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).

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

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 $|c| \leq \eta n$ 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 diststance and the rate of the small codes C_{A_j}, $\delta\Delta$ satisfay the eqution $r^2\left(1 - \delta\right) < \frac{1}{2}\delta^3$ and also the code C_{A_1} contains the word 1^{Δ}.

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 noramls. 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: $|x + c| \leq |x|$.

Proof. Let g be an aribtrary vertex in V_0 we know by Leverrir and Zemor that the local views of g in $\Gamma_{\square_1}, \Gamma_{\square_2}$ are $\Delta^{3/2}$ close to $C_{A_1} \otimes C_{A_2}$ and $C_{A_1} \otimes C_{A_3}$ by the w-robustness propperty.

So we can repreasnt the locals views on g as the following disjointess vectors, each lays on $\Gamma_{\square_1}, \Gamma_{\square_2}$:

$$y = y_1 y_2^\top + \xi_y$$
$$z = z_1 z_2^\top + \xi_z$$

such that $y_1 y_2^\top \in C_{A_1} \otimes C_{A_2}$, $z_1 z_2^\top \in C_{A_1} \otimes C_{A_3}$ and the ξ_y, ξ_z are the coressponded errors of the local views from the tensor codes.

Let $\{y_1^j y_2^{i\top}\}, \{z_1^j z_2^{i\top}\}$ be the bases for $C_{A_1} \otimes C_{A_2}$ and $C_{A_1} \otimes C_{A_3}$ such that $y_1^j, z_1^j \in C_{A_1}$ and $y_2^i \in C_{A_2}, z_2^i \in C_{A_3}$. And denote by $\alpha_{ij}, \beta_{ij} \in \mathbb{F}_2$ the coffeicents of $y_1 y_2^\top$ and $z_1 z_2^\top$.

By the fact that $1^\Delta \in C_{A_1}$ we have that for any i, j the vecotr:

$$\begin{aligned} \bar{y_1}^j y_2^{i\top} &= 1^\Delta y_2^{i\top} \\ &+ y_1^j y_2^{i\top} = \left(1^\Delta + y_1^j\right) y_2^{i\top} \\ &\in C_{A_1} \otimes C_{A_2} \end{aligned}$$

And by the same calculation we get also that $\bar{z_1}^j z_2^{i\top} \in C_{A_1} \otimes C_{A_3}$.

Claim. Assume that $y_1 y_2^\top$ and $z_1 z_2^\top$ are in the bases defined above. Let $\tau \in \mathbb{F}_2^{A \times B \times C}$ such that $\tau_{abc} = \left(y_1 y_2^\top\right)_{ab} \left(z_1 z_2^\top\right)_{ac}$ then:

$$d\left(\tau, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \leq (1 - \delta)\, \Delta^3$$

Proof. First noitce that $y_{1a} y_{2b} z_{2c}$ is a valid codeword of $C_{A_1} \otimes C_{A_2} \otimes C_{A_3}$. That beacuse that the projection obtained bt fixing any two coordinates yields ethier a zero or a codeword of one the codes.

Therefore we could consider the following codeword $\tilde{\tau}_{abc} = (y_{1a} + \bar{z}_{1a})\, y_{2b} y_{2c}$ and bounding the distance of τ by

$$\begin{aligned} &d\left(\tau, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \leq d\left(\tau, \tilde{\tau}\right) \\ &= \sum_{abc} \left(y_{1a} + \bar{z}_{1a}\right) y_{2b} y_{2c} \oplus \left(y_{1a} z_{1a}\right) y_{2b} y_{2c} \\ &= \sum_{abc} \left(y_{1a} + \bar{z}_{1a} \oplus y_{1a} z_{1a}\right) y_{2b} y_{2c} \\ &\leq \left|\left\{y_{1a} = 0 \text{ and } z_{1a} = 0\right\}\right| \cdot \Delta^2 \leq (1 - \delta)\, \Delta^3 \end{aligned}$$

Claim. Let $y_1 y_2^\top, z_1 z_2^\top$ be codewords in $C_{A_1} \otimes C_{A_2}, C_{A_1} \otimes C_{A_3}$. And let w be the vector define by $w_{abc} = \left(y_1 y_2^\top\right)_{ab} \left(z_1 z_2^\top\right)_{ac}$. Then

$$d\left(w, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \leq (r\Delta)^4 (1 - \delta)\, \Delta^3$$

Consider the local

$$\begin{aligned} x_{abc} &= y_{ab} z_{ac} = \left(y_1 y_2^\top + \xi_y\right)_{ab} \left(z_1 z_2^\top + \xi_z\right)_{ac} \\ &\left(y_1 y_2^\top\right)_{ab} \left(z_1 z_2^\top\right)_{ac} = \left(\sum_{ij} \alpha_{ij} y_1^i y_2^{j\top}\right)_{ab} \left(\sum_{ij} \beta_{ij} z_1^i z_2^{j\top}\right)_{ac} \\ &= \sum_{ijlk} \alpha_{ij} \beta_{lk} y_{1a}^i y_{2b}^{j\top} z_{1a}^l z_{2c}^{k\top} \\ &\Rightarrow d\left(\left(y_1 y_2^\top\right)_{ab} \left(z_1 z_2^\top\right)_{ac}, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \\ &\quad \leq (\Delta r)^4 (1 - \delta)\, \Delta^3 \end{aligned}$$

ss ss

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