

# Quantum LTC With Positive Rate

David Ponnarovsky

September 1, 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  $\mathbf{GPL}(2, \mathbb{Z}/q\mathbb{Z})$  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 union of the Balance product of

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

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.

**Claim** for any ?  $[[n, k, d]]$  CSS code property 1 holds . **Proof.** let  $y \in \{0, 1\}^n$  be a vector such  $y \in G_z^\delta$ , let assume that  $|y|_{c^{\perp}} \leq C_2 d$  then for any  $c \in C_x^\perp$ :

$$\delta r_z \geq |H_z y| = |H_z(y + c)|$$

**Robustness** Let  $\omega \leq \Delta^2$ . Let  $C_A$  and  $C_B$  be codes of length  $\Delta$  with minimum distance  $d_A$  and  $d_B$ . We shall say that the dual tensor code  $C = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$  is  $\omega$ -robust, if for any codeword  $c \in C$  of Hamming weight  $|c| \leq \omega$ , there exist  $A' \subset A, B' \subset B, |A'| \leq |c|/d_B, |B'| \leq |c|/d_A$ , such that  $c_{ab} = 0$  whenever  $a \notin A', b \notin B'$ .

**Definition. Sub-Tensor Pair** We will say that  $C'_A, C'_B$  are sub-tensor pair of  $C_A, C_B$  if each of the code is subspace of  $C_A, C_B$  respectively and in addition one of the minimal codeword in  $C_A$  is also contained in  $C'_A$  (and similar to  $C'_B$ ).

Note that the distance of each subcode is equal to the one from which its derived. And also such code can be generated efficiently by choosing  $\Delta$  non trivial coordinate of one of the minimal codewords and sets a check nodes over them. (Assuming that  $\Delta$  is even and that there is at least one different codeword in the code which has an overlap with that minimal codeword).

**Claim. Subcode Robustness.** Consider the sub-tensor pair  $C'_A \subset C_A, C'_B \subset C_B$ , such that the dual tensor of  $C'_A, C'_B$  is  $\omega$ -robust then the dual tensor of  $C'_A, C'_B$  is also  $\omega$ -robust.

**Proof.** Let  $c$  be a codeword in the dual tensor of  $C'_A, C'_B$  then it's clear that  $c$  is also in the dual tensor of  $C_A, C_B$  and therefore there exists  $V, U$  subsets of  $A, B$  respectively such that  $c$  supported only on them, and their size is less then  $|c|/d_B, |c|/d_A$ . As the length's space of the each of the subcode is identical to his container, and by the fact that the distance of each of the subcode is equal to one which contain it, It's follow that (1)  $U \subset A' = A$  and (2)  $|c|/d_A = |c|/d_{A'}$ .

**Existence Of Sub-Tensor Pair** [\[COMMENT\]](#)  
Try to prove existence by the probabilistic method.

**Theorem 1.** Let  $C_0 = C_A \otimes C_B$ , and  $C_1 = C_A'^{\perp} \otimes C_B'^{perp}$  such that  $C'_A, C'_B$  are sub-tensor pair of  $C_A, C_B$ , and each of the code has length  $\Delta$  and relative distance  $\delta$ . Consider the  $G$ -balance product of graph with good algebraic expansion  $\Gamma_0^\square, \Gamma_1^\square$ . Then the pair of the tanner codes  $\mathcal{T}(\Gamma_0^\square, C_0)$  and  $\mathcal{T}(\Gamma_1^\square, C_1^\perp)$  define a CSS code with linear distance, positive rate, and local testability for some constant  $\kappa$ .

**Proof.** First, it's clear that each pair of  $X$  and  $Z$  generators are orthogonal by design. d dd