Magic States Distillation Using Quantum LDPC Codes.

David Ponarovsky

April 1, 2024

1 Current Status.

1. Section 5 - Correct. In any CSS code, one can find a large subspace $\Lambda \subset C_X$ with a dimension that is linear in n and this subspace also satisfies the required relation for distillation. Specifically, for any $x \in \Lambda, y, z \in C_X$, it holds that $xy = 0$ and $xyz = 0$.

2. Sections 6 and 7 - Incorrect. Initially, I believed that assuming the code is LDPC, one could encode the state $C_Z^{\frac{1}{}}$ in constant depth. However, this idea turned out to be incorrect both in calculation and in contrast to the fact that synthesizing the ground state of the Toric code requires $\Omega(\log n)$ depth.

2 Classic Codes With Few Checks.

Claim 2.1. *There is a family of classic binary codes, with positive rate, $\Theta(n^{\frac{1}{3}})$ distance, and $\gamma n^{\frac{1}{3}}$ checks.*

Proof. We are going to show the existences of bipartite expander, over n left vertices and $\gamma n^{\frac{1}{3}}$ right vertices such that for any $S \subset L$ at size at most $\alpha n^{\frac{1}{3}}$, the neighbors of S is at size at least $\beta|S|$. We use the standard probabilistic 'fusion construction', meaning that we are going to sample permutation from $[n \times d_1]$ to $[n^{\frac{1}{3}} \times d_2$ and fuse together d_1's left vertices subsets $\{d_1 \cdot j, d_1 \cdot j + 1, d_1 \cdot j + 2, .., d_1 \cdot (j + 1) - 1\}$ and similarly fuse together d_2 right vertices.

Now observes that the probability of neighbors $S \subset L$ being contained in $T \subset R$ is at most:

$$\mathbf{Pr}\left[X_{S,T}\right] \leq \frac{|T|d_2 \cdot (|T|d_2 - 1) \cdots (|T|d_2 - |S|d_1)}{nd_1 \cdot (nd_1 - 1) \cdots (nd_1 - |S|d_1)} \leq \left(\frac{|T|d_2}{nd_1 - |S|d_1}\right)^{|S|d_1}$$

And for the $|T| < \beta|S|$ the above is lower than:

$$\mathbf{Pr}\left[X_{S,T}\right] \leq \left(\frac{2\beta|S|d_2}{nd_1}\right)^{|S|d_1}$$

By the union bound we get that the probability that there exist S at size $|S| < \alpha n^{\frac{1}{3}}$ such that the neighbors of S is at size less than $\beta|S|$ is bounded by:

$$
\begin{aligned}
\mathbf{Pr}\left[\bigcup_{\substack{|S|<\alpha n^{\frac{1}{3}}\\|T|<\beta|S|}}\right] &\leq \sum_{\substack{|S|<\alpha n^{\frac{1}{3}}\\|T|<\beta|S|}} \mathbf{Pr}\left[X_{S,T}\right]\\
&\leq \sum_{k\geq 1}^{\alpha n^{\frac{1}{3}}} \binom{n}{k}\binom{\gamma n^{\frac{1}{3}}}{\beta k}\cdot\left(\frac{2\beta k d_2}{n d_1}\right)^{k d_1}\\
&\leq \sum_{k\geq 1}^{\alpha n^{\frac{1}{3}}} \left(\frac{e^{2+\beta}}{k}\cdot\frac{n^{1+\beta/3}}{\beta^{\beta}k^{\beta}}\cdot\left(\frac{2\beta k d_2}{n d_1}\right)^{d_1}\right)^{k}\\
&= \sum_{kge1}^{\alpha n^{\frac{1}{3}}} \left(\frac{e^{2+\beta}}{k}\cdot\frac{n^{1+\beta/3}}{\beta^{\beta}k^{\beta}}\cdot\left(\frac{2\beta k n^{2/3} d_1}{n d_1}\right)^{d_1}\right)^{k}\\
&= \sum_{k\geq 1}^{\alpha n^{\frac{1}{3}}} \left(\frac{e^{2+\beta}(2\beta)^{d_1}}{\beta^{\beta}}\cdot\frac{k^{d_1-\beta-1}}{n^{d_1/3-\beta/3-1}}\right)^{k}\\
&\leq \sum_{k\geq 1}^{\infty} \left(\frac{e^{2+\beta}(2\beta)^{d_1}}{\beta^{\beta}}\cdot\gamma^{d_1-\beta/3-\frac{1}{3}}\right)^{k}
\end{aligned}
$$

□

3 Candidate For Triorthogonal LDPC Code.

Claim 3.1. *Consider the ring $\mathbb{F}_q[x]$ where q is a prime number. Let $\Delta = 4^c$ where $c \geq 3$. Then we have:*

$$\sum_{x\in[\Delta]} x^i =_{\Delta} \in \{0\ ,\ \Delta/2\}$$

Proof. By induction on c.

1. Base. For $c = 3$ we computes the summation bruthforcely.
2. Assumption. Assume the correctness of the claim for $c - 1$.
3. Step. Denote by $B_j(\Delta)$ the bucket $\Delta\cdot j+1, \Delta\cdot j+2, ..\Delta\cdot(j+1)-1$. Observes that:

   $$\sum_{x\in B_{j+1}(\Delta)} x^i =_{\Delta} \sum_{x\in B_{j+1}(\Delta)} (x-\Delta)^i =_{\Delta} \sum_{x\in B_j(\Delta)} x^i$$

   On the other hand, by the induction assumption, there is some integer a for which:

   $$\sum_{x\in B_1(\Delta/4)} x^i = \Delta/8\cdot a$$

   Thus the summation over Δ elements equals to:

   $$\sum_{x\in[\Delta]} x^i = \sum_{j\in[4]}\sum_{x\in B_j(\Delta/4)} x^i = \Delta/8\cdot a\cdot 4 = \Delta\cdot a/2$$

□

Definition 3.1. *Let $G = (L, R, E)$ be a bipartite graph, and let Δ be an integer. Define G' to be the graph: $G' = (\Delta \times L, R, E')$ defined as follows:*

$$E' = \{\{(i, v), u\} : i \in [\Delta], \{u, v\} \in E\}$$

In addition, we define the equivalence relation $u \sim v$ for $u, v \in \Delta \times L$ to hold if the first coordinates of u and v are equal.

Let G' be a graph constructed as described above. Consider the code C over the $\mathbb{F}_q$ alphabet, defined as all the assignments of symbols from $\mathbb{F}_q$ to the $\Delta \times L$ vertices. Such any vertex on the right side of G sees a polynomial of degree at most d on its local view, in addition the x's value of bit in $\Delta \times L$ is the same module Δ for all the checks. To clarify, if one checks, treat $u \in \Delta \times L$ as the value of the polynomial at coordinate z, and treat the other check as the value of the polynomial at coordinate z', then $z =_\Delta z'$.

Claim 3.2. *C is a good LDPC code. (If G is expander graph).*

Proof. We obtain a lower bound on the code dimension by subtracting restrictions. So,

$$\dim C = \Delta \cdot |L| - |R| \cdot (1 - \rho) \cdot q$$

Now, assume trough contradiction that there is $x \in C$ at weight $|x| < \gamma n$ denote by $S' \subset \Delta \times L$ the set of vertices setted to a non-trivial symbol. And observes that in the original graph G, S' induce a set of vertices S by taking the delegations of the equivalence classes.

Since G is a (n, m, γ, α) expander, and $|S| < |S'| < \gamma n$, it followees that $|\Gamma(S)| > \alpha|S| \Rightarrow$

$$\begin{aligned} |S|/|\Gamma(S)| &< \frac{1}{\alpha} \\ \Rightarrow |S'|/|\Gamma(S)| &< \frac{\Delta}{\alpha} \end{aligned}$$

So there is a check that sees a local view at weight less than $\frac{\Delta}{\alpha}$ bits. (Otherwise, $|S'| > |\Gamma(S)| \cdot \frac{\Delta}{\alpha}$). So, if $\frac{\Delta}{\alpha}$ is lower than C_0 distance we get a contradiction. ☐

Claim 3.3. *Let h_1, h_2, h_3 be arbitrary checks of C, not necessarily different. Then:*

$$\begin{aligned} h_1 h_2 &=_4 0 \\ h_1 h_2 h_3 &=_4 0 \end{aligned}$$

Proof. Complete it. ☐

Consider the Tanner **Graph**, such that the graph G is bipartite, and every two checks overlap on the ith bucket, Δ-size, bits. So for any two checks, we have that

$$\begin{aligned} \sum_{x=i\cdot\Delta}^{(i+1)\Delta} x^j &=_\Delta \sum_{x'=(i-1)\cdot\Delta}^{i\Delta} (x' + \Delta)^j \\ &=_\Delta \sum_{x=(i-1)\cdot\Delta}^{i\Delta} x'^{,j} = \sum_{x \in \mathbb{F}_\Delta} x^j \\ \sum_{x \in \mathbb{F}_\Delta} (x + a\Delta)^i (x + b\Delta)^j &= \sum_{x \in \mathbb{F}_\Delta} x^{i+j} \end{aligned}$$

So it's left to show that if we take the bipartite graph to be an expander graph then we have a good code.

Let G be a bipartite graph $G = (L, R, E)$ that is a (n, m, γ, α) expander. This means that for any subset $S \subset V(G)$ with $|S| < \gamma n$, the size of the group of neighbors of S is at least $\Gamma(|S|) > \alpha|S|$. Consider the graph $G' = (\Delta \times L, R, E')$ defined as follows:

$$E' = \{\{(i, v), u\} : i \in [\Delta], \{u, v\} \in E\}$$

Thus for any $S \subset \Delta \times L$ if $|S|/\Delta < \gamma n$ we have that: $\Gamma'(S) < \Gamma(|S|/\Delta)$.

Therefore, if S is the set of vertices associated with the non-trivial symbols induced by the assignment of a codeword on the vertices, then if $|S| < \gamma n$, we have:

$$\frac{|S|}{\Gamma'(|S|)} \leq \frac{|S|}{\Gamma(|S|/\Delta)} \leq \frac{\Delta}{\alpha}$$

So there is a check that sees on his local view less than Δ/α non-trival bits $< d(C_0)$.

4 Hyprproduct Code of two Triorthogonal Codes.

Suppose that H is a parity check matrix scuh that $h_i h_j =_\Delta \in \{\Delta, \ , \ \Delta/2\}$ for any two rows. IS that true that the same property holds for the following check matrix?

$$H' \leftarrow [H \otimes I | I \otimes H]$$

$$H'_i H'_j = (H \otimes I)_i (H \otimes I)_j + (I \otimes H)_i (I \otimes H)_j$$

Denote $i = (i_1, i_2)$ and $j = (j_1, j_2)$. So:

$$(H \otimes I)_i (H \otimes I)_j = \delta_{i_2, j_2} H_{i_1} H_{j_1}$$

and

$$(I \otimes H)_i (I \otimes H)_j = \delta_{i_1, j_1} H_{i_2} H_{j_2}$$

5 The problem with the above.

The code that is obtained by the polynomial tanner is (almost) self dual code, module Δ the multiplication $x \cdot x$ belongs to $\{0, \Delta/2\}$. While what we actually want to have is $x \cdot x =_4 1$. An idea how to correct that, sets the checks such only two of them don't commute. After taking the Hyprproduct code, they will turned to $\Theta(\sqrt{n})$ that don't commute. So if we have a perfect $\Theta(\sqrt{n})$ T states, we can cancel their phase before the encoding.

Let B be the bucket which matches $\{2, 3, ..\Delta - 1\}$. On that bucket, the multiplication of the checks corresponds to $\sum_{x \in \mathbb{F}_\Delta} x^i - 1^i$, which is $\in \{-1, \Delta/2 - 1\}$. On the otherhand, the codeword ξ that corresponds to the constant function $f(x) = 1$ in every bucket gives $\xi \cdot \xi =_\Delta -1$.

So $\xi' = \xi \otimes I$ padding with zeros, is a codeword of the Hyprproduct code, such that $\xi' \cdot \xi' = 1$.

6 Good Codes With Large Λ.

Claim 6.1. *Let $v_1, v_2..v_k$ vectors in $\mathbb{F}_2^n$, then there are $u_1, u_2..u_{k'}$ for $k' > k/2$. Such span $\{u_1, u_2..u_{k'}\} \subset$ span $\{v_1, v_2..v_k\}$ and for any i, j it holds that $u_i u_j = 0$.*

Proof. Consider Algorithm 1a, We are going to prove that at line number (8) the alg always finds a subset S that satisfies the equality. 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 ith 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

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

Let $J \leftarrow \emptyset$
for $i \in [k/2]$ **do**
  $J \leftarrow J \cup \{v_{2i-1}, v_{2i}\}$
  for $S \subset J$ **do**
    Compute the vector m_S define as $m_{S,j} = u_j \sum_{w \in S} w$
  end
  Pick S such $m_S = 0$ and set $u_i \leftarrow \sum_{w \in S} w$
  Choose randomly $w \in S$ and set $J \leftarrow J/w$
end
: Find commuted vectors $u_1, u_2, ..u_{k'}$

Let $J \leftarrow \emptyset$
for $i \in [k/3]$ **do**
  $J \leftarrow J \cup \{v_{3i-2}, v_{3i-1}, v_{3i}\}$
  for $S \subset J$ **do**
    Compute the vector m_S define as $m_{S,j,j'} = u_{j'} u_j \sum_{w \in S} w$
  end
  Pick S such $m_S = 0$ and set $u_i \leftarrow \sum_{w \in S} w$
  Choose randomly $w \in S$ and set $J \leftarrow J/w$
end
: Find commuted vectors $u_1, u_2, ..u_{k'}$

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. □

Claim 6.2. *Let $v_1, v_2..v_k$ vectors in $\mathbb{F}_2^n$ and m be an integer $m < k$, then there are $u_1, u_2..u_{k'}$ for $k' > k/2 - m$. Such span $\{u_1, u_2..u_{k'}\} \subset$ span $\{v_{m+1}, v_{m+2}..v_k\}$, for any i, j it holds that $u_i u_j = 0$ and for any $i \in]k'$, $j \leq m$ it holds that $u_i v_j = 0$.*

Proof. Modify the Algorithm 1a as follows, Initialize $u_1, .u_m$ to be $v_1, .., v_m$ and $J = \{v_{m+1}, ..v_{2m+2}\}$. Notice that in the ith iteration, for the counting argument to works in the proof of Claim 6.1, we have to ensure that:

$$|J| \geq m + i + 1, \text{So } m + i + 1 \leq k - m - i$$
$$\Rightarrow i \leq k/2 - m - \frac{1}{2}$$

In the end, $u_{m+1}, u_{m+2}, .., u_{k'}$ will satisfy the equations. □

Claim 6.3. *Let $v_1, v_2..v_k$ vectors in $\mathbb{F}_2^n$, then there are $u_1, u_2..u_{k'}$ for $k' > k/4$. Such span $\{u_1, u_2..u_{k'}\} \subset$ span $\{v_1, v_2..v_k\}$. And for any i, j $\sum u_{i,k} u_{j,k} =_4 0$.*

Proof. Use the Algorithm 1a 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 6.1. □

Claim 6.4. *[COMMENT] Complete for the above the version, which handle triples. number of options is $(2^i)^2 = 2^{2i}$ and therefore we have the correctness if $|J| > 2i + 1$.*

Claim 6.5. *Consider the Left-Right (Δ,n)-Complex Γ. $\dim C_X/C_Z^{\perp} \cap C_Z/C_X^{\perp}$ is linear in n.*

Proof. The rates of both $C_X/C_Z^{\perp}$ and $C_Z^{\perp}/C_X^{\perp}$ are $(2\rho - 1)^2$, where ρ can be any number in the range $(0, 1)$ [LZ22]. Consider choosing ρ 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 2α. □

Corollary 6.1. *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 $y, z \in C_Z^{\perp} \cup \Lambda$ it holds that:*

1. $xy =_4 0$
2. $xyz =_4 \sum_i x_i y_i z_i =_4 0$

Claim 6.6. *Consider C, Λ and C', Λ' defined in ??. Denote by $\bar{\Lambda}$ the subspace C/Λ. 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 Λ row to a $\bar{\Lambda}$ row. **[COMMENT]** Continue, Easy. Just need to perform the row reduction when rows of Λ 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 6.7 (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* $x \in$ *gen* Λ', $|x|_4 = 1$*, 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 ith row to satisfy the requirements. □

7 Compute $|C_Z^{\perp}\rangle$ In Constant Depth. [COMMENT] Wrong Section.

Let C_0 be a Δ-length error linear binary code, Γ a Δ-regular bipartite graph, and let C_Z be the Tanner code defined by C_0 and Γ. We are about to prove that the uniform superposition over $C_Z^{\perp}$ codewords can be computed with constant probability at a depth dependent only on Δ, in particular independent of the $C_Z^{\perp}$-length. For this, we are going to use Proposition 10 in [MN98], which states that both the encoder and the decoder of any stabilizer m-length code can be implemented by a circuit at depth $\Theta(\log m)$ with $\Theta(m^2)$ ancillae.

Claim 7.1. *Let G be a Δ-regular bipartite graph, and denote by $C_Z^{\perp}$ the dual-tanner code $\mathcal{T}(G, C_0^{\perp})^{\perp}$. Then there is a circuit that with constant probability computes the state $|C_Z^{\perp}\rangle$ at $\Theta(\log \Delta)$ depth, and $\Theta(\Delta^2)n$ ancillary qubits.*

Proof. Let E_v and D_v be the encoder and the decoder of C_0 over the local view of vertex v, By [MN98] we have that both have depth $\Theta(\log \Delta)$ and require Δ^2 ancillae. Since Γ is bipartite, we can decompose V into V^- and V^+ such that the local views of any two vertices in $V^{\pm}$ are disjoint. Therefore, for any two different vertices $v, u \in V^{\pm}$, the encoders E_v and E_u act on disjoint subsets of qubits, each corresponding to the local view of either v or u. Consider the following algorithm:

1 Initialize $2n$ qubits.
2 Call the left and right segments L and R.
3 Apply E_v in parallel on L for any $v \in V^+$.
4 Apply E_v in parallel on R for any $v \in V^-$.
5 XOR R into L by applying CNOT from the ith bit of R to the ith bit of L.
6 Apply D_v in parallel on R for any $v \in V^-$.
7 Apply H^k on L. And measure.
8 Accept if the result in C_Z

Algorithm 1: Compute $|C_Z^{\perp}\rangle$

For any $v \in V$, let $|z_v\rangle$ be the superposition of codewords in C_0 supported by the local view of v. Similarly, for any subset of vertices $W \subset V$, let $|z_W\rangle$ be the uniform superposition over the subspace spanned by the generators supported by the vertices in W. In other words:

$$|z_W\rangle = |\sum_{v \in W} z_v\rangle$$

Using the notation, applying the encoders E_v, E_u for any pair of vertices with disjoints local view become:

$$\begin{aligned} E_v \cup E_u \left|0\right\rangle^n &= E_v \left|0 + z_u\right\rangle = E_v \left|0_{/u\text{'s view}}\right\rangle \otimes \left|z_u\right\rangle \\ &= |z_v\rangle \, |z_u\rangle = |z_u + z_v\rangle = |z_{\{u,v\}}\rangle \end{aligned}$$

So applying all the encoders E_v at once over the positive vertices results in:

$$\left(\cup_{v\in V^+}E_v\right)|0\rangle^n = \left(\cup_{v\in V^+/v_0}E_v\right)|z_{v_0}+0\rangle = |z_{V^+}\rangle$$

Thus the whole computation sum up into:

$$\begin{aligned}
\left(\cup_{v\in V^+}E_v\right)\otimes\left(\cup_{v\in V^+}E_v\right) && |0\rangle^n\otimes|0\rangle^n \mapsto \\
\text{CNOT}\sum_{z\in A}\sum_{z'\in B} && |z_{V^+}\rangle|z_{V^-}\rangle \mapsto \\
I\otimes H^k\sum_{z\in A}\sum_{z'\in B} && |z+z'\rangle|z'\rangle \mapsto \\
\sum_{z\in A}\sum_{z'\in B} && |z+z'\rangle(-1)^{wz'}|w\rangle \mapsto
\end{aligned}$$

So if $w\in C_Z$ then clearly $z'w=0$. The probability for that to occur is

$$\mathbf{Pr}\left[w\in C_Z\right] = \frac{|C_Z|}{\mathbb{F}_2^n} = 2^{(\rho-1)n}$$

□

8 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:

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

So in our case:

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

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

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

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.

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

Denote by M_1, M_2 the gates:

$$M_1 = \prod_{g \in \text{ gen } \Lambda, h} \{CZ_{g,h}|I\}$$
$$M_2 = \prod_{g,h \in \text{ gen } C_Z^{\perp}} \{CS_{g,h}|CZ_{g,h}|I\} \quad \prod_{g,h,l \in \text{ gen } C_Z^{\perp}} \{CCZ_{g,h,l}|I\}$$

And then we get that

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

Claim 8.1. *Let $v \in V^-$, and let g_1 be the generator supported by v, which matches an assignment of a codeword in $C_A \otimes C_B$ on the local view of v. Denote by U_{v,g_1} the control-gate which, depending on the control bit $(v, 1)$, turns on g_1 over the edges associated with the local view of v in the graph G. Then, the depth of U_{v,g_1} depend only on Δ.*

Claim 8.2. *Let (v, g_1) and (u, g_2) be control wires for two different generators in the graph G. Then U_{v,g_1} and U_{u,g_2} **[COMMENT]** There must be a claim about the relationship between two different generators intersection, But I don't sure exactly why.*

Definition 8.1. *We say that a quantum circuit C is well error spreading if the light cone define by any T.*

Claim 8.3. *The state:*

$$\sum_{z \in C_Z^{\perp}} \exp\Big(-2 \cdot \pi/4 \sum_{g,h \in \text{ gen } C_Z^{\perp}} \hat{X}_g \hat{X}_h |g \cdot h| \\ + 4 \cdot i\pi/4 \sum_{g,h \in \text{ gen } C_Z^{\perp}} \hat{X}_g \hat{X}_h \hat{X}_l |g \cdot h \cdot l| \Big) \left|z\right\rangle$$

Can be computed such that any

Proof. Denote by U_v the gate which turn on all the generators supported on v. As any of them is just of a code word of $C_A \otimes C_B$, namely turning on generator require touching at most constant number of qubits combing □

Claim 8.4. *The state $\left(M_2^{\dagger} \otimes I\right) \left|C_Z^{\perp} + \Lambda\right\rangle \left|0\right\rangle$ can be computed, such that the light cone depth of any non-clifford gate is bounded by constant.*

Proof.

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

□

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 [BH12].

Claim 8.5. *There are constant numbers ζ_Δ, ξ_Δ, and a circuit $\mathcal{C}$ such that:*

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

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

2. *Otherwise, the circuit computes the state*

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

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

Proof. Concatinate the $T^n \otimes I$ with the gate in Claim 8.4. □

Claim 8.6. *For any $\alpha \in (0,1)$ the probability that $|e| > (1+\alpha)p\zeta_\Delta$ is less than:*

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

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

Definition 8.2. *We will said that a decoder $\mathcal{D}$ for the good qunatum LDPC code is an good-local decoder if*

1. *There is a treashold μn 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. ($\star$)*

⋆ *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 8.7. *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

[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.

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