

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

David Ponarovsky

August 16, 2024

## 1 Notations and Definitions.

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.

**Definition 1.1.** Let  $C, \tilde{C}$  be linear binary codes at the same length, We will say that  $\tilde{C}$  is a Triorthogonal in 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  $\tilde{C}$ .

## 2 The Construction.

Let  $x_0$  be a codeword of  $C_X/C_Z^\perp$ , Denote by  $w \in \mathbb{F}_2^n$  the binary string presents the  $Z$ -generator that anti commute with the  $X$ -generator corresponds to  $x_0$ . Let  $\mathcal{X} = \{x_0, x_1, \dots, x_{k'}\} \in \mathbb{F}_2^n$  be a subset of a base for the code  $C_X/C_Z^\perp$ . Such  $(\text{span } \mathcal{X}/x_0)|_w$  is Triorthogonal code. Let us denote by  $\mathcal{X}'$  the base  $\{y_1, y_2, \dots, y_{k'}\} \in \mathbb{F}_2^n$  defined such:  $y_i = x_j + x_0$ .

Denote by  $E$  the circuit that encodes the logical  $i$ th bit to  $y_i$ , by  $T^{(w)}$  the application of  $T$  gates on the qubits for which both  $w$  and  $x_0$  act non trivial, means  $T^{(w \cap x_0)}$  is a tensor product of  $T$ 's and identity where on the  $i$ th qubit  $T^{(w)}$  apply  $T$  if  $w_i$  and  $(x_0)_i$  are both 1 and identity otherwise. And finally by  $D$  denote the gate that decode binary strings in  $\mathbb{F}_2^n$  back into the logical space.

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

### 3 Proof of Theorem 1.

**Definition 3.1.** Let  $\Delta$  be a constant integer,  $C_0, \tilde{C}_0$  codes over  $\Delta$  bits such  $\tilde{C}_0$  is Triorthogonal and  $C_0^\perp$  contains  $\tilde{C}_0$ ,  $C_0$  has parameters  $\Delta[1, \delta_0, \rho_0]$ , and  $C_0^\top$  has relative distance greater than  $\delta_0$ . Let  $C_{\text{Tanner}}$  be a Tanner code, defined by taking an expander graph with good expansion and  $C_0$  as the small code. Let  $C_{\text{initial}}$  be the dual-tensor code obtained by taking  $(C_{\text{Tanner}}^\perp \otimes C_{\text{Tanner}}^\perp)^\perp$ . Notes that first this code has positive rate and  $\Theta(\sqrt{n})$  distance, second this code is an LDPC code as well. Notice also that  $C_{\text{initial}}^\top$  obtained by transporting the parity check matrix, and therefore equals to  $(C_{\text{Tanner}}^{\top, \perp} \otimes C_{\text{Tanner}}^{\top, \perp})^\perp$ . Hence  $C_{\text{initial}}^\top$  has a square root distance as well.

Let  $Q$  the CSS code, obtained by taking the Hyperproduct of  $C_{\text{initial}}$  with itself. So  $Q$  is an quantum qLDPC code with parameters  $[n, \Theta(n^{\frac{1}{4}}), \Theta(n)]$ .

**Claim 3.1.** 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:

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

*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  $C_{\text{Tanner}}$  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  $\Delta$ -size buckets, define by  $w(i)$  the  $i$ th coordinate on which  $w$  isn't trivial. For example if  $w(1) = j$  then  $j$  is the first nonzero coordinate of  $w$ . Denote by  $B_1, B_2, \dots, B_{\lceil w/\Delta \rceil}$  the partion of  $w$ 's bits:

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

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

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

For example lets consider the quantum Tanner code. Since the distance of the quantum Tanner codes is  $\sim n/\Delta$ , where  $\Delta^2$  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 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 3.2.** There is a family of quantum circuits  $\mathcal{C}$  consists of Clifford gates and at most  $o(\sqrt{n})$  number of  $T$  gates such that:

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

*Proof.* Let  $\tau \in \text{span } \mathcal{X}' + C_Z^\perp$ , applying  $T^{(w)}$  on  $|\tau\rangle$  add a phase of  $i\frac{\pi}{4} |\tau|_w$ . Notice that  $\tau$  can decompose to the sum of  $x_0 + y + z$  when  $y \in \text{span } \mathcal{X}$  and  $z \in C_Z^\perp$ , so

$$\begin{aligned} |\tau|_w &= |x_0 + y + z|_w \\ &= |x_0|_w + |y|_w + |z|_w - 2|x \cdot y|_w - 2|x \cdot z|_w - 2|z \cdot y|_w + 4|x_0 \cdot y \cdot z|_w \\ &= |x_0 \cdot w| + |y|_w + |z|_w - 2|y|_w - 2|z|_w - 2|z \cdot y|_w + 4|y \cdot z|_w \end{aligned}$$

Since we picked  $\tilde{C}_0 \in C_0^\perp$  then  $y \cdot z|_w = 0 \Rightarrow |y \cdot z|_w$  is even. □