# Magic States Distillation Using Quantum Expander Codes.

David Ponarovsky

February 7, 2024

**Claim 0.1.** *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 $z(x) \in \mathbb{F}_2^{|V|}$ is defined as:*

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

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

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:

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

## 1 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.

## 2 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 2.1.** *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 2.2.** *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. □

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

**Claim 2.3.** *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 2.1.** *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 2.4.** *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 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 2.3 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 $|g_0 \otimes c| = |g_0| \cdot |c| =_m 1$. ☐

**Claim 2.5.** *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 2.4. 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 $g_1, g_2, g_3, \ldots, g_m$.

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. ☐

**Claim 2.6.** *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 $x \neq y \in G' \to x \cdot y =_8 0$*
2. *For any triple $x \neq y, z \in G' \to \sum_i x_i y_i z_i =_8 0$*
3. *For any $x \in G' \to |x| =_8 1$*

**Claim 2.7.** *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 2.6 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 2.6, 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 2.6. Denote by $f$ a codeword supported only on $S$ and denote by $X_s$ the indecator that indicate that $s$ supports $f$. Thus:

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

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.