Magic States Distillation Using Quantum LDPC Codes.

David Ponarovsky

March 7, 2024

1 Good Codes With Large Λ.

Claim 1.1. *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 the follow algorithm,

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

Algorithm 1: Find commuted vectors $u_1, u_2, ..u_{k'}$

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 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

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

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 $v_1, v_2..v_k$ 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 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 (Δ,n)-Complex Γ and let $C_0 = C_A \otimes C_B^\perp \oplus C_A^\perp \otimes C_B$. Then the Tanner code $\mathcal{T}(V_+, C_0)$ is:*

1. *Has a positive rate.*
2. *Disjoints to $C_Z^\perp$.*

Claim 1.4. *Let C be a $[n,k,d]$ binary linear code, and let Λ 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 Λ' 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 Λ. 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 Λ. 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 jth coordinate by C_0, which maps $1 \to w$ 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 Λ', 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 Λ' by removing the rows in S.

Observe that the number of satisfied equations is at least:

$$\frac{1}{2}\left(k'-1+(k'-1)^2\right)+\frac{1}{2}\left(k'-1+(k'-1)^2\right)+\frac{1}{2}\left(k'-2+(k'-2)^2\right)+..+\frac{1}{2}\left(1+(1)^2\right)$$
$$=\frac{1}{2}\left(\binom{k'+1}{2}+\frac{k'(k'+1)(2k'+1)}{6}\right)$$

So

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

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

Claim 1.5. *Consider C, Λ and C', Λ' defined in Claim 1.4. 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 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* $x \in$ *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. □

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:

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

So in our case:

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

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

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

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.

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

Denote by M_1, M_2 the gates:

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

And then we get that

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

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

Proof.

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

□

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 2.2. *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 2.1. $\square$

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

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

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 $\xi_\Delta n$. $\square$

Definition 2.1. *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. ($\star$)*

$\star$ *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 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.*

Claim 2.5. *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 2.2 (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 2.6. *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 ξ such that:

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

Assume that there is solution ξ 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 $O(1)$.

$$\sum_{r_i, l_j} |z_{r_i}\rangle |z_{l_j}\rangle = \sum_{z_{r_i'}} \sum_{r_i, l_j} |z_{r_i}\rangle |z_{l_j}\rangle |0 + \xi[z_{r_{i'}}] \cdot z_{r_i}\rangle \sum_{z_{l_j'}}$$

$$x$$

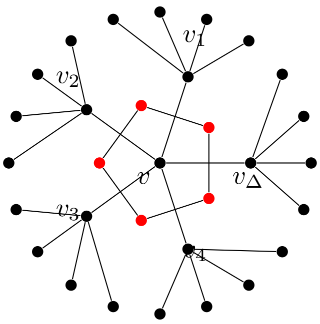
$\square$

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 Δ-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 ξ_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 ξ_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. $\square$



Definition 2.3. *Let $\{h_i\}_1^t$ be the checks of Δ-length code C_0. We say that ith bit and the jth bit collide if there a check h such that $h_i = h_j = 1$. We say that a C_0 is a checks-hashed if:*

$$\mathbf{Pr}_{i,j\sim[\Delta]^2}\left[i, j \text{ collide}\right] < \frac{1}{2\Delta}$$

Claim 2.7. *Suppose that $C_0^{\perp}$ is a checks-hashed. Then $\left(C_0^{\otimes m}\right)^{\perp}$ is also a checks-hashed.*

Proof.

$$\begin{aligned}\mathbf{Pr}_{u,v\sim[n]^2}\left[X_{u,v}^{(m)}\right] &\leq \mathbf{Pr}_{u,v\sim[\Delta]^2}\left[X_{u,v}^{(1)}\right] \cdot \mathbf{Pr}_{u,v\sim[n/\Delta]^2}\left[X_{u,v}^{(m-1)}\right] \\ &\leq \frac{1}{2\Delta} \cdot \left(\frac{1}{2\Delta}\right)^{m-1} = \left(\frac{1}{2\Delta}\right)^{m}\end{aligned}$$

$\square$

Consider the following decoder, we flip a bit if flipping it decrease the syndrome. Now observers that if a non faulty bit i has been flip then it means that there is at least one faulty bit j in the error e that i, j collide. Similarly if a faulty bit i hasn't been flip then it means that there is another faulty bit j that collide with him. In overall we conclude that the total number of incorrect flips made by the decoder is at most the number of collisions.

$$\mathbf{E}\left[\sum_{v\in e}\sum_{u\in[n]} X_{v,u}\right] \leq |e| \cdot n \cdot \left(\frac{1}{2\Delta}\right)^{m} = \frac{|e|}{2^m}$$

Now we are going to add a random error at weight $\frac{|e|}{2^m}$ to ensure that in the next iteration the $\frac{|e|}{2^{m-1}}$ error will distributed uniformly. Repeating for $\log_{2^{m-1}}$ rounds correct the error. (not exactly there is an error in each round that should be handled).

[COMMENT] We flip in over all $|e|\sum \frac{1}{2^i} < 2|e|$ bits, so we would like to have $|e| \leq d/4$.
[COMMENT] Yet we can do better, if $e = z + \tilde{e}$ where z commute with all our generators.
[COMMENT] And if it anticommute with only l of them, then we have only l errors.

$$\Delta^m \leq 1/p_0^2 \to \alpha \cdot 1/p_0^2, \frac{m}{2^m}\log\Delta$$

Claim 2.8. *Let H be a $|V| \times r$ binary parity check matrix of $\tilde{C}$. Also, let G be a Δ-regular graph. A bit assignment over G edges x will be said to be $\tilde{C}$-vertices-respect if the vector $z(x) \in \mathbb{F}_2^{|V|}$ which is defined as:*

$$z(x)_v = \begin{cases} 1 & v \text{ sees at least one } 1 \\ 0 & \text{otherwise} \end{cases}$$

is a codeword of $\tilde{C}$. Let Λ be the set of all $\tilde{C}$-vertices-respect assignments. Then $|\Lambda| > (1-\varepsilon)2^{\rho|V|}$.

Proof. Any $x \in \Lambda$ is a solution for the following system of equations:

$$\begin{aligned} z_v &= 1 + \prod_{e\in v}(1 - x_e) \\ Hz &= 0 \end{aligned}$$

□

Claim 2.9. *Assume that C_0 is a Δ-length code such that for any two non-trival codewords $c, c' \in C_0$ we have that $c \cdot c' = 1$, and denote by $C = \mathcal{T}(G, C_0)$. And let Λ be a the set of all $\tilde{C}$-vertices-respect assignments where $\tilde{C}$ satisfies relation R. Then also $C \cap \Lambda$ satisfies R.*

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. Observes that applying $T^{\otimes}$ on $|f\rangle$ yilds the state:

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

3 Many to One.

Assume that f is supported on exactly one generator. Then we have that $T^{\otimes n}|f\rangle = e^{i\pi|g|/4}|f\rangle$ Therefore, if $|g| = 4k+1$ then we are done.

4 Using Quntum Error Correction Codes.

Now assume that the code C_X is the quantum Tanner code, denote by G, A, B the group and the two generator sets that are used for constructing the square complex.

Claim 4.1. *Consider g, h that are supported on the same $v \in V$. We will call such a pair a source-sharing pair. Suppose that for any we have that $|g \cdot h|$ is even. Then there is a Clifford gate that computes $|f\rangle \mapsto \exp\Big(-i\pi\sum_{g,h \text{ source-sharing}} X_gX_h|g\cdot h|\Big)|f\rangle$.*

Claim 4.2. *Let C_A and $C_{A'}$ such that $C_{A'} \subset C_A$. Then $\left(C_A^\perp \otimes C_B^\perp\right)^\perp, C_{A'} \otimes C_{B'}$ form a **CSS** code C such there exists a subspace $V \subset C$ with effictive distance d.*

Proof. Idea. consider generators of the form $e_0 \otimes g$. Any codeword in their span is just a first row asssitmentd to a code word of C_A. If we assume less than linear number on that row then we will secucess to decode it, + some other generators that we don't care about. $\square$

$$C_X = \left((C_A \otimes C_0)^{\perp} \otimes C_0^{\perp} \right)^{\perp}$$
$$C_Z = ((C_A \otimes C_0) \otimes C_0)^{\perp}$$

Claim 4.3. *Let C be a code at rate $\rho(C) > 7/8$ has at least one codeword $x \in C$, such that $|x| =_8 1$.*

Definition 4.1. *We will say that a code C is (l, m)-genorthogonal if there exists a generator set G for C such that for any $I \subset G$ such that $1 < |I| < l$ we have that:*

$$\sum_{i \in [n]} \prod_{g_j \in I \subset G} g_j^i =_m 0$$

Claim 4.4. *If there exists a single (l, m)-genorthogonal code for a finite length Δ, then there is a family of (l, m)-genorthogonal good codes. Moreover, if there exists a generator in C_0 of weight $|\cdot|_m = 1$, then there exists a family that also has at least one generator of weight $|\cdot|_m = 1$.*

Proof. Denote by $C_0 = \Delta[1, \rho_0, \delta_0]$ an (l, m)-genorthogonal code and observes that for any $C = [n, \rho n, \delta n]$ the tensor code $C_0 \otimes C = [\Delta n, \rho_0 \rho \Delta n, \delta_0 \delta \Delta n]$ is also (l, m)-genorthogonal code.

For the seconed part of the claim, Choose C to be a good code with rate $> (2^m - 1)/2^m$ by Claim 4.3 there is at least on codeword c in C such that $|c| =_m 1$.

So pick the base for $C_0 \otimes C$ such the first generator is $g_0 \otimes c$ where g_0 denote a generator of C_0 satisfies $|g_0| =_m 1$. Then $|g_0 \otimes c| = |g_0| \cdot |c| =_m 1$. $\square$

Claim 4.5. *Suppose that there exists $(m + 1, m)$-genorthogonal code, such that any generator of it has weight $|\cdot| =_m 1$ then there exists also a family of good $(m + 1, m)$-genorthogonal codes such that a liner portion of his generators g have weight $|g| =_m 1$.*

Proof. Denote by C_0 a finte $(m + 1, m)$-genorthogonal code, such that any generator of it has weight $|\cdot| =_m 1$. Let C be a good $(m + 1, m)$-genorthogonal code with generator c such that $|c| =_m 1$, the existence of which is given by Claim 4.4. Denote its rate by ρ. If C has more than $\rho/m \cdot n$ generators at weight $|\cdot| =_m 1$ then we are done. Otherwise, by the pigeonhole principle, there is an i such that more than ρ/m portion of the generators are at weight $|\cdot| =_m i$. Denote them by $g_1, g_2, g_3, \ldots, g_m$.

Define the set $g_1^{'}, g_2^{\prime}..g_m^{\prime}$ as

$$g_t^{\prime} = c + \sum_{j=t}^{t+m} g_j$$
$$\Rightarrow |g_{t+1}^{\prime}| = |c| + \sum_{t} |g_j| + \sum_{|I|<l+1} \left| \prod_{g \in I} \alpha_{\star} g \right|$$
$$=_m c + m \cdot i =_m c =_m 1$$

Now take $C_0 \otimes C$, and set the new generator set to be $g_i^0 \otimes g_j^{\prime}$. And it's easy to verify that we got the code we wanted. $\square$

Claim 4.6. *There exists, a good LDPC code (classic) C such that $C^{\perp}$ is also a good code and a generator set G, for exists $G' \subset G$ and $|G'| = \Theta(|G|)$ such:*

1. *For any pair $x \neq y \in G' \rightarrow x \cdot y =_8 0$*
2. *For any triple $x \neq y, z \in G' \rightarrow \sum_i x_i y_i z_i =_8 0$*

3. *For any* $x \in G' \to |x| =_8 1$

Claim 4.7. *There is* $n \to \Theta(n)$ *magic states distillation into a binary qldpc code with* $\Theta(\sqrt{n})$ *distance, and therefore with asymptotic overhead approaching* 1

Proof. For the encoding we are going to use the hyperproduct code defined in [TZ14]. Let C be the code given by Claim 4.6 and consider the hyperproduct of C with itself $Q = Q(C \times_H C)$. In addition, denote by C_X, C_Z the CSS representation of Q.

By the fact that $C^\perp$ is also a good code, then Q is a positive rate, square root distance code. Let ρ be the rate of C and $1-\rho$ be the rate of $C^\perp$. As $\rho > 0$, then one can find $I \subset [n]$ coordinates such that for any $i \in I$ the indicator $e_i \notin C^\perp$. Hence, it holds from [TZ14] that any vector of the form $e_i \otimes x$ is a codeword of $C_X/C_Z^\perp$.

Denote by ρ' the portion of G' as defined in Claim 4.6, and define S to be:

$$S = \left\{ e_i \otimes x | e_i \notin C^\perp, x \in G' \right\}$$

Observes that $|S| = \rho' \rho n^2$ and in addition S satisfies the properties in Claim 4.6. Denote by f a codeword supported only on S and denote by X_s the indecator that indicate that s supports f. Thus:

$$\begin{aligned} T^{\otimes n} |f\rangle = \exp \Big(i\pi/4 \sum_g X_g \overbrace{|g|}^{8k+1} \\ - 2 \cdot i\pi/4 \overbrace{\sum_{g,h} X_g X_h |g \cdot h|}^{8k} \\ + 4 \cdot i\pi/4 \overbrace{\sum_{g,h} X_g X_h X_l |g \cdot h \cdot l|}^{8k} \Big) |f\rangle \end{aligned}$$

$$= \exp \Big(i\pi/4 \sum_{g \in S} X_g \Big) |f\rangle$$

Therefore we can, generate the enocded (**[COMMENT]** For now without spanning on on $C_Z^\perp$) product of $T^{\otimes |S|} |+\rangle^{|S|}$:

$$\prod_{s \in S} \Big(|0\rangle + \exp(i\pi/4) |s\rangle \Big)$$

[COMMENT] What is left:

1. Show that one can generate $\prod_{s \in S} \Big(|C_Z^\perp\rangle + \exp(i\pi/4) |C_Z^\perp + s\rangle \Big)$ without propagate the errors. I think I know how to do it.
2. Compute a threshold p_0 for using Baravi construction.

Thus we have that $\gamma = \log(n/k)/\log(d) = \log(n/|S|)/\log(\Theta(\sqrt{n})) \to 0$ and the overhead growes as $\log^\gamma(n) \to 1$ [BH12], [MEK12]. □

References

[BH12] Sergey Bravyi and Jeongwan Haah. "Magic-state distillation with low overhead". In: *Physical Review A* 86.5 (2012), p. 052329.

[MEK12] Adam M. Meier, Bryan Eastin, and Emanuel Knill. *Magic-state distillation with the four-qubit code*. 2012. arXiv: 1204.4221 [quant-ph].

[TZ14] Jean-Pierre Tillich and Gilles Zemor. "Quantum LDPC Codes With Positive Rate and Minimum Distance Proportional to the Square Root of the Blocklength". In: *IEEE Transactions on Information Theory* 60.2 (Feb. 2014), pp. 1193–1202. DOI: 10.1109/tit.2013.2292061. URL: https://doi.org/10.1109%2Ftit.2013.2292061.