Quantum LTC With Positive Rate

David Ponarovsky

September 19, 2022

Tasks.

1. Prove that the construction indeed yields a square complex. (The gentle point is to formalize a general TNC property).
2. Prove that C_x and C_z are indeed CSS pair. Its not so clear how to show that. We hope to prove that either we can choose as generator the forth tensor power product or at least that the generators cubics corresponded to edges in the original graph (i.e $(g \sim ag)$ edge) share structure (that enforce meeting between duals).
3. 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). (Make the requirement changes for the new 4D complex with minimal erases, as possible).
4. Show that we could actually choose such $\{A\}_i$ and the matched small codes. (Last priority.)
5. Write a program which plot small complex in a small scale for getting more intuition.

1 Existance Of 4D Robustness (Small) Codes.

Defintion. Let C be a linear binary code in $\mathbb{F}_2^{\Delta}$. We will say that C has the $(\gamma, \delta)-$*Base Generators Set* property if C is spanned by the vectors $V = \{v_0, v_1, v_2, \ldots v_m\}$ such that the weight of any $v_i \in V$ is at least $\delta\Delta$ and for any $j \in [\Delta]$ at most $\gamma\Delta$ vectors from V has the j'th bit turn on. Namly:

$$|\left\{v_i; v_i \in V, (v_i)_j = 1\right\}| \le \gamma\Delta$$

Robusntess Lemma. proof.

p-resistence conserve γ-property. proof.

Graph Represantion Of The Base. Def.

The Dual Tensors Have $(\gamma, \delta)-$generators base set. proof.

2 The Code.

The Construction. Fix primes q, p_0, p_2, p_3, p_4 such that each of them has 1 residue mode 4. Let A_1, A_2, A_3, A_4 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 the pairs A_1, A_2 and A_3, A_4 satisfy the TNC constraint and also they all satisfy that constraint together, manly for any $g \in \mathbf{PGL}$ and $a_1 \in A_1, a_2 \in A_2, a_3 \in A_3, a_4 \in A_4$ we have that $g \neq a_3 a_1 g a_2 a_4$.

For any $h \in \mathbb{Z}_3^2$ define the groups G^h, H^h to be:

$$\begin{aligned} H^h &= h + \mathbb{Z}_3^2 \cap \langle (1,1) \rangle \\ G^h &= \mathbf{PGL} \times H^h \end{aligned}$$

Then consider the graphs:

$$\begin{aligned}
\Gamma_{\square_1}^h &= \left(G^h, \left\{ ((g, h_1), (agb, h_1 + (1,1))) : \right.\right. \\
&\qquad \left.\left. a \in A_1, b \in A_2, h_1 \in H^h \right\} \right) \\
\Gamma_{\square_2}^h &= \left(G^h, \left\{ ((g, h_1), (cgd, h_1 + (1,1))) : \right.\right. \\
&\qquad \left.\left. c \in A_3, d \in A_4, h_1 \in H^h \right\} \right) \\
\Gamma_{\square\square}^h &= \left(G^h, \left\{ ((g, h_1), (cagbd, h_1 + (2,2))), (g, acgdb) : \right.\right. \\
&\qquad \left.\left. a \in A_1, b \in A_2, c \in A_3, d \in A_4, h_1 \in H^h \right\} \right)
\end{aligned}$$

Then define the codes:

$$\begin{aligned}
C_z &= \mathcal{T}\left(\Gamma_{\square\square}^h, (C_{A_1} \otimes C_{A_2})^{\perp} \otimes (C_{A_3} \otimes C_{A_4})^{\perp}\right) \\
C_x &= \mathcal{T}\left(\Gamma_{\square\square}^h, (C_{A_1}^{\perp} \otimes C_{A_2}^{\perp})^{\perp} \otimes (C_{A_3}^{\perp} \otimes C_{A_4}^{\perp})^{\perp}\right) \\
C_w &= \mathcal{T}\left(\Gamma_{\square\square}^h, \left((C_{A_1}^{\perp} \otimes C_{A_2}^{\perp})^{\perp} \otimes (C_{A_3}^{\perp} \otimes C_{A_4}^{\perp})^{\perp}\right)^{\perp}\right)
\end{aligned}$$

Notice that that C_x could be viewed as the classical LTC code in Levarier and Zemor construction by treating the tensor product as standing alone small code. **[COMMENT]** Task 1.

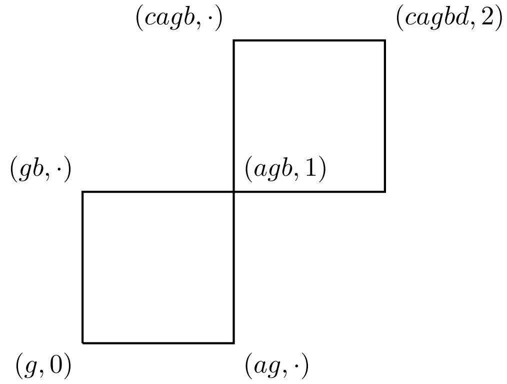

Figure 1: Square of the complex, with edges $(g,ag),(agb,gb)\in E_A,(g,gb),(agb,ag)\in E_B$.

Lemma 1 *The pair C_x, C_z defined above is CSS code.*

Proof. Let $c^{(1)}, c^{(2)}$ be codewords in C_x and C_z then:

$$\begin{aligned}\langle c^{(1)}, c^{(2)}\rangle &= \sum_{\text{plaquettes}} c_i^{(1)}c_i^{(2)} = \sum_{\text{plaquettes}} c_{gabcd}^{(1)}c_{gabcd}^{(2)}\\ &= \sum_{cd}\sum_{gab} c_{gabcd}^{(1)}c_{gabcd}^{(2)}\end{aligned}$$

By the fact that for any fixed c,d we have that the induced words are codewords of the orignal codes (from Zemor and Levarier) the product above is zeroed.

Plaquettes Expansion. Let, S,T be vertices subsets of G^h and Let $S^\star$ be the vertices which can be reached from S trough edges from $\Gamma^h_{\square_1}$. By regularity it's clear that $S^\star \leq \Delta^2|S|$. In addition, by the fact that G^h is a group, we have that $agb = ag'b$ if and only if $g=g'$. Therefore we could derive a lowerbound on the size of $S^\star$ by fixing a,b and consider the vertices corresponded to $aSb \subset S^\star$. Then by the mixing expansion lemma we get:

$$\begin{aligned}&E(S,T)_{\Gamma^h_{\square\square}} = E(S^\star,T)_{\Gamma^h_{\square_1}}\\ &|E(S,T)_{\Gamma^h_{\square\square}}| \leq \frac{\Delta^2}{n}\Delta^2|S||T| + \lambda_{\Gamma^h_{\square_2}}\Delta\sqrt{|S||T|}\\ &|E(S,T)_{\Gamma^h_{\square\square}}| \geq \frac{\Delta^2}{n}|S||T| - \lambda_{\Gamma^h_{\square_2}}\sqrt{|S||T|}\end{aligned}$$

Step-Edges Expansion. Let us define a step-edge to be a concation of e_1,e_2 edges in $\Gamma^h_{\square_1},\Gamma^h_{\square_2}$ such that e_1,e_2 are adjacent in the union of $\Gamma^h_{\square_1},\Gamma^h_{\square_2}$ and they both either left or right edges. Now consider again two vertices subsets S and T and denote by $E(S,T)_{\text{step}}$ the cut contains the step-edges between T and S. Consider now subsets $S^\star_L$ and $S^\star_R$ which are the vertices which can be reach from S trough left, right edges. And notice that each step-edge is a path compused by an source vertex from S, an intermdiate vertex from $S^\star_L$ or $S^\star_R$ and a target vertex from T.

In addition, by regularity the size of $S^\star_L$ is at most $\Delta|S|$. And again by the fact that the edges are coressponded to Group generators, $S^\star_L$ can be bounded from below by considering the multiplication of S by single generator.

Hence by applaing the Mixing Lemma we have:

$$\begin{aligned}&E(S,T)_{\text{step}} = E(S^\star_L,T)_{\cdot} + E(S^\star_R,T)_{\cdot}\\ &|E(S,T)_{\text{step}}| \leq \frac{2\Delta}{n}\Delta|S||T| + 2\lambda\sqrt{\Delta|S||T|}\\ &|E(S,T)_{\text{step}}| \geq \frac{2\Delta}{n}|S||T| - 2\lambda\sqrt{|S||T|}\end{aligned}$$

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 a step-edge is an heavy edge if it incidents to at least η plaquettes.

Let T be set of vertices in V_0 that are connected to (at least) one normal vertex through a heavy edge.

Recall that the distance of the tensor code equal to the notice that the number of vertices in the induced graph by x is bounded by it's weight: $|S| \leq \frac{2|x|}{\delta^2\Delta^2}$

By the mixing Lemma we get:

$$\begin{aligned}&|E(S,T)_{\text{step}}| \geq \eta|T|\\ &\Rightarrow |T|\left(\eta - \frac{2\Delta^2\cdot 2|x|}{n(\delta\Delta)^2}\right) \leq 2\lambda\sqrt{\Delta|S||T|}\end{aligned}$$

Hence we have that:

$$\begin{aligned}&\sqrt{|T|}\left(\eta - \frac{2\Delta^2\cdot 2|x|}{n(\delta\Delta)^2}\right) \leq 2\lambda\sqrt{\Delta|S|}\\ &|T| \leq \left(\frac{2\lambda\sqrt{\Delta}}{\eta - \frac{4|x|}{n\ \delta^2}}\right)^2|S|\end{aligned}$$

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 $\lambda^\star_2$ such that:

$$\begin{aligned}&|E(S,T)_{\Gamma^h_{\square\square}}| \geq \xi|S_e|\\ &\Rightarrow |S_e|\left(\xi - \frac{\Delta^4\cdot 2|x|}{n(\delta\Delta)^2}\right) \leq \lambda_{\Gamma^h_{\square_2}}\Delta\sqrt{|S||S_e|}\end{aligned}$$

Hence we have that:

$$\begin{aligned}&\sqrt{|S_e|}\left(\xi - \frac{\Delta^4\cdot 2|x|}{n(\delta\Delta)^2}\right) \leq \lambda_{\Gamma^h_{\square_2}}\Delta\sqrt{|S|}\\ &|S_e| \leq \left(\frac{\lambda_{\Gamma^h_{\square_2}}\Delta}{\xi - \frac{\Delta^2\cdot 2|x|}{n\ \delta^2}}\right)^2|S|\end{aligned}$$

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

$$\begin{aligned}\bar{d}_T &= \frac{|E(T,S/S_e)|}{T} \geq \frac{|S|-|S_e|}{|T|}\\ &\geq \left(1 - \left(\frac{\lambda_{\Gamma^h_{\square_2}}\Delta}{\xi - \frac{\Delta^2\cdot 2|x|}{n\ \delta^2}}\right)^2\right) \Big/ \left(\frac{2\lambda\sqrt{\Delta}}{\eta - \frac{4|x|}{n\ \delta^2}}\right)^2\end{aligned}$$

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

Since each vertex is a source for at most $2\Delta^2$ step-edges we get that $|S| - |S_e| \leq 2\Delta^2|T|$.

mark In the other-hand we have shown that

$$
\begin{aligned}
|S_e| &\leq \left(\frac{\lambda_{\Gamma^h_{\square_2}}\Delta}{\xi - \frac{\Delta^2\cdot 2|x|}{n\ \delta^2}}\right)^2 |S| \\
\Rightarrow |S| &\leq \left(1 - \left(\frac{\lambda_{\Gamma^h_{\square_2}}\Delta}{\xi - \frac{\Delta^2\cdot 2|x|}{n\ \delta^2}}\right)^2\right)^{-1} 2\Delta^2|T| \\
&= \left(1-\theta^2\right)^{-1} 2\Delta^2|T|
\end{aligned}
$$

And by using again the mixing Lemma we have that:

$$
\begin{aligned}
E\left(S_e, T\right)_{\text{step}} &\leq \frac{\theta^2}{1-\theta^2}2\Delta^2|T|^2\frac{2\Delta^2}{n} + \lambda\sqrt{\frac{\theta^2}{1-\theta^2}}|T| \\
&\leq \left(\frac{\theta^2}{1-\theta^2}4\Delta^2 + \lambda\sqrt{\Delta}\sqrt{\frac{\theta^2}{1-\theta^2}}\right)|T|
\end{aligned}
$$

Hence at most an $\frac{1}{6}\rho$ proportion of vertices of T are adjacent to more than $\frac{6}{\rho}\left(4\Delta^2+\lambda\right)$ vertices of S_e, And at least $\frac{5}{6}\rho$ proportion of T are adjacent to less then $\frac{6}{\rho}\left(4\Delta^2+\lambda\right)$. And therefore we have that at least $\frac{1}{6}\rho$ vertices are:

1. Incident to at least $\frac{1}{2}2\Delta^2\rho$ heavy edges.
2. Adjacent to at most $\frac{6}{\rho}\left(4\Delta^2+\lambda\sqrt{\Delta}\right)$ vertices of S_e.

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 $\Gamma_{\square_1}, \Gamma_{\square_2}$:

$$
\begin{aligned}
y &= y_1 y_2^\top + \xi_y \\
z &= z_1 z_2^\top + \xi_z
\end{aligned}
$$

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

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

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

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

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:

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

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

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

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

Theorem 2. *The code $C_w/\mathcal{T}\left(\Gamma_{\square\square}, \left(C_{A_1} \otimes C_{A_2} \otimes C_{A_3}\right)\right)$ 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.*

The Decoder. Let x be a candidate that might or might not be in C_x. The decoder $\mathcal{D}$ describe below return a valid codeword of C_X if x is at distance at most $\tilde{\alpha}$ from C_x and otherwise reject. First, for every positive (left) vertex $g \in G \times \mathbb{Z}_2$, $\mathcal{D}$ compute the codeword of the dual tensor code which is the closest to its local view. Denote each that codeword by c_g. Then define the mismatch to be $z = \sum_{g \in G} c_g$ and notice that by the fact that each face is summed up twice $|z|$ equal the number of disagreements.

If $|z|$ is indeed zero, then $\tilde{z}$ which define by taking the "AND" of local correction instead of xoring them is a valid codeword. $\mathcal{D}$ will defined to returns $\tilde{z}$ in that case.

Assume that $|z| > 0$. Then $\mathcal{D}$ will:

1. Compute for every negative vertex the closest local view correspond to $\phi_g^{\perp}$. Call it, ω_g.

2. Sum the $\omega' s$. And set the yielded bits on the plaquettes. Denote the word obtained by that by J.

Clearly $J \in C_w$. Denote by e the error, i.e $e + x \in C_x$. Let us decompose

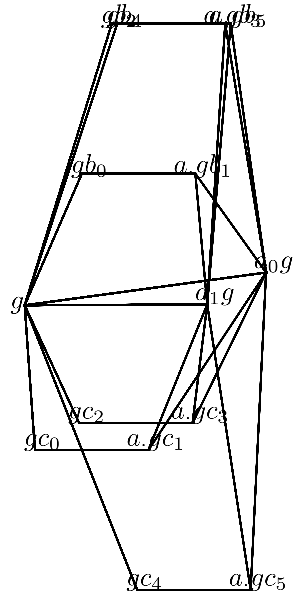

Figure 2: Square of the complex, with edges $(g, ag), (agb, gb) \in E_A, (g, gb), (agb, ag) \in E_B$.

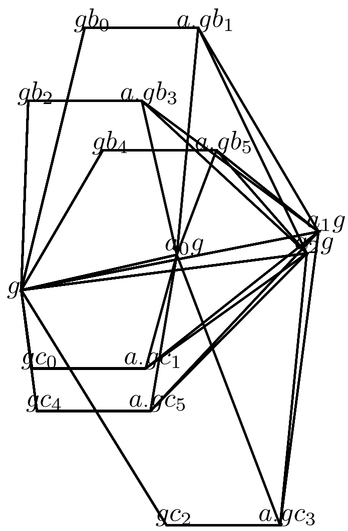

Figure 3: Square of the complex, with edges $(g, ag), (agb, gb) \in E_A, (g, gb), (agb, ag) \in E_B$.

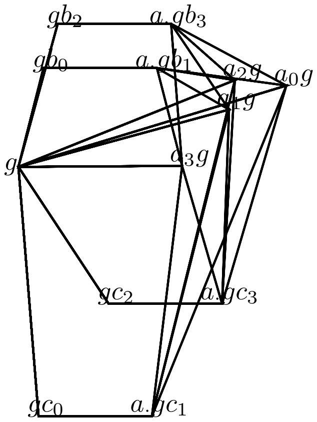

Figure 4: Square of the complex, with edges $(g, ag), (agb, gb) \in E_A, (g, gb), (agb, ag) \in E_B$.

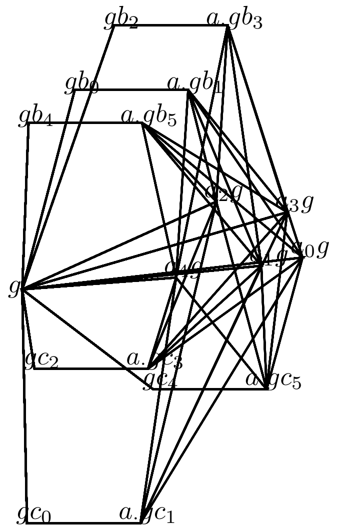

Figure 5: Square of the complex, with edges $(g, ag), (agb, gb) \in E_A, (g, gb), (agb, ag) \in E_B$.

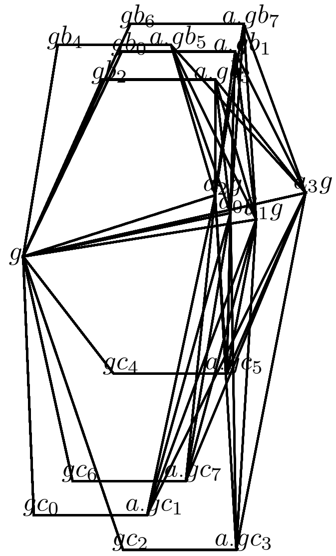

Figure 6: Square of the complex, with edges $(g, ag), (agb, gb) \in E_A, (g, gb), (agb, ag) \in E_B$.