Quantum LTC With Positive Rate

David Ponarovsky

September 1, 2022

preamble. preamble.

The Construction. Fix primes q, p_1, p_2, p_3 such that each of them has 1 resduie 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 gettring the soultions for $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p_i$ such that each pair A_i, A_j satisfiy the TNC constraint. Then consider the union of the Blance product of

$$\begin{aligned}
\Gamma_1 &= Cay_2\left(G, A_1\right) \times_G Cay_2\left(G, A_2\right) \\
\Gamma_2 &= Cay_2\left(G, A_1\right) \times_G Cay_2\left(G, A_3\right) \\
\Gamma_{\square_1} &= \left(G, \left\{(g, agb) : a \in A_1, b \in A_2\right\}\right) \\
\Gamma_{\square_2} &= \left(G, \left\{(g, agc) : a \in A_1, c \in A_3\right\}\right) \\
\Gamma_{\square\square} &= \left(G, \left\{(gb, agc), (gc, agb) : a \in A_1, b \in A_2, c \in A_3\right\}\right)
\end{aligned}$$

Then define the codes:

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

Notice that the faces of $\Gamma_{\square_1}, \Gamma_{\square_2}$ are disjointess and here the symbol $\mid$ means just joint them togther. The main focus here is to prove local testability for computaion base (i.e C_x) and for completence one also must to define the code

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

What We Currently Have. Given a canidate for a codeword c we could check efficently if $c \in C_z^{\perp}$. Additionaly summing up the local corretion of each vertex in C_x yields a codeword in C_w. Now we would want to show somthing similar to property 1 in Levarier and Zemor which imply that any codeword of C_w with weigh benteeth a linear treashold ηn must to be also in C_X. (And therefore we can reject canidates with heigh weight).

Assume that we have successed to do so, Then the testing protocol will be looked as follow, first we check that the canidate 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 κ_1, κ_2

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

Disclaimer. The use of the $\sim$ was made by purpose. The above should be formlize by inequlities. (And this also make another problem as the term $1 - \kappa_1 \cdot d\left(\right)$ is in the opposite direaction).

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 formolize as follow: Consider a codeword $c \in C_w$ such that $|c| \leq \eta n$ then we could alwayes 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 an Lemma 1 analogy. And while do so, undersand what are the properties we should require from the small code. (i.e w-robusstness and p-resistence for pancutring).

3. Show that we could acutaly choose such $\{A\}_i$ and the matched small codes.

4. Understand what it mean quantmlly test if a $c \in C_w / C_x$. Namly, is weight counting can be consider as $X-$check which commute with the other $Z-$checks.

5. Write a program which plot samll coplex in asmall scale for getting more intuion.

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 $|y|_{c^{x\perp}} \leq C_2 d$ then for any $c \in C_x^{\perp}$:

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

Robusstness *Let $\omega \leq \Delta^2$. Let C_A and C_B be codes of length Δ 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 ω-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 respeactivly 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 eqaul to the one from which its drived. And also such code can be generated efficintly by choosing Δ non trival coordinate of one of the minimal codewords and sets a check nodes over them. (Assunming that Δ is even and that there is at least one diffrent codeword in the code wich has an overlap with that minimal codewoed.

Claim. Subcode Robusstness. *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 ω-robust then the dual tensor of C'_A, C'_B is also ω-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 therfore there exists V, Usubsets of A, B respectivly 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 indentical 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) $|c|/d_A = |c|/d_{A'}$.

Existance Of Sub-Tensor Pair [COMMENT] Try to prove existance by the probablistic method.

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

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