Quantum LTC With Positive Rate

David Ponarovsky

September 6, 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).

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

Then define the codes:

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

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

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

Definition Define the mapping (not linear)

$$\phi : \mathcal{T}\left(\Gamma_{\square_1} \cup \Gamma_{\square_2}, \mathbb{F}_2\right) \rightarrow \mathcal{T}\left(\Gamma_{\square\square}, \mathbb{F}_2\right)$$

as the summtion over the fowlloing local maps ϕ_g. which for given vertex $g \in V\left(\Gamma_{\square\square}\right)$ with local view c_1 on $\Gamma_{\square_1}$ and local view c_2 on $\Gamma_{\square_2}$ compute the tensor $c_{abc} = c_{1_{ab}} c_{2_{ac}}$ and set result bit on the plaquette defined by the vertices g, ag, gb, gc, agb, agc.

We will abuse the notation by defining for every subset of vertices $S \subset V$ the map $\phi_S = \sum_{g \in S} \phi_g$.

Lemma 1 Fix a vertex g and assume that the local views c_1, c_2 that lay over the graphs $\Gamma_{\square_1}, \Gamma_{\square_2}$ belongs to the dual tensors $\left(C_{A_1}^{\perp} \otimes C_{A_2}^{\perp}\right)^{\perp}, \left(C_{A_1}^{\perp} \otimes C_{A_3}^{\perp}\right)^{\perp}$. And inaddtion $1^{\Delta} \in C_{A_1}$ then

$$\phi_g\left(c_1, c_2\right) \in \left(C_{A_1}^{\perp} \otimes C_{A_2}^{\perp} \otimes C_{A_3}^{\perp}\right)^{\perp}$$

Proof. The case where $c_1 \in \mathbb{F}^{A_1} \otimes C_{A_2}$ or $c_2 \in \mathbb{F}^{A_1} \otimes C_{A_3}$ is trival. Suppose that both $c_1 \in C_{A_1} \otimes \mathbb{F}^{A_2}$ and $c_2 \in C_{A_1} \otimes \mathbb{F}^{A_3}$. And consider by h arbirary check of C_{A_1}.Then:

$$\begin{aligned}
\left\langle h_{bc}, \phi_g\left(c_1, c_2\right)\right\rangle \quad &= \sum_a h_a c_{abc} = \sum_a h_a c_{1_{ab}} c_{2_{ac}} = \\
&\overbrace{=}^{\text{for } y,z \in C_{A_1}} \quad \langle h, zy \rangle \\
&=
\end{aligned}$$

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 Vertices Are Normal Define a normal 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 and the rate of the small codes C_{A_j}, $\delta\Delta$ satisfy the equation $(\Delta r)^4 (1-2\delta) < \frac{1}{2}\delta^3$ 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 normal. 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 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 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 property.

So we can represent the locals views on g as the following disjointed 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 corresponded 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 coefficients 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 vector:

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

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 notice that $y_{1a} y_{2b} z_{2c}$ is a valid codeword of $C_{A_1} \otimes C_{A_2} \otimes C_{A_3}$. That because that the projection obtained by fixing any two coordinates yields either a zero or a codeword of one the codes.

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

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

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

$$d\left(w, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \leq (r\Delta)^4 (1-\delta)\,\Delta^3 + \Theta\left(\Delta^{2\frac{1}{2}}\right)$$

Consider again the representation of the local view w on the vertex g.

$$w_{abc} = y_{ab} z_{ac} = \left(y_1 y_2^\top + \xi_y\right)_{ab} \left(z_1 z_2^\top + \xi_z\right)_{ac}$$

$$\left(y_1 y_2^\top\right)_{ab} \left(z_1 z_2^\top\right)_{ac} = \left(\sum_{ij} \alpha_{ij} y_1^i y_2^{j\top}\right)_{ab} \left(\sum_{ij} \beta_{ij} z_1^i z_2^{j\top}\right)_{ac}$$

$$= \sum_{ijlk} \alpha_{ij} \beta_{lk} y_{1a}^i y_{2b}^{j\top} z_{1a}^l z_{2c}^{k\top}$$

$$\begin{aligned}&\Rightarrow d\left(\sum_{abc} \left(y_1 y_2^\top\right)_{ab} \left(z_1 z_2^\top\right)_{ac}, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \\ &\quad\leq (\Delta r)^4 (1-\delta)\,\Delta^3\end{aligned}$$

In addition its clear that $\left|\sum_{abc} \xi_{ab} \left(z_1 z_2^\top + \xi\right)_{ac}\right| \leq \sum_c \sum_{ab} |\xi_{ab}| \leq \Delta^{2\frac{1}{2}}$. Hence, we have that

$$d\left(w, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right) \leq (r\Delta)^4 (1-\delta)\,\Delta^3 + \Theta\left(\Delta^{2\frac{1}{2}}\right)$$

Dense Normal Net Counting Let us call the normal vertices the vertices with degree less then ξ in $\Gamma^{\cup,\square} = \Gamma^x_{\square,1} \cup \Gamma^x_{\square,2}$. And Let us say that that an edge of $\Gamma^\cup$ is heavy if it is incident to at least η squares in $\Gamma_{\square_1}$ and $\Gamma_{\square_2}$. Let T be set of vertices in V_0 that are connected to (at least) one normal vertex through a heavy edge.

First notice that the number of vertices in the induced graph by x is bounded by it's weight: $|S| \leq \frac{2|x|}{\delta\Delta}$

By the mixing Lemma we get:

$$
\begin{aligned}
&|E(S,T)| \geq \eta |T| \\
&|E(S,T)| = |E(S,T)_{\Gamma_1} \cup E(S,T)_{\Gamma_2}| \\
&\qquad \leq \frac{|S||T|}{n}(2 \cdot 2\Delta - \Delta) \\
&\qquad\quad + \sqrt{|S||T|}\,(2 \cdot \lambda_{\text{double cover}} + \lambda_{\text{ramnujan}})
\end{aligned}
$$

Hence we have that:

$$
|T|\left(\eta - \frac{2|x|}{\delta\Delta} \cdot \frac{3\Delta}{n}\right) \leq \sqrt{|S||T|}\lambda^\star
$$

$$
|T| \leq \left(\frac{\lambda^\star}{\eta - \frac{6|x|}{n\delta}}\right)^2 |S|
$$

Denote by S_e the set of vertices in $\Gamma^{\cup,\square}$ with degree greater then ξ. Then by repeating on the above calculation, while substituting Γ_i by $\Gamma_{i,\square}$, We obtain that there is $\lambda_2^\star$ such that:

$$
|S_e| \leq \left(\frac{\lambda_2^\star}{\xi - (2\Delta^2 - \Delta)\frac{|x|}{n\delta\Delta}}\right)^2 |S|
$$

Define $\bar{d}_T$ to be the average (over T) of heavy edges incident to a vertex of T. So

$$
\begin{aligned}
\bar{d}_T &= \frac{|E(T, S/S_e)|}{T} \geq \frac{|S| - |S_e|}{|T|} \\
&\geq \left(1 - \left(\frac{\lambda_2^\star}{\xi - (2\Delta^2 - \Delta)\frac{|x|}{n\delta\Delta}}\right)^2\right) \Big/ \left(\frac{\lambda^\star}{\eta - \frac{6|x|}{n\delta}}\right)^2
\end{aligned}
$$

Let us call to the quantity above $\Delta\rho$ and denote by $1-\tau$ the fraction of vertices of T with degree less then $\frac{1}{2}\Delta\rho$. Then $\Delta\rho \leq \bar{d}_T \leq 3\Delta\tau + (1-\tau)\Delta\rho \Rightarrow \tau \geq \frac{\rho}{2(3-\rho)} \geq \rho/3$. Namely, at least $\rho/3$ of vertices of T are incident to at least $\frac{1}{2}\Delta\rho$ heavy edges.

Since $\Gamma^\cup$ is 3Δ regular we get that $|S| - |S_e| \leq 3\Delta|T|$. In the other-hand we have shown that

$$
\begin{aligned}
&|S_e| \leq \left(\frac{\lambda_2^\star}{\xi - (2\Delta^2 - \Delta)\frac{|x|}{n\delta\Delta}}\right)^2 |S| \\
&\Rightarrow |S| \leq \left(1 - \left(\frac{\lambda_2^\star}{\xi - (2\Delta^2 - \Delta)\frac{|x|}{n\delta\Delta}}\right)^2\right)^{-1} 3\Delta|T| \\
&= (1 - \theta^2)\, 3\Delta|T|
\end{aligned}
$$

And by using again the mixing Lemma we have that:

$$
\begin{aligned}
E(S_e, T) &\leq \frac{\theta^2}{1-\theta^2} 3\Delta|T|^2 \frac{3\Delta}{n} + \lambda^\star\sqrt{\frac{\theta^2}{1-\theta^2}}|T| \\
&\leq \left(\frac{\theta^2}{1-\theta^2} 9\Delta^2 + \lambda^\star\sqrt{\frac{\theta^2}{1-\theta^2}}\right)|T| \\
&\leq (9\Delta^2 + \lambda^\star)|T|
\end{aligned}
$$

Hence at most an $\frac{1}{6}\rho$ proportion of vertices of T are adjacent to more than $\frac{6}{\rho}(9\Delta^2 + \lambda^\star)$ vertices of S_e, And at least $\frac{5}{6}\rho$ proportion of T are adjacent to less then $\frac{6}{\rho}(9\Delta^2 + \lambda^\star)$. And therefore we have that at least $\frac{1}{6}\rho$ vertices are:

1. Incident to at least $\frac{1}{2}\Delta\rho$ heavy edges.
2. Adjacent to at most $\frac{6}{\rho}(9\Delta^2 + \lambda^\star)$ vertices of S_e.

Proof Of Theorem 1 Let us call to the set of vertices satisfy the constraints above **good vertices**. Pick any good vertex $g \in T$. Remember that each heavy edge between a normal vertex of S and a vertex of T corresponds to either a row or a column shared by the two local views.

By w-robustness, for any small enough $\xi \leq w$, the local view of any normal vertex is supported on at most $\frac{\xi}{\delta\Delta}$ rows and columns. Hence, the row (or column) shared between the normal vertex and v is at distance at most $\frac{\xi}{\delta\Delta}$ from a nonzero codeword of C_{A_1} (or C_{A_2}, C_{A_3}).

Let us denote by $x_{v'}$ the the local view obtained by taking only the rows and columns that shared between v and normal vertices. The γ-resistance to puncturing property implies that if we could find η, ξ such that for any $|x| \leq d$ we have:

$$
\frac{6}{\rho}(9\Delta^2 + \lambda^\star) \leq \gamma \qquad \left(\Theta\left(\Delta^{\frac{1}{2}}\right)\right)
$$

Then the local view of v is at distance at most:

$$
\begin{aligned}
&d(x_v, C_{A_1} \otimes C_{A_2} \otimes C_{A_3}) \\
&\quad \leq d(x_{v'}, \cdot) + |\text{ ignored bits }| \\
&\quad \leq d(x_{v'}, \cdot) + \frac{3}{2}\Delta^2 \cdot \frac{6}{\rho}(9\Delta^2 + \lambda^\star)
\end{aligned}
$$

Choosing $\eta, \xi, \delta, \gamma, w, |x| < d$ such that the above is lower than $\frac{1}{2}(\delta\Delta)^3$ finishes the proof.

Theorem 2. *The code $C_w/\mathcal{T}(\Gamma_{\square\square}, (C_{A_1} \otimes C_{A_2} \otimes C_{A_3}))$ has positive rate and linear distance.*

Theorem 3. *The code defined by C_x has an efficient test for rejecting candidate with high error weigh.*