Quantum Coding Theory **(UC Berkeley CS294, Spring 2024)**

Lecture 21: Quantum Tanner Code Distance

April 10, 2024

Lecturer: John Wright *Scribe: Angelos Pelecanos*

Recall that in the last two lectures, we saw the construction of quantum Tanner codes [LZ22], computed some of their parameters, and proved that they are a CSS code. In this lecture, we continue our study of quantum Tanner codes, and in particular, we will compute their distance.

Let us first recall what we know about quantum Tanner codes.

1 Quantum Tanner code review

1.1 Left-right Cayley complex

Let G be a group and A, B be two sets of generators each of size Δ that are closed under inverse. We defined the *left-right Cayley* complex to be a graph on 4 copies of the set of elements of G. In particular, let $V_{ij} = G \times \{ij\}$ for $i, j \in \{0, 1\}$. The left-right Cayley complex has vertex set $V_{00} \cup V_{01} \cup V_{10} \cup V_{11}$ and it has 4 kinds of edges, labeled as A- or B-edges.

- A-edge between $(g, 00)$ and $(ag, 10)$ for all $a \in A, g \in G$.
- A-edge between $(gb, 01)$ and $(agb, 11)$ for all $a \in A, g \in G$.
- B-edge between $(g, 00)$ and $(gb, 01)$ for all $b \in B, g \in G$.
- B-edge between $(ag, 10)$ and $(agb, 11)$ for all $b \in B, g \in G$.

Notice how the vertices $(g, 00), (ag, 10), (agb, 11), (gb, 01)$ and their connections are connected in a square, for all values of a, g, b. We defined Q to be the set of such squares, and the quantum Tanner code is defined on these squares.

For a vertex $v \in V_{00}$, we define its Q-neighborhood to be the set of squares incident to v. It is not hard to see that each square incident to v is parametrized by (a, b) in $A \times B$. Thus we can arrange the Q-neighborhood of v in a $\Delta \times \Delta$ square, where each row corresponds to an element of A and each column corresponds to an element of B.

We define the Q-neighborhood for vertices in $V_{01} \cup V_{11} \cup V_{10}$ in a similar way (but slightly different for each set), such that we can arrange the Q-neighborhood squares in the convenient way shown in Figure 1.

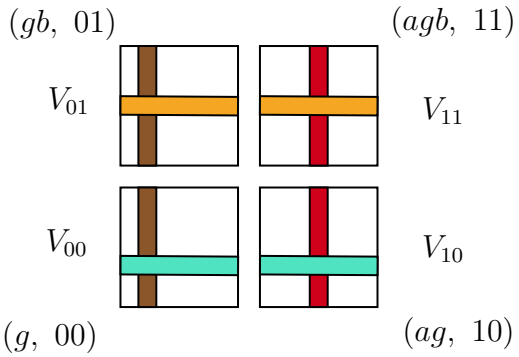

Figure 1: A convenient way to represent the Q-neighborhoods of vertices. Each vertex participates in Δ^2 squares, one for each pair $(a, b) \in A \times B$. These can be arranged in $\Delta \times \Delta$ squares. Moreover, if we arrange the squares as above, the vertices $(g, 00)$ and $(gb, 01)$ share a column (the one that corresponds to $b \in B$ for $(g, 00)$). Similarly for other vertices, any two columns and rows with the same color are shared in the figure above.

1.2 X and Z codes

Armed with the left-right Cayley complex setup, we defined two codes on it:

- Code C_A with parameters $[\Delta, \rho\Delta]$, and
- Code C_B with parameters $[\Delta, (1-\rho)\Delta]$.

Last class, we showed that the resulting quantum Tanner code has constant rate as long as $\rho \neq \frac{1}{2}$. We will also see today that for our code to have good distance, we want the codes $C_A, C_B, C_A^\perp, C_B^\perp$ to have distance at least $\delta\Delta$ for some positive constant δ.

Since the quantum Tanner code is a CSS code, it suffices to specify its X and Z codes to describe it. For that, let us define the "square" graph $\mathcal{G}_0^\square$ to be the bipartite graph with vertex set $V_{00} \cup V_{11}$ that has an edge between $(v, 00)$ and each vertex of V_{11} that is in its Q-neighborhood, and vice versa. The bipartite graph $\mathcal{G}_1^\square$ is defined similarly, over the vertices of $V_{01} \cup V_{10}$.

- We denote the X code by Code_0. It requires that for all $v \in V_{00} \cup V_{11}$,

$$Q(v) \in C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp.$$

  Equivalently, this is the (classical) Tanner code $\mathrm{Tan}\left(\mathcal{G}_0^\square, C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp\right)$.

- We denote the Z code by Code_1. It requires that for all $v \in V_{01} \cup V_{10}$

$$Q(v) \in C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B.$$

  Equivalently, this is the (classical) Tanner code $\mathrm{Tan}\left(\mathcal{G}_1^\square, C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B\right)$.

1.3 More properties

Another desirable property for our sets A, B is that we want their left and right Cayley graphs $\mathsf{Cay}_L(G, A), \mathsf{Cay}_R(G, B)$ respectively to be Ramanujan. This implies that the resulting square graphs $\mathcal{G}_0^\square$ and $\mathcal{G}_1^\square$ are *almost* Ramanujan, which means that[1]

$$\lambda(\mathcal{G}_0^\square), \lambda(\mathcal{G}_1^\square) \leq 4\Delta.$$

We also saw that we want the two codes

$$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B \quad \text{and} \quad C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp$$

to be K-product expanding [KP23] [2]. This means that each codeword $x \in C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$ can be decomposed as $x = c + r$, where the columns of c are codewords of C_A, and the rows of r are codewords of C_B.

$$c = \underbrace{\begin{bmatrix} | & | & | \\ | & | & | \\ | & | & | \end{bmatrix}}_{\in C_A}, \quad r = \begin{bmatrix} - & - & - \\ - & - & - \\ - & - & - \end{bmatrix} \in C_B$$

This decomposition of x must satisfy that $|x| = |c + r| \geq K\Delta\left(\|c\| + \|r\|\right)$. Here we use $\|\cdot\|$ to denote the *norm* of a codeword. In particular, $\|c\|$ and $\|r\|$ are equal to the number of non-zero columns of c and non-zero rows of r respectively. One may be able to write some x as a sum of $c + r$ in multiple ways, but we will be interested in the pair (c, r) that minimizes the sum of the norms $\|c\| + \|r\|$.

Definition 1.1 (Minimal representation of a codeword)**.** The *minimal representation* of x is the decomposition $x = c + r$ which minimizes $\|c\| + \|r\|$.

2 Distance of Z Code

We will start by bounding the distance of the Z code, which turns out to be slightly easier than the distance of the X code. Recall that the distance of the Z code is defined as follows

$$d_Z^+ = \min_{x \in \mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp} |x|.$$

Let $x \in \mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp$. Let x_v be the restriction of the codeword x to the Q-neighborhood of v. Then for all $v \in V_{01} \cup V_{10}$,

$$x_v \in C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B.$$

[1] Recall that the square graphs are Δ^2-regular, and thus the bound on their eigenvalue is only twice the bound for a Ramanujan graph.

[2] Can you find a code that is not K-product expanding?

2.1 Codewords of minimal norm

To bound the distance of the Z code we are interested in the minimum Hamming weight of a codeword. In this section, we will study the *norm* of a codeword, a related quantity to the Hamming weight.

Consider the following thought experiment: We will decompose the word x_v into its minimal representation $x_v = c_v + r_v$ and consider the sum of c_v and r_v's for all $v \in V_{01}$. In particular, we will define

$$C_0 = \sum_{v \in V_{01}} c_v, \quad R_1 = \sum_{v \in V_{01}} r_v.$$

Here C_0, R_1 are bit-strings of length Q and satisfy $C_0 + R_1 = x$.

We will repeat the above thought experiment for the vertices in V_{10}. Formally, let

$$C_1 = \sum_{v \in V_{10}} c_v, \quad R_0 = \sum_{v \in V_{10}} r_v.$$

Like before, $C_1 + R_0 = x$. Let us now extend the notion of a minimal representation to codewords of the quantum Tanner code[3].

Definition 2.1 (Representation and minimal representation)**.** The tuple (C_0, C_1, R_0, R_1) is a *representation* of x. It is *minimal* if its norm $\|C_0\| + \|C_1\| + \|R_0\| + \|R_1\|$ is minimized, where $\|C_i\|$ is the number of non-zero columns, and $\|R_i\|$ is the number of non-zero rows.

The two representations (C_0, R_1) and (C_1, R_0) may seem unrelated, except for the fact that they both sum to x. We will now see another important relationship between these two pairs of strings. We start from the fact that they have the same sum

$$C_0 + R_1 = C_1 + R_0,$$

and add $R_0 + R_1$ to both sides. Since we are working modulo 2, we get

$$C_0 + R_0 = C_1 + R_1.$$

We have concluded that the two sums above, which we defined in our thought experiment, are equal, and somehow give us an alternative weird way of labeling the squares. Let their sum be equal to $x_0 \in \{0,1\}^Q$. We will see that this x_0 does not lie in the codes we have so far but rather lies in another, related code.

Recall the quantum Tanner code picture of Figure 2. We can see that $x_0 = C_0 + R_0$, when restricted to the Q-neighborhood of $(g, 00)$ is in $C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$. The same holds for x_0, when restricted to the Q-neighborhood of $(agb, 11)$. Thus x_0 lies in a different code than Code_0, and in particular x_0 is a completely new string in $\mathrm{Tan}\left(\mathcal{G}_0^{\square}, C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B\right)$.

[3] Definition 1.1 defined a minimal representation for a codeword restricted to a $Q(v)$-neighborhood. We extend this definition to a codeword of the whole Tanner code.

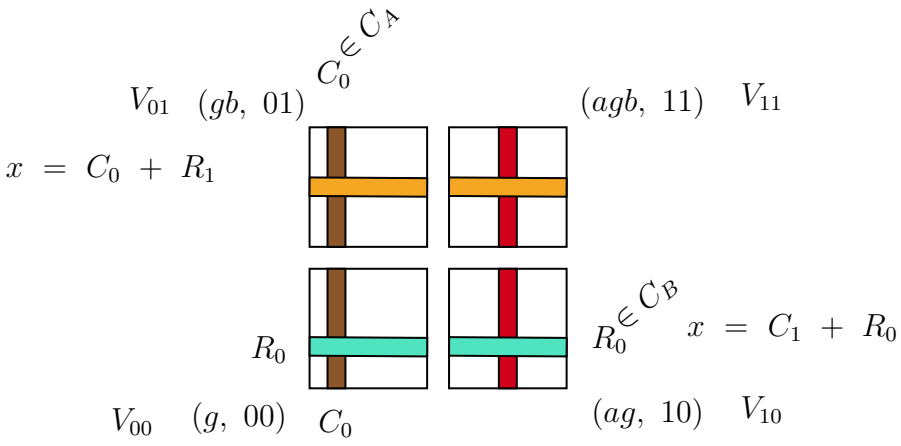

Figure 2: The quantum Tanner code.

To conclude the distance of the Z code, we will show that (C_0, C_1, R_0, R_1) is also a minimal representation for x_0.

For the sake of contradiction, assume that (C_0, C_1, R_0, R_1) is not minimal for some $v \in V_{00} \cup V_{11}$. For simplicity, let's assume that $v \in V_{00}$. Then

$$\begin{aligned}(x_0)_v &= (C_0)_v + (R_0)_v \\ &= c_v + r_v.\end{aligned}$$

Since it is not minimal, we can also write $x_0 = c'_v + r'_v$ for some c'_v, r'_v with fewer non-zero rows and columns. Then instead,

$$\begin{aligned}(x_0)_v &= c'_v + r'_v \\ &= (c_v + t_v) + (r_v + t_v).\end{aligned}$$

since for c'_v, r'_v to have the same sum, it must hold that we have added to both the same value t_v (modulo 2).

Observation 2.2. *The value of t_v must be a codeword of $C_A \otimes C_B$.*

Proof. We can write t_v as $c'_v + c_v$. Since both c'_v and c_v have columns that are in C_A, so are the columns of t_v. Similarly, $t_v = r'_v + r_v$. Both r'_v and r_v have rows that are in C_B, which must also hold for t_v. Thus $t_v \in C_A \otimes C_B$. □

But recall that

$$t_v \in C_A \otimes C_B = \left(C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp\right)^\perp = \mathsf{Code}_0^\perp.$$

Remark 2.3. It may be useful to remember here the toric code, where the elements of $C_Z \setminus C_X^\perp$ were cycles, and two cycles were equivalent up to adding plaquette boundaries, which are in $C_X^\perp$.

Back to the quantum Tanner code, we will take our string C_0 and replace it with $C_0 + t_v$, and we will do the same with R_0 with $R_0 + t_v$. Then indeed

$$\|C_0 + t_v\| + \|R_0 + t_v\| + \|C_1\| + \|R_1\| < \|C_0\| + \|R_0\| + \|C_1\| + \|R_1\|.$$

But now we have changed our x string, because

$$x = \begin{array}{ccc} C_0 + R_1 & \to & C_0 + R_1 + t_v \\ C_1 + R_0 & \to & C_1 + R_0 + t_v \end{array} = \text{element of } \{x + \mathsf{Code}_0^\perp\} \text{ with reduced norm.}$$

Since $x \in \mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp$ by construction, $x + t_v$ also lies in the same set. We conclude the following lemma.

Lemma 2.4. *If x has a minimal norm in coset $\{x + \mathsf{Code}_0^\perp\}$ then a minimal representation for x is equal to a minimal representation for x_0.*

2.2 From minimal norm to distance bound

In the previous section, we identified a minimal norm codeword in a coset. In this section, we will use the K-product expanding property to transfer norm bounds to Hamming weight bounds and compute the distance.

Our goal will be to show that the norm of each element in $\mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp$ is at least a constant times the number of qubits n.

Claim 2.5. *For any $x \in \mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp \in \{0,1\}^Q$,*

$$\|x\| \geq \frac{\delta^2 K \cdot n}{512 \cdot \Delta^2}.$$

We will prove this claim in the next lecture. For the remainder of this lecture, we will demonstrate a lower bound on the distance of the Z code, assuming the statement of Claim 2.5.

Theorem 2.6. *The distance of the Z code satisfies*

$$d_Z^+ = \min_{x \in \mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp} |x| \geq \frac{\delta^2 K^2}{1024 \cdot \Delta} \cdot n.$$

Proof. Let x be an element of the set $\mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp$ with minimal norm. Moreover, let (C_0, C_1, R_0, R_1) be a minimal representation of x. Look at the decomposition $x = C_0 + R_1 = \sum_{v \in V_{01}} (c_v + r_v)$. It holds that

$$|x| = \sum_{v \in V_{01}} |c_v + r_v| \geq \sum_{v \in V_{01}} K \cdot \Delta \cdot (\|c_v\| + \|r_v\|) = K\Delta \cdot (\|C_0\| + \|R_1\|). \tag{1}$$

We can similarly decompose $x = C_1 + R_0$, so

$$|x| \geq K\Delta \cdot (\|C_1\| + \|R_1\|). \tag{2}$$

We deduce that $|x|$ is at least the average of the two quantities from Equations (1) and (2)

$$\begin{aligned}|x| &\geq \frac{1}{2}K\Delta \cdot (\|C_0\| + \|C_1\| + \|R_0\| + \|R_1\|) \\ &= \frac{1}{2}K\Delta \cdot \|x\| \\ &\geq \frac{\delta^2 K^2}{1024 \cdot \Delta} \cdot n.\end{aligned}$$

Bounding the Hamming weight of x suffices since any other element of $\mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp$ will have norm at least $\|x\|$, and thus the same Hamming weight lower bound applies. □

In conclusion, Claim 2.5 and Theorem 2.6 formalized our intuition that lower bounding the norm of a codeword in $\mathsf{Code}_1 \setminus \mathsf{Code}_0^\perp$ provides a lower bound for this Hamming weight, which in turn allows us to bound the distance of the Z code.

References

[KP23] Gleb Kalachev and Pavel Panteleev. Two-sided robustly testable codes, 2023. 1.3

[LZ22] Anthony Leverrier and Gilles Zémor. Decoding quantum tanner codes, 2022. (document)