

# Quantum LTC With Positive Rate

David Ponnarovsky

September 3, 2022

**preamble.** preamble.

**The Construction.** Fix primes  $q, p_1, p_2, p_3$  such that each of them has 1 residue mode 4. Let  $A_1, A_2, A_3$  be a different generators sets of  $\mathbf{PGL}(2, \mathbb{Z}/q\mathbb{Z})$  obtained by taking the solutions for  $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p_i$  such that each pair  $A_i, A_j$  satisfy the TNC constraint. Then consider the graphs: ( $G$  is the  $\mathbf{PGL} \times \mathbb{Z}_2$  group).

$$\begin{aligned}\Gamma_1 &= \text{Cay}_2(G, A_1) \times_G \text{Cay}_2(G, A_2) \\ \Gamma_2 &= \text{Cay}_2(G, A_1) \times_G \text{Cay}_2(G, A_3) \\ \Gamma_{\square_1} &= (G, \{(g, agb) : a \in A_1, b \in A_2\}) \\ \Gamma_{\square_2} &= (G, \{(g, agc) : a \in A_1, c \in A_3\}) \\ \Gamma_{\square\square} &= (G, \{(g, gb, agc), (g, gc, agb) : a \in A_1, b \in A_2, c \in A_3\})\end{aligned}$$

Then define the codes:

$$\begin{aligned}C_z^\perp &= \mathcal{T}(\Gamma_{\square_1}, C_{A_1}^\perp \otimes C_{A_2}^\perp) \\ &\quad | \mathcal{T}(\Gamma_{\square_2}, C_{A_1}^\perp \otimes C_{A_3}^\perp) \\ C_x &= \mathcal{T}(\Gamma_{\square_1}, (C_{A_1} \otimes C_{A_2})^\perp) \\ &\quad | \mathcal{T}(\Gamma_{\square_2}, (C_{A_1} \otimes C_{A_3})^\perp) \\ C_w &= \mathcal{T}(\Gamma_{\square\square}, (C_{A_1} \otimes C_{A_2} \otimes C_{A_3})^\perp)\end{aligned}$$

Notice that the faces of  $\Gamma_{\square_1}, \Gamma_{\square_2}$  are disjointed and here the symbol  $|$  means just joint them together. The main focus here is to prove local test-ability for computation base (i.e  $C_x$ ) and for completeness one also must to define the code

$$C_{w_z} = \mathcal{T}(\Gamma_{\square\square}, (C_{A_1}^\perp \otimes C_{A_2}^\perp \otimes C_{A_3}^\perp)^\perp)$$

**What We Currently Have.** Given a candidate for a codeword  $c$  we could check efficiently if  $c \in C_z^\perp$ . Additionally summing up the local correction of each vertex in  $C_x$  yields a codeword in  $C_w$ . Now we would want to show something similar to property 1 in Levrier and Zemor which imply that any codeword of  $C_w$  with weigh beneath a linear threshold  $\eta n$  must to be also in  $C_x$ . (And therefore we can reject candidates with high weight).

Assume that we have succeed to do so, Then the testing protocol will be looked as follow, first we check that the candidate is not in  $C_z^\perp$  and then we check that is indeed in  $C_x$ . And repeat again in the phase base. Then

there are constants  $\kappa_1, \kappa_2$

$$\begin{aligned}\text{accept} &\sim \kappa_1 \cdot d(c, C_z^\perp) \\ &\quad + [1 - \kappa_1 \cdot d(c, C_z^\perp)] \kappa_2 d(c, C_x) \\ \text{reject} &\sim [1 - \kappa_1 \cdot d(c, C_z^\perp)] \\ &\quad + \kappa_1 \cdot d(c, C_z^\perp) \cdot [1 - \kappa_2 d(c, C_x)]\end{aligned}$$

**Disclaimer.** The use of the  $\sim$  was made by purpose. The above should be formalize by inequalities. (And this also make another problem as the term  $1 - \kappa_1 \cdot d()$  is in the opposite direction).

**The Hard Part.** It seems (at least for now) that the hard part is to find an analog for Lemma 1 in Levrier-Zemor, Which can formalize as follow: Consider a codeword  $c \in C_w$  such that  $|c| \leq \eta n$  then we could always find a vertex in  $\Gamma_{\square_1}$  and a local codeword  $\xi \in C_{A_1} \otimes C_{A_2}$  on his support such that  $|c + \xi| < |c|$ .

**Tasks.**

1. Prove that  $\Gamma_{\square\square}$  is indeed an expander. Should be (relative) easy.
2. Prove a Lemma 1 analogy. And while do so, understand what are the properties we should require from the small code. (i.e w-robustness and p-resistance for puncturing).
3. Show that we could actually choose such  $\{A\}_i$  and the matched small codes.
4. Understand what it mean quantomlly test if a  $c \in C_w/C_x$ . Namely, is weight counting can be consider as  $X$ -check which commute with the other  $Z$ -checks?
5. Write a program which plot small complex in a small scale for getting more intuition.

**All The Verticis Are Normal** Define a noraml vertex in  $V_1$  to be a vertex such his local view (a codeword in a dual tensor code). supported on less then  $w = \Delta^{\frac{3}{2}}$  faces. Consider the code  $C_w$  defined above, and assume in addition that the distance of the small codes  $C_{A_j}$ ,  $\delta\Delta$  satisfy the equation  $1 - \delta < \frac{1}{2}\delta^3$  and also the code  $C_{A_1}$  contains the word  $1^\Delta$ .

Then for any  $x \in C_w$  such that all the vertices in the induced graphs  $\Gamma_{\square_1}, \Gamma_{\square_2}$  by it are noraml. Then there

exists a vertex  $g \in V_0$  and a local codeword  $c_{1 \otimes 2 \otimes 3}$  supported entirely on the neighborhood of  $g$  such that:  $|x + c| \leq |x|$ .

**Proof.** Let  $g$  be an arbitrary vertex in  $V_0$  we know by Leverrier and Zemor that the local views of  $g$  in  $\Gamma_{\square_1}, \Gamma_{\square_2}$  are  $\Delta^{3/2}$  close to  $1 \otimes 2$  and  $1 \otimes 3$  sum of the rows and columns shared with vertices of  $V_1$ . For example,  $(g, -)$  and  $(ag, +)$  share the faces  $\{(g, -), (agb, -)\}, \{(g, -), (agc, -)\}$ . By the definition of  $w$ -robustness any local codeword on  $V_1$  vertices supported on at most  $w/d_B = \sqrt{\Delta}$  columns. And therefore a codeword could be thought as a table which constructed by gathering rows which are codewords of  $C_A$  plus a small error which corresponded to the contribution of codewords of the code  $\mathbb{F}^A \otimes C_B$ . And viceversa, by the fact that each vertex has  $2\Delta$  neighbors we have that the total error from a table corresponded to  $C_A \otimes C_B$  is less than  $2\Delta^{\frac{3}{2}}$ . Now we know that we can represent the local view on  $g$  as the sum of two disjoint vectors, each lay on  $\Gamma_{\square_1}, \Gamma_{\square_2}$  in the following manner:

$$\begin{aligned} y &= y_1 y_2^\top + \xi_y \\ z &= z_1 z_2^\top + \xi_z \end{aligned}$$

such that  $y_1 y_2^\top \in C_A \otimes C_B$ ,  $z_1 z_2^\top \in \text{otimes} C_C$  and the  $\xi_y, \xi_z$  are the corresponding errors of the local views from the tensor codes.

**Lemma** There exists  $u \in C_{A_1}, v \in C_{A_2}, w \in C_{A_3}$  such that