

Removing The w -Robustness Assumptions.

David Ponnarovsky

February 3, 2023

Abstract

We propose an alternative simple construction of good LTC codes.

1 Preambles

In this work, we propose a new construction for good LDPC codes, which also have a good testability parameter. In the sense that verifying a constant number of random checks, would be enough to detect any error with probability proportional to the error size. In contrast to previous constructions made by [Din+22], [LZ22] and [PK21], our construction doesn't require spicel properties of the small codes, such as w -robustness and p -resistance for puncturing.

Our proof also indirectly answers the following question. Why most of the good LDPC codes are known to be bad in terms of detecting errors? In other words, It seems that for most of them, there exist strings that are very far from being in the code and, meanwhile, fail to satisfy only a small number of restrictions. While the previous LDPC constructions focused on ensuring that the yielded code would have a good rate and distance parameters, our construction enforces the restrictions collection to have a nontrivial fraction of degeneration. That is, removing a single restriction will not change the code, as any restriction is linearly dependent on the others.

1.1 Tanner testability.

This subsection will explain why testability is so hard to achieve. Let C be a good Tanner expander code as defined above. And consider an arbitrary vertex $u \in V$ and arbitrary restriction of C_0 , h . Now define \tilde{C} as the code obtained by requiring all the restrictions of C except h on u . That is, u is satisfied if his local view satisfies all the C_0 restrictions apart from h . Also, for convenience, denote the small code u enforces on his local view by C_0^u . Let us assume that the distance of C_0^u is at least $\delta\Delta$. Then, by repeating almost exactly the steps above with caution, one could prove that \tilde{C} also has a linear distance.

Assume that $\tilde{C} \neq C \Rightarrow$ there exists $x \in \tilde{C}/C$. By definition, for any $v \in V/\{u\}$ it holds that $x|_v \in C_0$. Hence, the assumption that $x \notin C$ implies $x|_u \notin C_0$. So, clearly, x fails at a constant number of C 's checks. On the other hand, the closest codeword $y \in C$ to x is also a codeword of \tilde{C} as $y|_v \in C_0$ for every $v \in V$. Hence:

$$d(x, C) = d(x, y) \geq d(\tilde{C}) = \Theta(n)$$

Even if a linear number of bits needed to be flipped to correct x , only a single check observes that x is indeed an error.

2 Construction

2.1 Almost LTC With Zero Rate

Definition. The Disagreement Code. Given a Tanner code $C = \mathcal{T}(G, C_0)$, define the code C_\oplus to contain all the words equal to the formal summation $\sum_{v \in V(G)} c_v$ when c_v is an assignment of a codeword $c_v \in C_0$ on the edges of the vertex $v \in V(G)$. We call to such code the *disagreement code* of C , as edges are set to 1 only if their connected vertices contribute to the summation codewords that are different on the corresponding bit to that edge. In addition, we will call to any contribute c_v , the *suggestion* of v . And notice that by linearity, each vertex suggests, at most, a single suggestion.

Finally, given a bits assessment $x \in \mathbb{F}_2^E$ over the edges of G , we will denote by $x^\oplus \in C_\oplus$ the codeword which obtained by summing up suggestions set such each vertex suggests the closet codeword to his local view. Namely, for each $v \in V$ define:

$$\begin{aligned} c_v &\leftarrow \arg_{\tilde{c} \in C_0} \min d(x|_v, \tilde{c}) \quad \forall v \in V \\ x^\oplus &\leftarrow \sum_{v \in V} c_v \end{aligned}$$

We will think about x^\oplus as the disagreement between the vertices over x .

Lemma. Linearity Of The Disagreement. Consider the code $C = \mathcal{T}(G, C_0)$. Let $x \in \mathbb{F}_2^E$ then for any $y \in C$ it holds that:

$$(x + y)^\oplus = (x)^\oplus$$

Proof. Having that $y \in C$ follows $y|_v \in C_0$ and therefore $\arg_{\tilde{c} \in C_0} \min d(z, \tilde{c}) = y|_v + \arg_{\tilde{c} \in C_0} \min d(z, \tilde{c} + y|_v)$, Hence the suggestion made by vertex v is:

$$\begin{aligned} c_v &\leftarrow \arg_{\tilde{c} \in C_0} \min d((x + y)|_v, \tilde{c}) \\ &\leftarrow y|_v + \arg_{\tilde{c} \in C_0} \min d((x + y)|_v, \tilde{c} + y|_v) \\ &\leftarrow y|_v + \arg_{\tilde{c} \in C_0} \min d(x|_v, \tilde{c}) \end{aligned}$$

It follows that:

$$\begin{aligned} (x + y)^\oplus &= \sum_{v \in V} c_v = \sum_{v \in V} y|_v + \sum_{v \in V} \arg_{\tilde{c} \in C_0} \min d(x|_v, \tilde{c}) \\ &= y^\oplus + x^\oplus = x^\oplus \end{aligned}$$

When the last transition follows immediately by the fact that $y \in C$ and therefore any pair of connected vertices contribute the same value for their associated edge \square

Definition. Let $C = \mathcal{T}(G, C_0)$. We say that $x \in C_\oplus$ is *reducible* if there exists a vertex v and a small codeword c_v , for which, adding the assignment of c_v over the v 's edges to x decreases the weight. Namely, $|x + c_v| < |x|$. If $x \in C_\oplus$ is not a reducible codeword then we say that x is *irreducible*.

Theorem 1. There exist a constant $\alpha > 0$ and an infinite family of Tanner Codes $C = \mathcal{T}(G, C_0)$ such that any irreducible codeword x of a corresponding disagreement code $x \in C_\oplus$ at length n , weight at least αn .

Proof. By induction over the number of vertices $V' \subset V$, which suggest a nontrivial codeword to x . Base, assume that a single vertex $v \in V$ suggests a nontrivial codeword $c_v \in C_0$. Then it's clear that $x = c_v$. And therefore, we have that $|x + c_v| = 0 < |x|$.

Assume the correctness of the argument for every codeword defined by at most m nontrivial suggestions made by $V' \subset V$. And consider the graph (V', E') induced by them. If the graph has more than a single connectivity component, then any of them is also a codeword of C_\oplus but composed of at most $m - 1$ nontrivial suggestions. Therefore, by the assumption, we could find a vertex v and a proper small codeword $c_v \in C_0$, such that the addition of the suggestion will decrease the weight of the codeword defined on that component and therefore decrease the total weight of x .

So, we can assume that the vertices in V' compose a single connectivity component. Let be $x|_v \in \mathbb{F}_2^\Delta$ the bits of x on the indices corresponding to v 's edges. If there is any v , with suggestion c_v , such that $\frac{1}{2}w(c_v) < w(x|_v)$, then we could pick to turn on c_v again and have that:

$$\begin{aligned} |x + c_v| &= |x|_v + x_v + c_v| = |x|_v| + w(c_v) + w(x|_v) \\ &< |x|_v| + \frac{1}{2}w(c_v) \leq |x|_v| + w(x|_v) = |x| \end{aligned}$$

Hence it is left to consider the case that for any $v \in V'$, it holds that $\frac{1}{2}w(c_v) > w(x|_v)$ (Notice that if they equal, then by turn on c_v , we back again to codeword made by $m - 1$ nontrivial suggestions). We will prove that this case is possible only for codewords with wight at least $\alpha|E|^{1-\epsilon}$.

For any $S \subset E$, define $w_S(x)$ as the weight that x induces over S . And notice that any edge of E connected only to a single vertex in V' equals the corresponding bit in the original suggestion made by c_v . Hence for every $v \in V'$, it holds that $w_{E/E'}(x|_v) = w_{E/E'}(c_v)$.

Claim. For any $v \in V'$ and corresponded suggestion c_v it holds that: $w_{E'}(c_v) \geq \frac{1}{2}\delta_0\Delta$.

Proof: By using the previews insight we get:

$$\begin{aligned} w_{E'}(c_v) &= w(c_v) - w_{E/E'}(c_v) = w(c_v) - w_{E/E'}(x|_v) \\ &\geq w(c_v) - w(x|_v) \geq \frac{1}{2}w(c_v) = \frac{1}{2}\delta_0\Delta \end{aligned}$$

□

Consider an arbitrary vertex $r \in V'$, and consider the DAG obtained by the BFS walk over the subgraph (V', E') starting at r . Denote this directed tree by T .

Claim. The size of T is at least:

$$|T| \geq \left(\frac{1}{4}\delta_0 - \frac{\lambda}{\Delta} \right) n$$

Proof: By the fact that for any $v \in T$ the degree of v is at least $\frac{1}{2}\delta_0\Delta$ we have that: $E(T, T) \geq \frac{1}{2} \cdot \frac{1}{2}\delta_0\Delta|T|$. Combine the Mixing Expander Lemma we obtain:

$$\begin{aligned} \frac{1}{4}\delta_0\Delta|T| &\leq \frac{\Delta}{n}|T|^2 + \lambda|T| \\ \Rightarrow \left(\frac{\Delta}{n}|T| + \lambda - \frac{1}{4}\delta_0\Delta \right) |T| &\geq 0 \\ \Rightarrow |T| &\geq \left(\frac{1}{4}\delta_0 - \frac{\lambda}{\Delta} \right) n \end{aligned}$$

□

Claim. Suppose that G is an expander graph with a second eigenvalue λ , then For any layer U there exist a layer U' such that:

$$\begin{aligned} (1) \quad &|U'| \geq |U| \\ (2) \quad &w_{E/E'}(x|_{U'}) \geq \Delta|U'| \left(\delta_0 - \frac{2}{3} - \frac{2\lambda}{\Delta} \right) \end{aligned}$$

Proof: Consider layer U and denote by U_{-1} and U_{+1} the preceding and the following layers to U in T . It follows from the expander mixing lemma that:

$$\begin{aligned} w_{E/E'}(x|_U) &\geq \delta_0\Delta|U| - w\left(E(U_{-1} \cup U_{+1}, U)\right) \geq \\ &\delta_0\Delta|U| - \left(E(U_{-1} \cup U_{+1}, U)\right) \\ &\delta_0\Delta|U| - \Delta \frac{|U||U_{-1}|}{n} - \Delta \frac{|U||U_{+1}|}{n} \\ &- \lambda\sqrt{|U||U_{-1}|} - \lambda\sqrt{|U||U_{+1}|} \end{aligned}$$

Claim. We can assume that $|U| \geq |U_{-1}|, |U_{+1}|$.

Proof: Suppose that $|U_{+1}| > |U|$, so we could choose U to be U_{+1} . Continuing stepping deeper till we have that $|U| > |U_{+1}|, |U_{-1}|$. Similarly, if $|U| > |U_{+1}|$ but $|U_{-1}| > |U|$, then we could take steps upward by replacing U_{-1} with U . At the end of the process, we will be left with U at a size greater than the initial layer and $|U| > |U_{+1}|, |U_{-1}|$ \square

Using the the claim, we have that $(|U_{+1}| + |U_{-1}|) / n < \frac{2}{3}$ and therefore:

$$w_{E/E'}(x|_U) \geq \left(\delta_0 - \frac{2}{3} - \frac{2\lambda}{\Delta} \right) \Delta |U| \quad \square$$

That immediately yields the following: let $U_{\max} = \arg \max_{U \text{ layer in } T} |U|$ then:

$$|x| \geq w_{E/E'}(x|_{U_{\max}}) \geq \left(\delta_0 - \frac{2}{3} - \frac{2\lambda}{\Delta} \right) \Delta |U_{\max}|$$

Claim. Consider again the maximal layer U_{\max} then:

$$w_{E/E'}(x) \geq \left(\delta_0 - \frac{|U_{\max}|}{n} - \frac{\lambda}{\Delta} \right) \Delta |T|$$

Proof. Similarly to above, now we will bound the weight that all the nodes in T induce over E/E' . Denote by $U_0, U_1 \dots U_m$ the layers of T ordered corresponded to their height, thus we obtain:

$$\begin{aligned} w_{E/E'}(x) &\geq \delta_0 \Delta |T| - \sum_{i \in [m]} w(E(U_i, U_{i+1})) \\ &\geq \delta_0 \Delta |T| - \sum_{i \in [m]} E(U_i, U_{i+1}) \\ &\geq \delta_0 \Delta |T| - \sum_{i \in [m]} \frac{\Delta}{n} |U_i| |U_{i+1}| + \lambda \sqrt{|U_i| |U_{i+1}|} \\ &\geq \delta_0 \Delta |T| - \sum_{i \in [m]} \frac{\Delta}{n} |U_i| |U_{i+1}| + \lambda \frac{|U_i| + |U_{i+1}|}{2} \\ &\geq \delta_0 \Delta |T| - \frac{\Delta}{n} |T| |U_{\max}| - \lambda |T| \\ &\geq \left(\delta_0 - \frac{|U_{\max}|}{n} - \frac{\lambda}{\Delta} \right) \Delta |T| \end{aligned}$$

\square

Proof of Theorem 1. Consider the size of the maxiaml layer $|U_{\max}|$ and sepearte to the following two cases. First, consider the case that $|U_{\max}| \geq \alpha n$ in that case it follows immedily that if $\delta_0 > \frac{2}{3} - \frac{2\lambda}{\Delta}$ there exists $\alpha' > 0$ such that:

$$|x| \geq \left(\delta_0 - \frac{2}{3} - \frac{2}{\lambda} \Delta \right) \Delta |U_{\max}| \geq \alpha' n$$

So, it is lefts to consider the second case in which $|U_{\max}| < \alpha n$ in that case, we have from the second inequality that:

$$\begin{aligned} |x| &\geq w_{E/E'}(x) \geq \left(\delta_0 - \frac{|U_{\max}|}{n} - \frac{\lambda}{\Delta} \right) \Delta |T| \\ &\geq \left(\delta_0 - \alpha - \frac{\lambda}{\Delta} \right) \Delta |T| \end{aligned}$$

Setting $\alpha \geq \frac{2}{3}$ we complete the proof \square

Unfortunately, Singelton bound doesn't allow both $\delta_0 > \frac{2}{3}$ and $\rho_0 \geq \frac{1}{2}$, so in total, we prove the existence of code LDPC code which is good in terms of testability and distance yet has a zero rate. In the following subsection, we will prove ([COMMENT] sec 3.4, which currently is a failure) that one can overcome this problem by requiring only half of the vertices to restrict their local view to be codewords of high relative distance.

2.2 Overcoming The Vanishing Rate.

Consider the following code; instead of associating each edge with pair of checks, let's define the vertices to be the checks of small codes over $q \in [0, 1]$ fraction of their edges. That is, now each vertex defines only $(1 - \rho_0)q\Delta$ restrictions. Hence, the rate of the code is at least:

$$\begin{aligned}\rho \frac{1}{2}\Delta n &\geq \frac{1}{2}\Delta n - (1 - \rho_0)q\Delta n \\ \Rightarrow \rho &\geq \left(2\rho_0 + \left(\frac{1}{q} - 2\right)\right)q \\ \rho_0 &\geq 1 - \frac{1}{2q}\end{aligned}$$

for example, if $q = 2/3$, then for having constant rate, it is enough to ensure that $\rho_0 \geq 1 - \frac{3}{4} = \frac{1}{4}$.

Intuition For Testability. Before expand the construction let's us justify why one should even expects that removing constraints preserves testability. Assume that is guranteed that the lower bound of the flux on the trivial vertices remains up to multiplication by the fraction factor q , or put it differently, one could just stick q in every inequality without lose correctness, Then:

$$\begin{aligned}w_{E/E'}(x|_U) &\geq \delta_0 q \Delta |U| - q w(E(U_{-1} \cup U_{+1}, U)) \\ \Rightarrow |x| &\geq \left(\delta_0 - \frac{2}{3} - \frac{2\lambda}{\Delta}\right) q \Delta |U_{\max}|\end{aligned}$$

As you can see, irreducible words of the disagreement have a linear weight, despite that the original code has non-vanish rate.

Theorem 1+. There exist a constant $\alpha > 0$ and infinite family of codes which satisfies Theroem 1 and also good.

Yet, We still require more to prove a linear distance. By repeating on the *Singleton Bound* proof it follows that the small code \tilde{C}_0 obtained by ignoring arbitrary $(q - \frac{1}{2})\Delta$ coordinates yield a code with distance:

$$\left(\delta_0 - \left(q - \frac{1}{2}\right)\right)\Delta$$

So assume that we could engineer an expander family such that the graphs obtained by removing $\frac{1}{2}$ of the edges connected for each vertex result also expanders, and in addition, regarding \tilde{C}_0 each edge is checked by both vertices on its support. Namely, a good Tanners Code could be defined on the restricted graphs; Then, any string that satisfies the original checks also has a linear weight. To achieve this property, we will restrict ourselves to a particular family of Cayley Graphs.

Definition. Testability-Tanner-Code. Let $q > \frac{1}{2}$ and let J be a generator set for group Γ such that $|J| = \Delta$, $q|\Delta$, J closed for inverse, and there exist subset of J , denote it by, J' such that J' is a generator set of Γ and $|J'| = \frac{1}{2}\Delta$. Let C_0 be a code with parameters $C_0 = q\Delta [1, \rho_0, \delta_0]$. For any vertex assoicate a subset $\bar{J}_v \subset J/J'$ at size:

$$|\bar{J}_v| = \left(q - \frac{1}{2}\right)\Delta \Rightarrow |\bar{J}_v \cup J'| = q\Delta$$

Define the code $\mathcal{T}(J, q, C_0)$ to be the subspace such that any vertex's local view over the edges defined by $\bar{J}_v \cup J'$ is a codeword of C_0 . In addition, let's associate a code \tilde{C}_v obtained for any vertex by ignoring the bits supported on the \bar{J}_v coordinates. Notice that code defined by requiring that the local view of any vertex v of $\text{Cayley}(\Gamma, J')$ is a codeword of \tilde{C}_v is a TannerCode. Denote it by $\tilde{\mathcal{T}}(J, q, C_0)$.

Lemma. Let J be defined as above such that both $\text{Cayley}(\Gamma, J)$, $\text{Cayley}(\Gamma, J')$ are expanders with algebraic expansion greater then λ and C_0 with the parameters $\rho_0 > 1 - \frac{1}{2q}$ and $\delta_0 - (q - \frac{1}{2}) > \lambda$. Then the code $\mathcal{T}(J, q, C_0)$ is a good code.

Proof. We have already proven that the code has a positive rate. Consider a codeword x and denote by x' the restriction of x to $\text{Cayley}(\Gamma, J')$ which is a codeword of $\tilde{C} = \tilde{\mathcal{T}}(J, q, C_0)$. But \tilde{C} is a Tanner Code such that any vertex sees at least $\tilde{\delta}_0\Delta := (\delta_0 - (q - \frac{1}{2}))\Delta$ nontrivial bits, Therefore as the expansion of the graph $\text{Cayley}(\Gamma, J')$ is lower than $\tilde{\delta}\Delta$ than any subset S of V at the size at most $|S|/|V| < \tilde{\delta}_0 - \lambda/\Delta$ must contain at least one vertex that sees less than $\tilde{\delta}\Delta$ nontrivial bits, In contradiction for the fact that $x' \in \tilde{C}$. \square

Claim. Existence of such *Cayley's*. Let S be a generator set such that $\text{Cayley}(\Gamma, S)$ has a second largest eigenvalue greater than λ . And consider an arbitrary group element $g \in \Gamma$ such that gSg^{-1} disjointness to S [COMMENT] remove the disjointness requirement. Denote by S_g the set gSg^{-1} . Then the second eigenvalue of the graph obtained by $(\Gamma, S) \cup (\Gamma, S)$ is at most 2λ .

Proof. Denote by G, G' the *Cayley* graphs corresponding to S, S_g , for convinient we will use the notation of $\sum_{v \sim_G u}$ to denote a summation over all the neighbors of v in the graph G . Let $A_{G'}$ be the adjacency matrix of G' . Recall that G' is a Δ regular graph, and therefore the uniform distribution $\mathbf{1}$ is the eigenstate with the maximal eigenvalue, and the second eigenvalue is given by the min-max principle:

$$\begin{aligned} \max_{f \perp \mathbf{1}} \frac{f^\top A_{G'} f}{f^\top f} &= \max_{f \perp \mathbf{1}} \sum_v \sum_{u \sim_{G'} v} \frac{f(u) f(v)}{f^\top f} \\ &= \max_{f \perp \mathbf{1}} \sum_v \sum_{\tau \in S} \frac{f(g\tau g^{-1}v) f(v)}{f^\top f} \\ &= \max_{f \perp \mathbf{1}} \sum_{gv} \sum_{\tau \in S} \frac{f(g\tau g^{-1}gv) f(gv)}{f^\top f} \\ &= \max_{f \perp \mathbf{1}} \sum_{gv} \sum_{\tau \in S} \frac{f(g\tau v) f(gv)}{f^\top f} \\ &= \max_{f \perp \mathbf{1}} \sum_{gv} \sum_{u \sim_{G'} v} \frac{f(gu) f(gv)}{f^\top f} \end{aligned}$$

As for any function $f : V \rightarrow \mathbb{R}$ one could define a function $f' : E \rightarrow \mathbb{R}$ such that $f'(v) = f(v)$ and f' preserves the norm:

$$\begin{aligned} f'^\top f' &= \sum_{v \in V} f'(v) f'(v) = \sum_{v \in V} f^\top(vg) f(vg) = f^\top f \\ \Rightarrow \max_{f \perp \mathbf{1}} \frac{f^\top A_{G'} f}{f^\top f} &= \max_{f \perp \mathbf{1}} \sum_{gv} \sum_{u \sim_{G'} v} \frac{f(gu) f(vg)}{f^\top f} \end{aligned}$$

By the Interlacing Theorem, [Hae95] the second eigenvalue of any subgraph of G' is less than the λ' . In particular, the eigenvalue of the graph obtained by taking the edges that are associated with elements of the S_g/S , denote that subgraph by $G'_{/S}$. Because $S_g/S \cap S = \emptyset$, we have that the edges sets of G, G' are disjointness sets. Hence the adjacency matrix of the graphs union equals the sum of their adjacency matrices. So in total, we obtain that:

$$\begin{aligned} \lambda' &= \max_{f \perp \mathbf{1}} \frac{f^\top (A_G + A_{G'_{/S}}) f}{f^\top f} \\ &\leq \max_{f \perp \mathbf{1}} \frac{f^\top A_G f}{f^\top f} + \max_{f \perp \mathbf{1}} \frac{f^\top A_{G'_{/S}} f}{f^\top f} \\ &\leq \lambda + \lambda = 2\lambda \end{aligned}$$

□

Claim. If Δ is a constant greater than two, and G is a λ -algebraic expander with girth at length $\Omega(\log n)$, then it there exists a $g \in \Gamma$ such that $S_g \cap S = \emptyset$.

Proof. As $\Delta > 2$ there must be at least two different elements $s_1, s_2 \in S$ such that $s_1 \neq s_2, s_2^{-1}$. Pick $g = s_1 s_2$. Now assume through contradiction that there also exists $s, t \in S$ such that $gsg^{-1} = r \Rightarrow gs = rg$ and notice that the fact that $s_1 \neq s_2^{-1}$ guarantees that both terms are a product of 3 element group. Therefore either that there is a 6-length cycle in the graph, Or that there is element-wise equivalence, namely $s_1 = r, s_2 = s_1, s = s_2$. The first case contradict the lower bound on the expander girth, which is at least $\Omega(\log_\Delta(n))$, while the other stand in contradiction to the fact that $s_1 \neq s_2$ □

Remark. Regarding Quantum Codes. Notice that any complex designed to hold CSS qLDPC codes must have constant length cycles. Otherwise, the distance of C_x will not be constant, and therefore the condition $H_x H_z^\top = 0$ could be satisfied only if H_z is not a constant row-weight matrix, Put differently C_z is not an LDPC code. Consequently, any trial to generalize the construction for obtaining quantum codes must not rely on that claim.

Remark. Note On Random Construction. One might wonder if using *Cayley* is necessary. We conjecture that there is a constant $c > 0$ such that sampling pair of $(1+c) \frac{1}{2}\Delta$ regular random graphs, and then take the anti-symmetry union of them might also obtain a good expander such that each of the residue part also has good expansion with high probability.

Lemma. [COMMENT] Rewrite. Consider the graph G as defined above (direct subset of *Cayley* graph) and let S, T be subsets of the vertices. Then the flux of S over T is at most:

$$E_{G'}(S, T) \leq \frac{1}{2}\Delta \frac{|S||T|}{n} + \lambda\sqrt{|S||T|}$$

Proof. The only edges that can interfere are the edge defined by J' . Therefore it's enough to use the mixing expander lemma on the $\frac{1}{2}\Delta$ -regular graph. \square

Proof of Theorem 1+. Notice that $\frac{1}{2} < \frac{2}{3} = q$, Thus repeating exactly over proof above obtains that:

$$w_{E/E'}(x|_{U_{\max}}) \geq \left(\delta_0 - \frac{2}{3} - \frac{1}{q} \frac{2\lambda}{\Delta} \right) q\Delta |U_{\max}|$$

Choosing J such that $\text{Cayley}(\Gamma, J)$ is Ramanujan provides that $\frac{2\lambda}{\Delta q}$ scales as $\Theta\left(\frac{1}{\sqrt{\Delta}}\right)$. That closes the case in which there is a linear size layer of nontrivial suggestions. In other case, in which any such layer is at size less than $\alpha'n$ ($\alpha' = (\delta_0 - (q - \frac{1}{2}))$?) then we obtain the testability for free \square

3 Good Quantum Codes, logarithmic-check-weight.

In the following section we will construct a family of complexes on which we will define a pair of Tanner Codes, eventually, they will be used to compose a CSS pair of good quantum codes.

Infinite Family Of Tanner Quantum Codes. Let p be a prime and $\delta \in (0, 1)$. Consider the Cayley graphs obtained by taking uniformly a $c(\delta) \log n$ generators of the cyclic group at order p , denote that set by S . It was shown by N. Alon [COMMENT] cite Noga that with high probability that process yields a Graph with δ -algebraic expansion. Now, consider the double cover of that graph and denote it by $G = (V = V^+ \cup V^-, E)$. And define the following graph denoted by $\Gamma^\pm = (V^\pm, E')$:

$$((u, \pm), (v, \pm)) \in E' \Leftrightarrow \exists a \neq b \in S \text{ s.t. } abu = v$$

4 Decoding and Testing

For completeness, we show exactly how Theorem 1 implies testability. The following section repeats Levenshtein's and Zemor's proof [LZ22]. Consider a binary string x that is not a codeword. The main idea is the observation that the number of bits flipped by (any) decoder, while decoding x , bounds the distance $d(x, C)$ from above. In addition, the number of positive checks in the first iteration is exactly the number of violated restrictions.

Definition. Let $L = \{L_i\}_0^{2|E|}$ be a series of $2|E|$. Such that for each vertex $v \in V$ $\sum_{e=\{u,v\}} L_{e_v} \in C_0$. We will call L a *Potential list* and refer to the e_v 's as the element of L as a suggestion made by the vertex $v \in V$ for the edge $e \in E$. Sometimes we will use the notation L_v to denote all the L 's coordinates of the form $L_{e_v} \forall e \in \text{Support}(v)$. Define the *Force* of L to be the following sum $F(L) = \sum_{e=\{v,u\} \in E} (L_{e_v} + L_{e_u})$ and notice that $F(L) \in C_\oplus$. And define the *state* $S(L) \subset \mathbb{F}_2^{|E|}$ of L as the vector obtained by choosing an arbitrary value from $\{L_{e_v}, L_{e_u}\}$ for each edge $e \in E$.

Claim. Let L be the Potential list. If $F(L) = 0$ then $S(L) \in C$.

Proof. Denote by $\phi(e) \subset \{L_{e_v}, L_{e_u}\}$ the value which was chosen to $e = \{v, u\} \in E$. By $F(L) = 0$, it follows that $L_{e_v} + L_{e_u} = 0 \Rightarrow L_{e_v} = L_{e_u} = \phi(e)$ for any $e \in E$. Hence for every $v \in V$ we have that $S(L)|_v = \sum_{u \sim v} \phi(\{v, u\}) = \sum_{u \sim v} L_{e_v} \in C_0 \Rightarrow S(L) \in C$.

The decoding goes as follows. First, each vertex suggests the closest C_0 's codeword to his local view. Those suggestions define a Potential list, denote it by L , then if $F(L) < \tau$, by Theorem 1, one could find a suggestion of vertex v and a codeword c_v such that updating the value of $L_v \leftarrow L_v + c_v$ yields a Potential list with lower force. Therefore repeating the process till the force vanishes, obtain a Potential list in which its state is a codeword.

Definition. Let $\tau > 0, f : \mathbb{N} \rightarrow \mathbb{R}^+$, and consider a Tanner Code $C = \mathcal{T}(G, C_0)$. Let us Define the following decoder and denote it by \mathcal{D} .

Algorithm 1: Decoding

Data: $x \in \mathbb{F}_2^n$
Result: $\arg \min \{y \in C : |y + x|\}$ if $d(y, C) < \tau$ and False otherwise.
1 $L \leftarrow \text{Array}\{\}$
2 **for** $v \in V$ **do**
3 $c'_v \leftarrow \arg \min \{y \in C_0 : |y + x|_v|\}$
4 $L_v \leftarrow c'_v$
5 **end**
6 $z \leftarrow \sum_{v \in V} c'_v$
7 **if** $|z| < \tau \frac{n}{f(n)}$ **then**
8 **while** $|z| > 0$ **do**
9 find v and $c \in C_0$ such that $|z + c_v| < |z|$
10 $z \leftarrow z + c_v$
11 $L_v \leftarrow L_v + c_v$
12 **end**
13 **else**
14 reject.
15 **end**
16 **return** $S(L)$

Theorem. Consider a Tanner Code $C = [n, n\rho, n\delta]$ and the disagreement code C_\oplus defined by it. Suppose that for every codeword $z \in C_\oplus$ in C_\oplus such that $|z| < \tau'n/f(n)$, there exists another codeword $y \in C_\oplus$ such that $|y| < |z|$, set $\tau \leftarrow \frac{\tau'}{6\Delta}\delta$ then,

1. \mathcal{D} corrects any error at a weight less than $\tau n/f(n)$.
2. C is $f(n)$ testable code.

Proof. So it is clear from the claim above that if the condition at line (6) is satisfied, then \mathcal{D} will converge into some codeword in C . Hence, to complete the first section, it left to show that \mathcal{D} returns the closest codeword. Denote by e the error, and by simple counting arguments; we have that \mathcal{D} flips at most:

$$d_{\mathcal{D}}(x, C) \leq 2|e|\Delta + \tau \frac{n}{f(n)}\Delta$$

bits. Hence, by the assumption,

$$d_{\mathcal{D}}(x, C) \leq 3\Delta\tau \frac{n}{f(n)} \leq 3\Delta\tau\delta n < \frac{1}{2}\delta n$$

Therefore the code word returned by \mathcal{D} must be the closet. Otherwise, it contradicts the fact that the relative distance of the code is δ . To obtain the correctness of the second section, we will separate when the conditional at the line (5) holds and not. And prove that the testability inequality holds in both cases. Let $x \in \mathbb{F}_2^n$ and consider the running of \mathcal{D} over x . Assume the first case, in which the conditional at line (5) is satisfied. In that case, \mathcal{D} decodes x into its closest codeword in C . Therefore:

$$\begin{aligned} d(x, C) &\leq d_D(x, C) \leq m\xi(x)\Delta + |z|\Delta \\ &\leq m\xi(x)\Delta + m\xi(x)\Delta^2 \\ \frac{d(x, C)}{n} &\leq \kappa_1\xi(x) \end{aligned}$$

Now, consider the other case in which: $|z| \geq \tau \frac{n}{f(n)}$.

$$\begin{aligned} \frac{d(x, C)}{n} &\leq 1 \leq \frac{|z|}{\tau n} f(n) \leq \frac{m}{n} \frac{1}{\tau} \Delta \xi(x) f(n) \\ &\leq \kappa_2 \xi(x) f(n) \end{aligned}$$

Picking $\kappa \leftarrow \max\{\kappa_1, \kappa_2\}$ proves $f(n)$ -testability \square

References

- [Hae95] Willem H. Haemers. “Interlacing eigenvalues and graphs”. In: *Linear Algebra and its Applications* 226-228 (1995). Honoring J.J.Seidel, pp. 593–616. ISSN: 0024-3795. DOI: [https://doi.org/10.1016/0024-3795\(95\)00199-2](https://doi.org/10.1016/0024-3795(95)00199-2). URL: <https://www.sciencedirect.com/science/article/pii/0024379595001992>.
- [PK21] Pavel Panteleev and Gleb Kalachev. *Asymptotically Good Quantum and Locally Testable Classical LDPC Codes*. 2021. DOI: 10.48550/ARXIV.2111.03654. URL: <https://arxiv.org/abs/2111.03654>.
- [Din+22] Irit Dinur et al. *Good Locally Testable Codes*. 2022. DOI: 10.48550/ARXIV.2207.11929. URL: <https://arxiv.org/abs/2207.11929>.
- [LZ22] Anthony Leverrier and Gilles Zémor. *Quantum Tanner codes*. 2022. arXiv: 2202.13641 [quant-ph].