

# Magic States Distillation Using Quantum LDPC Codes.

David Ponarovsky

March 6, 2024

## 1 Good Codes With Large $\Lambda$ .

**Definition 1.1.** Let  $M \in \mathbb{F}_2^{k \times n}$  upper triangular matrix such that  $k < n$ . We say that  $M$  has the 1-stairs property if  $M_{ij} = 1$  any  $j < i$ .

**Claim 1.1.** Any  $M \in \mathbb{F}_2^{k \times n}$  upper triangular matrix can be turn into upper triangular matrix that has the 1-stairs property by elementary operation.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 1 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

*Proof.* Consider the following algorithm: Let  $M$  be our initial matrix. We iterate over the rows from left to right. In the  $i$ th iteration, we check for any row  $j < i$  if  $M_{ji} = 1$ . If not, we set  $M$  to be the matrix obtained by adding the  $i$ th row to the  $j$ th row. Since  $M$  is an upper triangular matrix, adding the  $i$ th row does not change any entry  $M_{js}$  for  $s < i$ . Therefore, the obtained matrix is still an upper triangular matrix and the entries at  $M_{js}$  for  $j, s < i$  remain the same, namely 1 if and only if  $j \leq s$ .

Continuing with the process eventually yields, after  $k$  iterations, a matrix with the 1-stair property.  $\square$

**Claim 1.2.** Let  $C$  be a  $[n, k, d]$  binary linear code, and let  $\Lambda$  be subcode  $\Lambda \subset C$  at dimension  $k'$  and distance  $d'$ . Then there exists a code  $C' = [\leq 2n, \geq k - k'/2, d]$  and a subcode of it  $\Lambda'$  in it at dimension  $\geq k'/2$  and distance  $d'$ , such:

1. For every  $x \in \Lambda'$  and  $y \in C'$   $x \cdot y = 0$
2. For every  $x \in \Lambda'$  and  $y, z \in C'$   $x \cdot y \cdot z = 0$

*Proof.* First, we can assume that the generator matrix of  $C$  is an upper triangular matrix, such that the first  $k'$  rows span  $\Lambda$ . Notice that after applying the algorithm from claim 1.1 starting from the first row and stopping at the  $k'$ th row, the first  $k'$  rows are kept in  $\Lambda$ . So let's assume that is the form of the generator matrix.

Now, let's consider the following process: going uphill, from right to left, starting at the  $k'$  row. Initially, set  $j \leftarrow k'$  and in each iteration, advance it to be the index of the next row, namely  $j \leftarrow j - 1$ . In each iteration, ask how many rows  $G_m$ , such that  $m \leq j$ , satisfy  $G_m G_j = 0$  and how many pairs of rows  $G_m, G_{m'}$  such that  $m, m' \leq j$  satisfy  $G_m \cdot G_{m'} \cdot G_j = 0$ . Denote by  $p$  the probability to fall on unsatisfied equation from the above.

- If  $p \geq \frac{1}{2}$  then we move on to the next iteration.
- Otherwise, we encode the  $j$ th coordinate by  $C_0$ , which maps  $1 \rightarrow w$  such that  $w \cdot w = 0$ . This flips the value of  $G_m G_j$  for any pair and  $G_m G_{m'} G_j$  for any triple such that  $m, m' \leq j$ , so we get that the majority of the equations are satisfied. Also notice that the concatenation doesn't change the value of any multiplication at the form  $G_m G_{j'}$  for  $j' > j$ . Therefore, for any  $j < j' \leq k'$  the number of the satisfied equations relative to  $j'$  is not changed, meaning it is still the majority.

Set  $G$  to be the new matrix after the concatenation by  $C_0$ .

In the end of the process  $G$  is going to be the generator matrix of  $C'$ . It's left to construct  $\Lambda'$ , we are going to do so by taking from the  $k'$  rows a subset that satisfies the desired property in Claim 1.2.

Let  $S$  be the set of rows among the first  $k'$  rows for which there is at least one unsatisfied equation. We will now prove that if  $k'$  is large enough, specifically linear in  $k$ , then  $|S|$  is small enough to obtain  $\Lambda'$  by removing the rows in  $S$ .

Observe that the number of satisfied equations is at least:

$$\begin{aligned} & \frac{1}{2} (k' - 1 + (k' - 1)^2) + \frac{1}{2} (k' - 1 + (k' - 1)^2) + \frac{1}{2} (k' - 2 + (k' - 2)^2) + \dots + \frac{1}{2} (1 + (1)^2) \\ &= \frac{1}{2} \left( \binom{k' + 1}{2} + \frac{k'(k' + 1)(2k' + 1)}{6} \right) \end{aligned}$$

So

$$\begin{aligned} |S| \cdot k + |S| \cdot k^2 &\leq k' (k + k^2) - \frac{1}{2} \left( \binom{k' + 1}{2} + \frac{k'(k' + 1)(2k' + 1)}{6} \right) \\ \Rightarrow |S| &< k' - \frac{1}{2} \left( \frac{1}{k^2 + k} \binom{k' + 1}{2} + \frac{1}{k^2 + k} \frac{k'(k' + 1)(2k' + 1)}{6} \right) \\ \Rightarrow |S| &< k' - \frac{k'^3}{24k^2} \end{aligned}$$

Therefore, if  $k' \geq \alpha k$  we have that  $|S| < (\alpha - \frac{\alpha^3}{24})k$  implies that  $\dim \Lambda' \geq \frac{\alpha^3}{24}k$ . □

**Claim 1.3** (Not Formal). *It is easy to see that by using concatenation again, one can obtain the code  $\dim \Lambda' \leftarrow \frac{1}{2} \dim \Lambda'$ . For any  $x \in \Lambda'$ ,  $|x|_4 = 1$ , and for any  $x \in C'/\Lambda'$ , we have  $|x|_4 = 0$ .*

**[COMMENT]** The argument above that the distance  $d'$  remain the same is not correct. Yet, if we are defining the distance of any codeword in  $C/(C/\Lambda)$  to be greater than  $d'$  then we win. (The problem was that gauss elimination might change the weight of rows associate with  $\Lambda$  generators.

## 2 Distillate $|\Lambda + C_{\mathbb{Z}}^{\perp}\rangle$ Into Magic.

Let  $|f\rangle$  be a codeword in  $C_X$ , and let  $X_g$  be the indicator that equals 1 if  $f$  has support on  $X_g$ , and 0 otherwise. Observe that applying  $T^{\otimes}$  on  $|f\rangle$  yields the state:

$$\begin{aligned} T^{\otimes n} |f\rangle &= T^{\otimes n} \left| \sum_g X_g g \right\rangle = \exp \left( i\pi/4 \sum_g X_g |g| - 2 \cdot i\pi/4 \sum_{g,h} X_g X_h |g \cdot h| \right. \\ &\quad \left. + 4 \cdot i\pi/4 \sum_{g,h} X_g X_h X_l |g \cdot h \cdot l| - 8 \cdot i\pi/4 \cdot \text{integers} \right) |f\rangle \\ &= \exp \left( i\pi/4 \sum_g X_g |g| - 2 \cdot \pi/4 \sum_{g,h} X_g X_h |g \cdot h| + 4 \cdot i\pi/4 \sum_{g,h} X_g X_h X_l |g \cdot h \cdot l| \right) |f\rangle \end{aligned}$$

So in our case:

$$\begin{aligned} T^{\otimes n} |f\rangle &= \\ &= \exp \left( i\pi/4 \sum_{g \in \Lambda} X_g \right. \\ &\quad - 2 \cdot \pi/4 \sum_{g \in \Lambda, h} 2X_g X_h \\ &\quad - 2 \cdot \pi/4 \sum_{g,h \in C_{\mathbb{Z}}^{\perp}} X_g X_h |g \cdot h| \\ &\quad \left. + 4 \cdot i\pi/4 \sum_{g,h \in C_{\mathbb{Z}}^{\perp}} X_g X_h X_l |g \cdot h \cdot l| \right) |f\rangle \end{aligned}$$

So eventually, we have a product of gates when non-Clifford gates are applied on only one generator of  $C_Z^\perp$ .

$$T^n |f\rangle = \prod_{g \in \Lambda} T_g \prod_{g \in \Lambda, h} \{CZ_{g,h}|I\rangle\} \prod_{g,h \in C_Z^\perp} \{CS_{g,h}|CZ_{g,h}|I\rangle\} \prod_{g,h,l \in C_Z^\perp} \{CCZ_{g,h,l}|I\rangle\} |f\rangle$$

Decompose  $f = f_1 + f_2$ , where  $f_1$  is supported only on  $C_X/C_Z^\perp$  and  $f_2$  is supported only on  $C_Z^\perp$ . By using commuting relations, the above can be turned into.

$$T^n |f\rangle = \prod_{g \in \Lambda, h} \{CZ_{g,h}|I\rangle\} \prod_{g \in \Lambda} T_g X_{f_1} \prod_{g,h \in C_Z^\perp} \{CS_{g,h}|CZ_{g,h}|I\rangle\} \prod_{g,h,l \in C_Z^\perp} \{CCZ_{g,h,l}|I\rangle\} |f_2\rangle$$

Denote by  $M_1, M_2$  the gates:

$$M_1 = \prod_{g \in \Lambda, h} \{CZ_{g,h}|I\rangle\}$$

$$M_2 = \prod_{g,h \in C_Z^\perp} \{CS_{g,h}|CZ_{g,h}|I\rangle\} \prod_{g,h,l \in C_Z^\perp} \{CCZ_{g,h,l}|I\rangle\}$$

And then we get that

$$\prod_{g \in \Lambda} T_g |f\rangle = M_1^\dagger T^n M_2^\dagger |f\rangle$$

$$\prod_{g \in \Lambda} T_g |f\rangle = M_1^\dagger T^n E L[M_2^\dagger] |L[f]\rangle$$

$$\prod_{g \in \Lambda} (I + T_g X_g) |C_Z^\perp\rangle = M_1^\dagger T^n \prod_{g \in \Lambda} (I + X_g) E L[M_2^\dagger] |L[f]\rangle$$

**Claim 2.1.** The logical operator  $CX_g$  relative the code  $C_Z^\perp$  can be implement such it acts on constant number of qubits. **Notice**, implementation of the gate  $CX_g$  relative to  $C_Z^\perp$  might incorrect for computing  $CX_g$  relative to  $C_X$ .

**Definition 2.1** (Source of  $g \in C_Z^\perp$ ). Let  $C$  be the quantum Tanner code, and let  $g$  be a generator of  $C_Z^\perp$ . The vertex  $v$  will be called the source of  $g$ . If  $g$  is a codeword of the tensor code  $C_A \otimes C_B$ , it can be viewed locally on  $g$ .

**Claim 2.2.** Let  $Q = (C_X, C_Z)$  a good qLDPC CSS code. Then for any  $g$  generator in  $C_Z^\perp$  there is a logical gate compute  $CX_g$  acting on at most  $O(1)$  qubits.

*Proof.* Recall that the generator matrix of  $C_Z^\perp$  is the parity check matrix of  $C_Z$ . So we are looking for  $\xi$  such that:

$$H_Z \begin{bmatrix} | \\ | \\ | \\ | \\ | \end{bmatrix} \xi = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Assume that there is solution  $\xi$  for the equations system. If  $H_z$  is a parity check matrix of ltc code then  $d(\xi, C_Z) = O(1)$  so we could picck some  $z + \xi$  such that  $z \in C_Z$  and having a solution that it's weight is  $O(1)$ .

$$\sum_{r_i, l_j} |z_{r_i}\rangle |z_{l_j}\rangle = \sum_{z_{r'_i}} \sum_{r_i, l_j} |z_{r_i}\rangle |z_{l_j}\rangle |0 + \xi[z_{r'_i}] \cdot z_{r_i}\rangle \sum_{z_{l'_j}}$$

$x$

□

*Proof.* Let  $g$  be a generator of  $C_Z^\perp$ . As the generators of  $C_Z^\perp$  are defined to be the set of codewords of some 'small code' ( $C_0$ ) over the local view of the vertices in a  $\Delta$ -regular graph, it holds that first, there is a vertex  $v$  on which  $g$  is supported. Second, only the generators supported by  $v$ 's neighbors have a non-vanishing overlap with  $g$ .

Let  $g$  be a generator of  $C_Z^\perp$  and denote by  $v$  the source of  $g$ . First, we will prove that there exist  $\xi_1, \xi_2, \xi_3 \in \mathbb{F}_2^N$  such that each  $\xi_i$  has a weight of at most  $\frac{1}{2}\Delta$ ,  $\xi_i \cdot g = 1$ , and for any other generator  $h \neq g$  in  $C_Z^\perp$ , there is at least one  $i$  such that  $\xi_i \cdot h = 0$ .

Let  $B_1, B_2, B_3$  be subsets of  $[\Delta]$  such that  $|B_i| = \frac{2}{3}\Delta$  and  $B_1 \cap B_2 \cap B_3 = \emptyset$ . Now, define  $\xi_i$  to be the vector supported only on  $B_i$  and satisfies  $\xi_i \cdot g = 1$ . For any other generator  $h$  such that  $v$  is its source, and also  $h|_{B_i} \neq g|_{B_i}$ , we have  $\xi_i \cdot h = 0$ . Notice that for every  $h \neq g$ , there must be at least one  $B_i$  for which  $g|_{B_i} \neq h|_{B_i}$ . Each  $x_i$  is a solution for a linear system with (at most)  $\rho\Delta$  equations and  $\frac{1}{2}\Delta$  bits. So, if  $1/2 > \rho$ , then there is a solution for each equations system.

Clearly, for any generator  $h$  such  $v$  is it's source there are not  $i$ 's such  $\xi_i h = 1$ . It's left to show for remian generators.

□

