Magic States Distillation Using Quantum Expander Codes.

David Ponarovsky

January 8, 2024

Claim 0.1. *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 effective distance d.*

Claim 0.2. *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 0.1. *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 0.3. *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 $> \left(2^m - 1\right)/2^m$ by Claim 0.2 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 0.4. *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 0.3. 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 $g_1^{'}, g_2^{'} .. g_m^{'}$ as

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

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. □

Claim 0.5. *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 0.6. *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 0.5 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 0.5, 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 0.5. 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 $\gamma = \log(n/k)/\log(d) = \log(n/|S|)/\log(\Theta(\sqrt{n})) \rightarrow 0$ and the overhead growes as $\log^\gamma(n) \rightarrow 1$ [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.