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

David Ponarovsky

August 20, 2024

1 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 ρ for its rate. The minimum distance of the code will be denoted as d, and the relative distance, i.e., d/n, as δ. 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 1.1. *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* $\tilde{C}$.

For example, the empty code, that contains only the zero code word, is a Triorthogonal with respect to any code. In fact for proving Theorem 1.1 taking the empty code is sufficient.

Definition 1.2. *Let Δ be a constant integer, C_0 and $\tilde{C}_0$ be codes over Δ 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 δ_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 $(C^{\top,\perp}_{Tanner} \otimes C^{\top,\perp}_{Tanner})^{\perp}$. *Hence,* $C^{\top}_{initial}$ *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.*

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 $\frac{1}{\epsilon}$. 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')**.** *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*.*

1.1 The Protocol's Description.

Consider the code Q, defined in definition 1.2 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 2.1 states that $\mathcal{X}'$ is not empty and even has linear size at n.

Denote by E the circuit that encodes the ith 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 ith 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 $2^{-\alpha n}$.

Let $|\mathcal{X}'\rangle \propto \sum_{x \in \text{span } \mathcal{X}'} |x\rangle$.

2 Proof of Theorem 1.

Claim 2.1. *There exists family of non-trivial distance quantum LDPC codes* Q *such the codes span* $\mathcal{X}'$ *chosen respect to them has a positive rate. Furthermore, the rate of span* $\mathcal{X}'$ *is a asymptotically converges to* Q *rate:*

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

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_{Tanner} on the first $n^{\frac{1}{4}}$ bits and padding by zeros the rest. Clearly, $|w| = \Theta(n^{\frac{1}{4}})$.

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: Divide the first w bits into Δ-size buckets, define by $w(i)$ the ith coordinate on which w isn't trivial. For example if $w(1) = j$ then j is the first nonzero coordinate of w,

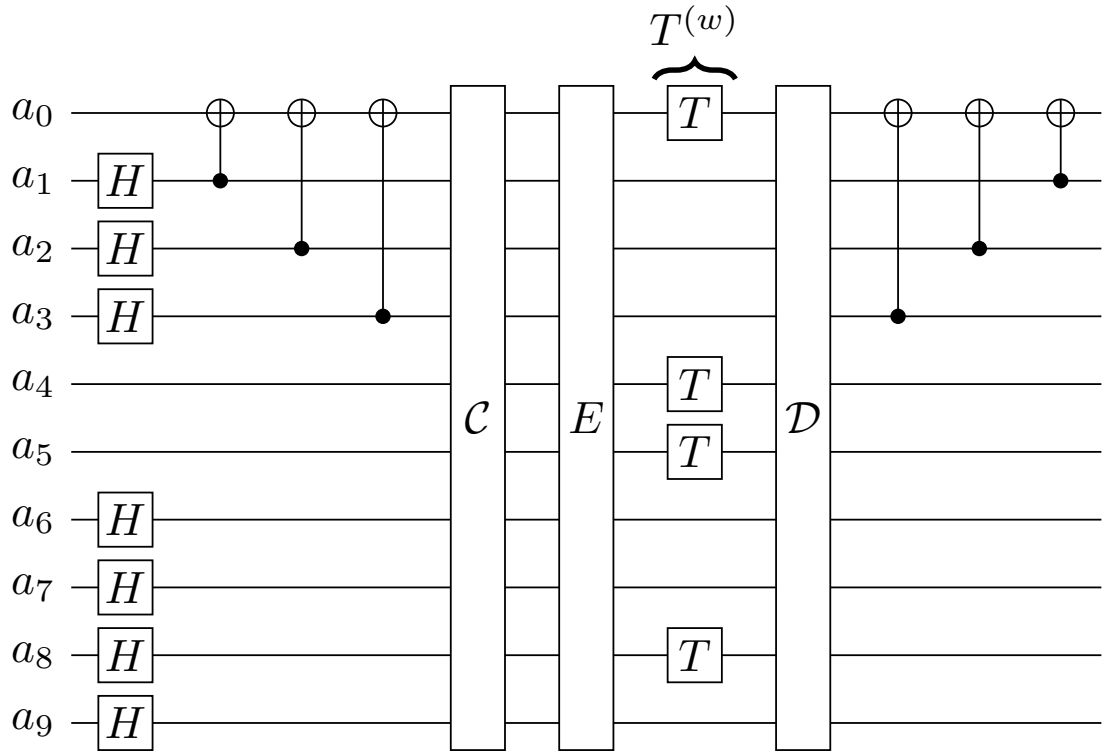

Figure 1: The circuit.

Denote by $B_1, B_2, .., B_{|w|/\Delta}$ the partion of w's bits:

$$\begin{aligned} B_1 &= \{w(1), w(2), .., w(\Delta)\} \\ B_2 &= \{w(\Delta+1), w(\Delta+2), .., w(2\Delta)\} \\ B_i &= \{w((i-1)\Delta+1), w((i-1)\Delta+2), .., w(i\Delta)\} \end{aligned}$$

Then let span $\mathcal{X}$ be all the codewords of $C_X/C_Z^\perp$ satisfying $\tilde{C}_0$ restrictions for each bucket, Let us name the union of $\tilde{C}_0$ restrictions over the buckets by B. The dimension of the space satisfies both C_X restrictions and B is at least:

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

And by the fact that the dimension of $C_Z^\perp$'s codewords satisfying B is strictly lower then $\dim C_Z^\perp$, we get the following lower bound:

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

□

Remark 2.1. *We emphasise that the above proof can be easily adapted to result the following for general CSS codes:*

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

For example lets consider the quantum Tanner code. Since the distance of the quantum Tanner codes is $\sim n/\Delta$, where Δ^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 correspond to a specific single left generator), we get that for any $\rho \in (0, \frac{1}{2})$ one there is a good qLDPC such that the dimension of span $\mathcal{X}'$ obtained respecting to it $\geq (1-2\rho)^2 n - n/\Delta\cdot(1-\rho(\tilde{C}_0))$.

Claim 2.2. *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:*

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

Proof. Let $\tau \in \text{span } \mathcal{X}' + C_Z^{\perp}$, applying $T^{(w)}$ on $|\tau\rangle$ add a phase of $i\frac{\pi}{4}\left|\tau\right|_w$. Notice that τ 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 τ. Let us denote by Λ the union of the generators. So:

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

Since span $\mathcal{X}|_w$ 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 $i\frac{\pi}{4}2|'z_j$ OR $x_0'\cdot z_i|_w$ and triple $i\frac{\pi}{4}4|'z_j$ 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.

□