

# Magic States Distillation Using Quantum LDPC Codes.

David Ponnarovsky

March 7, 2024

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

**Claim 1.1.** *Let  $v_1, v_2, \dots, v_k$  vectors in  $\mathbb{F}_2^n$ , then there are  $u_1, u_2, \dots, u_{k'}$  for  $k' > k/2$ . Such  $\text{span}\{u_1, u_2, \dots, u_{k'}\} \subset \text{span}\{v_1, v_2, \dots, v_k\}$  and for any  $i, j$  it holds that  $u_i u_j = 0$ .*

*Proof.* Consider the follow algorithm,

```

1 Let  $J \leftarrow \emptyset$ 
2 for  $i \in [k/2]$  do
3    $J \leftarrow J \cup \{v_{2i-1}, v_{2i}\}$ 
4   for  $S \subset J$  do
5     Compute the vector  $m_S$  define as  $m_{S,j} = u_j \sum_{w \in S} w$ 
6   end
7   Pick  $S$  such  $m_S = 0$  and set  $u_i \leftarrow \sum_{w \in S} w$ 
8   Choose randomly  $w \in S$  and set  $J \leftarrow J/w$ 
9 end

```

**Algorithm 1:** Find commuted vectors  $u_1, u_2, \dots, u_{k'}$

Now, we are going to prove that Algorithm 1 always finds a subset  $S$  that satisfies the equality on line (7). Assume not. On one hand, the number of possible values that  $m_S$  can have is  $2^i - 1$ . On the other hand, since  $J$  contains  $i + 1$  vectors on the  $i$ th iteration, it follows that the number of subsets is  $2^{i+1} - 1 \geq 2^i$ .

Therefore, there must be at least two different subsets  $S$  and  $S'$  such that  $u_S = u_{S'}$ . However, this means that

$$\begin{aligned}
 m_{S \Delta S', j} &= u_j \sum_{w \in S \Delta S'} w = u_j \left( \sum_{w \in S \Delta S'} w + 2 \sum_{w \in S \cap S'} w \right) \\
 &= m_{S,j} + m_{S',j} = 0
 \end{aligned}$$

Thus,  $m_{S \Delta S'} = 0$ . Additionally, it is clear that the rank does not decrease, as for  $u_i$ , there exists one  $v_j$  such that only  $u_i$  is supported by  $v_j$ .  $\square$

**Claim 1.2.** *Let  $v_1, v_2, \dots, v_k$  vectors in  $\mathbb{F}_2^n$ , then there are  $u_1, u_2, \dots, u_{k'}$  for  $k' > k/4$ . Such  $\text{span}\{u_1, u_2, \dots, u_{k'}\} \subset \text{span}\{v_1, v_2, \dots, v_k\}$ . And for any  $i, j$   $\sum u_{i,k} u_{j,k} =_4 0$ .*

*Proof.* Use the Algorithm 1 twice. However, in the second iteration, define  $m_{S,j}$  to be the product of module 4. Note that  $m_{S,j}$  must be either  $4n$  or  $4n + 2$ . Thus, we can follow the proof of Claim 1.1.  $\square$

**Claim 1.3.** *Consider the Left-Right  $(\Delta, n)$ -Complex  $\Gamma$ .  $\dim C_X / C_Z^\perp \cap C_Z / C_X^\perp$  is linear in  $n$ .*

*Proof.* The rates of both  $C_X / C_Z^\perp$  and  $C_Z / C_X^\perp$  are  $(2\rho - 1)^2$ , where  $\rho$  can be any number in the range  $(0, 1)$  [LZ22]. Consider choosing  $\rho$  such that the rates of the quotient spaces are strictly greater than  $\frac{1}{2} + \alpha$ . This implies that the rate of their intersection is greater than  $2\alpha$ .  $\square$

**Corollary 1.1.** *Fix the rate of the small codes  $C_A$  and  $C_B$  to  $\rho = \frac{1}{2} + \alpha$ . There is a subspace  $\Lambda \subset C_X / C_Z^\perp$  at rate  $\frac{1}{4} \cdot 2\alpha$  such that for any  $x \in \Lambda$  and  $y \in C_Z^\perp \cup \Lambda$   $xy =_2 0$  and also for any  $x, y \in \Lambda$   $xy =_4 0$ .*

**Claim 1.4.** Let  $C$  be a  $[n, k, d]$  binary linear code, and let  $\Lambda$  be subcode  $\Lambda \subset C$  at dimension  $k' > \alpha k$  for some  $\alpha \in (0, 1)$ . Then there exists a code  $C' = [\leq 2n, \geq (1 - \alpha + \frac{\alpha^3}{24})k, d]$  and a subcode of it  $\Lambda'$  in it at dimension  $\geq \frac{\alpha^3}{24}k$ , 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 ?? 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 1.4.

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

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

Therefore, if  $k' \geq \alpha k$  we have that  $|S| < (1 - \frac{\alpha^2}{24})k'$  implies that  $\dim \Lambda' \geq \frac{\alpha^3}{24}k$ . □

**Claim 1.5.** Consider  $C, \Lambda$  and  $C', \Lambda'$  defined in Claim 1.4. Denote by  $\bar{\Lambda}$  the subspace  $C/\Lambda$ . Then:

$$d(C'/\bar{\Lambda}') \geq d(C/\bar{\Lambda})$$

*Proof.* The way we perform Guess elimination is critical. We want to make sure that we do not add an  $\Lambda$  row to a  $\bar{\Lambda}$  row. **[COMMENT]** Continue, Easy. Just need to perform the row reduction when rows of  $\Lambda$  at bottom, and then rotate the matrix  $\curvearrowright$

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \curvearrowright \begin{bmatrix} D & C \\ B & A \end{bmatrix}$$

□

**Claim 1.6** (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  $x \in \text{gen } \Lambda'$ ,  $|x|_4 = 1$ , and for any  $x \in C'/\Lambda'$ , we have  $|x|_4 = 0$ .*

*Proof.* **[COMMENT]** We will do it by iterating the generators of  $C$  after performing rows reduction to the generator matrix. Now we will concatenate the  $i$  coordinate to complete the weight of the  $i$ th row to satisfy the requirements. □

## 2 Distillate $|\Lambda + C_Z^\perp\rangle$ Into Magic.

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

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

So in our case:

$$\begin{aligned} T^{\otimes n} |f\rangle &= \\ &= \exp \left( i\pi/4 \sum_{g \in \text{gen } \Lambda} \hat{X}_g \right. \\ &\quad - 2 \cdot \pi/4 \sum_{g \in \text{gen } \Lambda, h} 2\hat{X}_g \hat{X}_h \\ &\quad - 2 \cdot \pi/4 \sum_{g,h \in \text{gen } C_Z^\perp} \hat{X}_g \hat{X}_h |g \cdot h| \\ &\quad \left. + 4 \cdot i\pi/4 \sum_{g,h \in \text{gen } C_Z^\perp} \hat{X}_g \hat{X}_h \hat{X}_l |g \cdot h \cdot l| \right) |f\rangle \end{aligned}$$

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

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

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.

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

Denote by  $M_1, M_2$  the gates:

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

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

And then we get that

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

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

**Claim 2.1.** *The state  $(M_2^\dagger \otimes I) |C_Z^\perp + \Lambda\rangle |0\rangle$  can be computed, such that the light cone depth of any non-clifford gate is bounded by constant.*

*Proof.*

$$\begin{aligned} (I \otimes H_X) CX_{n \rightarrow n} (E \otimes E) I \otimes L[M_2^\dagger] \prod_{\substack{J \in \{\text{gen } \Lambda, g \in J \\ \text{gen } C_Z^\perp\}}} \prod (I + X_{L[g]}) & |0\rangle |0\rangle \\ = (I \otimes H_X) CX_{n \rightarrow n} \sum_{\substack{z \in C_Z^\perp \\ x \in \Lambda}} e^{\varphi(z)} & |x\rangle |z\rangle \\ = \sum_{\substack{z \in C_Z^\perp \\ x \in \Lambda}} e^{\varphi(z)} & |x+z\rangle |0\rangle \\ = \sum_{\substack{z \in C_Z^\perp \\ x \in \Lambda}} (M_2^\dagger \otimes I) & |x+z\rangle |0\rangle \\ = (M_2^\dagger \otimes I) & |C_Z^\perp + \Lambda\rangle |0\rangle \end{aligned}$$

□

Denote by  $p \in [0, 1]$  the error rate of input magic states, and let  $|A\rangle$  be an ancilla initialized to a one-qubit magic state. This  $|A\rangle$  can be used to compute the  $T$  gate, with a probability of  $Z$  error occurring with a probability of  $p$  [BF12].

**Claim 2.2.** *There are constant numbers  $\zeta_\Delta, \xi_\Delta$ , and a circuit  $\mathcal{C}$  such that:*

1. *In the no-noise setting, The circuit compute the state*

$$\mathcal{C} |0\rangle^{\Theta(n)} \otimes |A\rangle^{\Theta(n)} \rightarrow \prod_{g \in \text{gen } \Lambda} T_g |C_Z^\perp + \Lambda\rangle$$

2. *Otherwise, the circuit computes the state*

$$\mathcal{C} |0\rangle^{\Theta(n)} \otimes |A\rangle^{\Theta(n)} \rightarrow Z^e \prod_{g \in \text{gen } \Lambda} T_g |C_Z^\perp + \Lambda\rangle$$

, where the probability that  $e_i = 1$  is less than  $\zeta_\Delta \cdot p$ . Additionally, for any  $i$ , there are at most  $\xi_\Delta$  indices  $j$  such that  $e_i$  and  $e_j$  are dependent.

*Proof.* Concatenate the  $T^n \otimes I$  with the gate in Claim 2.1. □

**Claim 2.3.** For any  $\alpha \in (0, 1)$  the probability that  $|e| > (1 + \alpha)p\zeta_\Delta$  is less than:

$$\Pr[|e| > (1 + \alpha)\mathbf{E}[|e|]] < \frac{\zeta_\Delta(1 - \zeta_\Delta p)}{\alpha^2 \xi_\Delta p n} = o(1/n)$$

*Proof.* By the Chebyshev inequality, notice that the number for which  $\mathbf{E}[e_i e_j] - \mathbf{E}[e_i] \mathbf{E}[e_j] \neq 0$  is less than  $\xi_\Delta n$ . □

**Definition 2.1.** We will said that a decoder  $\mathcal{D}$  for the good quantum LDPC code is an good-local decoder if

1. There is a threshold  $\mu n$  such that if the error size is less than  $|e| < \mu n$  then  $\mathcal{D}$  correct  $e$  in constant number of rounds. With probability  $1 - o(1/n)$ .
2. In any rounds  $\mathcal{D}$  performs at most  $O(n)$  work (depth  $\times$  width).
3. The above is true in operation-noisy settings, where there is a probability of  $p$  for an error to occur after acting on a qubit. (★)

★ The motivation for this is that if the decoder does not act on the qubit, then it also does not apply a  $T$  gate on it. Therefore, in the distillation setting, there is zero chance for an error to occur.

**Claim 2.4.** Suppose there is a good local decoder  $\mathcal{D}$  for the good qLDPC code. Then, there exists  $p_0$  such that for any sufficiently large  $n$ , there is a distillation protocol that, given  $\Theta(n)$  magic states at an error rate  $p < p_0$ , successfully distills  $\Theta(n)$  perfect magic states with a probability of  $1 - o(1/n)$ . Furthermore, the protocol's space and time complexity (both quantum and classical) are  $\Theta(n)$  and  $\Theta(n^2)$ , respectively.

## References

- [BH12] Sergey Bravyi and Jeongwan Haah. “Magic-state distillation with low overhead”. In: *Physical Review A* 86.5 (2012), p. 052329.
- [LZ22] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. 2022. arXiv: [2202.13641](https://arxiv.org/abs/2202.13641) [quant-ph].