Magic States Distillation Using Δ-Toric (good qLDPC?).

David Ponarovsky

January 4, 2024

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:

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

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* $|f\rangle \mapsto \exp\Big(-i\pi\sum_{g,h \text{ source-sharing}} X_g X_h|g\cdot h|\Big)|f\rangle$.

3 Fail Attempt.

In addition, let us assume the existence of $d \in G$ such that d is non-identity and commutes with any element in $A \cup B$. Then, observe that multiplying by d preserves adjacency on the complex. Namely, if $\{u, v\} \in E$ then also $\{du, dv\} \in E$.

Consider $|f\rangle$ such that if X_g is not zero, and g is associated with a local codeword $c \in C_A \otimes C_B$ on vertex v, then the generator associated with the local codeword c on vertex $d\cdot v$ also supports f, denoted by g'. Thus, the exponent above becomes:

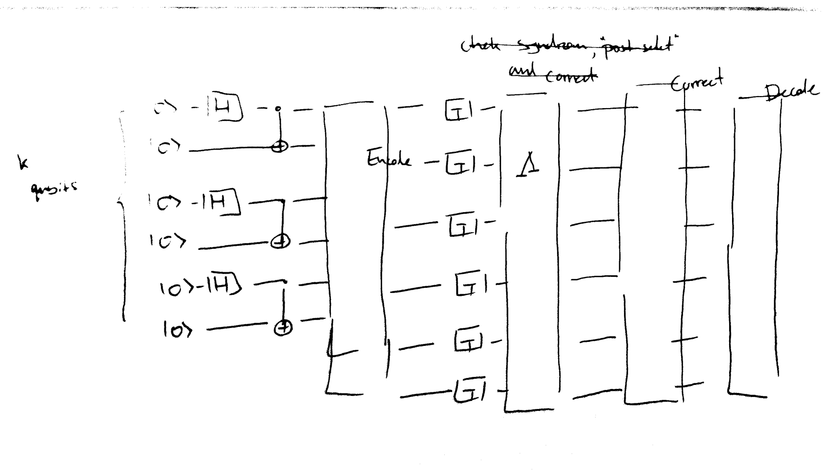

Figure 1: Quantum Circuit for distillation.

$$= \exp\Big(i\pi/4 \sum_g X_g|g| - 2\cdot\pi/4 \sum_{g,h\in G/a} X_gX_h|g\cdot h| + X_{g'}X_{h'}|g\cdot h|$$

$$+ 4\cdot i\pi/4 \sum_{g,h\in G/a} X_gX_hX_l|g\cdot h\cdot l| + X_{g'}X_{h'}X_{l'}|g\cdot h\cdot l|\Big)\,|f\rangle$$

$$= \exp\Big(i\pi/4 \sum_g X_g|g| - 2\cdot 2\cdot\pi/4 \sum_{g,h\in G/a} X_gX_h|g\cdot h| + 2\cdot 4\cdot i\pi/4 \sum_{g,h\in G/a} X_gX_hX_l|g\cdot h\cdot l|\Big)\,|f\rangle$$

$$= \exp\Big(i\pi/4 \sum_g X_g|g| - i\pi \sum_{g,h\in G/a} X_gX_h|g\cdot h|\Big)\,|f\rangle$$

Claim 3.1. *The gate* $|f\rangle \mapsto \exp\Big(-i\pi\sum_{g,h\in G/a} X_gX_h|g\cdot h|\Big)\,|f\rangle$ *is in the Clifford.*

Proof. Just decode f and apply **CZ** between any pair of qubits corresponding to the generators g, h such that $g \cap h = 1$. Then encode the state again. Observes that **CZ** is a Clifford gate, and by the fact that the code is a CSS code then the decoder and the encoder are both in the Clifford. □

Let's denote the circuit defined in Claim 3.1 by Λ. So we have that:

$$\Lambda^\dagger \exp\Big(i\pi/4 \sum_g X_g|g| - i\pi \sum_{g,h\in G/a} X_gX_h|g\cdot h|\Big)\,|f\rangle$$

$$= \exp\Big(i\pi/4 \sum_g X_g|g|\Big)\,|f\rangle$$

Maybe what do we need is to arrange in some way $|g| + |g'| = 4k+1$ and $\langle g, f\rangle = \langle g', f'\rangle$

Claim 3.2. *For any m codewords $x_1..x_m$ there is a set of coordinates I and $|I| < \alpha n$. Such that:*

$$\sum_{j\in[n]/I} x_a^j x_b^j = 0$$

For any pair x_a, x_b.

Claim 3.3. *For any m codewords $x_1..x_m$ there is a set of coordinates I and $|I| < \alpha n$. Such that:*

$$\sum_{a,b,j\in[n]/I} x_a^j x_b^j = 4k$$

For any pair x_a, x_b.

Claim 3.4. *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 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 3.5. *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 3.4 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 3.6. *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 3.5. 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

$$g_t' = c + \sum_{j=t}^{t+m} g_j$$

$$\Rightarrow |g_{t+1}'| = |c| + \sum_t |g_j| + \sum_{|I| < l+1} \left| \prod_{g \in I} \alpha_\star g \right|$$

$$=_m c + m \cdot i =_m c =_m 1$$

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 3.7. *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 3.8. *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 3.7 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 3.7, 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 3.7. Denote by f a codeword supported only on S and denote by X_s the indecator that indicate that s supports f. Thus:

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

$\square$

References

[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.