

# Magic States Distillation Using Quantum Expander Codes.

David Ponnarovsky

March 3, 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.

*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  $\Lambda$  be a set of independent  $k'$  codewords in  $[n, k, d]$  code. Then there is a code  $C' = [\leq 2n, \geq k - k'/2, d]$  and  $\Lambda'$  set of independent codewords of it, such that  $|\Lambda'| > \frac{1}{2}|\Lambda|$  and for every pair  $x, y \in \Lambda'$  we have that  $x \cdot y = 0$ .

*Proof.* First, consider the upper triangular matrix obtained by applying Gaussian elimination on  $\Lambda$ . Now, consider the following process: go up hill in the square matrix. Let  $j$  be the first nonzero coordinate in the bottom row of the matrix. In the  $i$ th iteration, we ask how many vectors  $u_m$  satisfy  $u_m u_{k'-i} = 0$  for  $m < k' - i$ . If encoding the  $j - i$  coordinate by  $C_0^1$  such that  $1_{C_0^1}$  gives  $|B_i| > |\bar{B}_i|$ , then choose to encode with  $C_0^1$ ; otherwise, encode that coordinate with  $C_0^0$ . Denote the vectors yielded from that process by  $\Gamma$ .

Denote by  $S \subset \Gamma$  the group of vectors such that there exists at least one vector in  $\Gamma$  for which their multiplication is not zero. Observe that the total number of pairs with zero multiplication is greater than:

$$\frac{k' - 1}{2} \frac{k' - 2}{2} + \dots + \frac{2}{2} = \frac{1}{2} \frac{(k' - 1)(k' - 2)}{2}$$

So

$$|S| \cdot (k' - 1) \leq \binom{k'}{2} - \frac{1}{2} \frac{(k' - 1)(k' - 2)}{2} < \frac{k'(k' - 1)}{2} \Rightarrow |S| < \frac{k'}{2}$$

Set  $\Lambda' \leftarrow \Gamma/S$ .

$\square$

[COMMENT] Change to  $\Pr_{j \sim [\Delta]} [i, j \text{ collide}] < \frac{1}{2\Delta}$

**Definition 1.2.** Let  $\{h_i\}_1^t$  be the checks of  $\Delta$ -length code  $C_0$ . We say that  $i$ th bit and the  $j$ th 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:

$$\Pr_{i,j \sim [\Delta]^2} [i, j \text{ collide}] < \frac{1}{2\Delta}$$

**Claim 1.3.** Suppose that  $C_0^\perp$  is a checks-hashed. Then  $(C_0^{\otimes m})^\perp$  is also a checks-hashed.

*Proof.*

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

□

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.

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

**Claim 1.4.** Let  $H$  be a  $|V| \times r$  binary parity check matrix of  $\tilde{C}$ . Also, let  $G$  be a  $\Delta$ -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  $\Lambda$  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 1.5.** Assume that  $C_0$  is a  $\Delta$ -length code such that for any two non-trivial codewords  $c, c' \in C_0$  we have that  $c \cdot c' = 1$ , and denote by  $C = \mathcal{T}(G, C_0)$ . And let  $\Lambda$  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. Observe that applying  $T^{\otimes}$  on  $|f\rangle$  yields the state:

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

## 2 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.

## 3 Using Quantum 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 3.1.** *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  $|f\rangle \mapsto \exp \left( -i\pi \sum_{g,h \text{ source-sharing}} X_g X_h |g \cdot h| \right) |f\rangle$ .*

**Claim 3.2.** *Let  $C_A$  and  $C_{A'}$  such that  $C_{A'} \subset C_A$ . Then  $(C_A^\perp \otimes C_B^\perp)^\perp, C_{A'} \otimes C_{B'}$  form a CSS code  $C$  such there exists a subspace  $V \subset C$  with effective distance  $d$ .*

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

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

**Claim 3.3.** *Let  $C$  be a code at rate  $\rho(C) > 7/8$  has at least one codeword  $x \in C$ , such that  $|x| = 1$ .*

**Definition 3.1.** *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 3.4.** *If there exists a single  $(l, m)$ -genorthogonal code for a finite length  $\Delta$ , 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 observe 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 second part of the claim, Choose  $C$  to be a good code with rate  $> (2^m - 1)/2^m$  by Claim 3.3 there is at least one 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  $|g_0 \otimes c|_m = |g_0|_m \cdot |c|_m = 1$ .  $\square$

**Claim 3.5.** *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 finite  $(m+1, m)$ -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 3.4. Denote its rate by  $\rho$ . 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  $\rho/m$  portion of the generators are at weight  $|\cdot| =_m i$ . Denote them by  $g_1, g_2, g_3, \dots, g_m$ .

Define the set  $g'_1, g'_2, \dots, g'_m$  as

$$\begin{aligned} g'_i &= c + \sum_{j=t}^{t+m} g_j \\ \Rightarrow |g'_{t+1}| &= |c| + \sum_t |g_j| + \sum_{|I| < l+1} \left| \prod_{g \in I} \alpha_{\star} g \right| \\ &=_m c + m \cdot i =_m c =_m 1 \end{aligned}$$

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

**Claim 3.6.** *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  $x \in G' \rightarrow |x| =_8 1$*

**Claim 3.7.** *There is  $n \rightarrow \Theta(n)$  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 3.6 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  $\rho$  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  $\rho'$  the portion of  $G'$  as defined in Claim 3.6, and define  $S$  to be:

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

Observes that  $|S| = \rho' \rho n^2$  and in addition  $S$  satisfies the properties in Claim 3.6. Denote by  $f$  a codeword supported only on  $S$  and denote by  $X_s$  the indicator that indicate that  $s$  supports  $f$ .

Thus:

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

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

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

[COMMENT] What is left:

1. Show that one can generate  $\prod_{s \in S} \left( |C_Z^\perp\rangle + \exp(i\pi/4) |C_Z^\perp + s\rangle \right)$  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  $\gamma = \log(n/k)/\log(d) = \log(n/|S|)/\log(\Theta(\sqrt{n})) \rightarrow 0$  and the overhead grows as  $\log^\gamma(n) \rightarrow 1$  [BH12], [MEK12].  $\square$

## 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>.