IEEE 56th Annual Symposium on Foundations of Computer Science.* IEEE, Oct. 2015. DOI: 10.1109/focs.2015.55. URL: https://doi.org/10.1109%2Ffocs.2015.55.

[PK21] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes.* 2021. DOI: 10.48550/ARXIV.2111.03654. URL: https://arxiv.org/abs/2111.03654.

[Din+22] Irit Dinur et al. *Good Locally Testable Codes.* 2022. DOI: 10.48550/ARXIV.2207.11929. URL: https://arxiv.org/abs/2207.11929.

[LZ22] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes.* 2022. arXiv: 2202.13641 [quant-ph].

[BFS23] Nouédyn Baspin, Omar Fawzi, and Ala Shayeghi. *A lower bound on the overhead of quantum error correction in low dimensions.* 2023. DOI: 10.48550/ARXIV.2302.04317. URL: https://arxiv.org/abs/2302.04317.

[WHY24] Adam Wills, Min-Hsiu Hsieh, and Hayata Yamasaki. *Constant-Overhead Magic State Distillation.* 2024. arXiv: 2408.07764 [quant-ph]. URL: https://arxiv.org/abs/2408.07764.