Quantum LTC With Positive Rate

David Ponarovsky

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).

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

Then define the codes:

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

Notice that the faces of $\Gamma_{\square_1}, \Gamma_{\square_2}$ are disjointed and here the symbol $\mid$ 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

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

What We Currently Have. Given a 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 Levarier and Zemor which imply that any codeword of C_w with weigh beneath a linear threshold ηn 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 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 formalize by inequalities. (And this also make another problem as the term $1 - \kappa_1 \cdot d\left(\right)$ 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 $|c| \le \eta n$ 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 Let $x \in C_w$. 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. Condisder the case in which all vertices in the induced graph by x are noraml. Then there exists a vertex $g \in V_0$ and a local codeword $c \in C_{A_1} \otimes C_{A_2} \otimes C_{A_3}$ supported entirly on the neighberhood of g such that: $|x + c| \le |x|$.

Proof. Let g be an aribtrary vertex in V_0 the local view of g is the sum of the rows and coloms shered with verticis of V_1. For example, $(g,-)$ and $(ag,+)$ share the faces $\{\{(g,-),(agb,-)\},\{(g,-),(agc,-)\}\}$. By the defination of w-robustness any local codeword on V_1 vertices supoorted on at most $w/d_B=\sqrt{\Delta}$ colomuns. And therefore a codeword could be thouht as a table which constructed by gaterring rows which are codewords of C_A plus a small error which coressponded to the contributed of codewords of the code $\mathbb{F}^A\otimes C_B$. And viceversa, by the fact that each vertex has 2Δ neighboors we have that the total error from a table corresponded to $C_A\otimes C_B$ is less then $2\delta^{\frac{3}{2}}$.