

# From classical to good quantum LDPC codes.

---

D. Ponnarovsky<sup>1</sup>

Master-Exam-Huji.

Faculty of Computer Science  
Hebrew University of Jerusalem

# Today.

- Brif Review of Coding.

# Today.

- Brif Review of Coding. Tanner and Expander codes.

# Today.

- Brief Review of Coding. Tanner and Expander codes.
- Quantum Error Correction Codes.

# Today.

- Brief Review of Coding. Tanner and Expander codes.
- Quantum Error Correction Codes.
- Good Classical Locally Testable Codes and Good Quantum LDPC.

Future.

"We understand quantum complexity".

Future.

"We understand quantum complexity".

Future.

"We understand quantum complexity".

BQP (P) ? QMA (NP) ? PSPACE.



Future.

"We understand quantum complexity.  
as well as we understand classical complexity".

$BQP(P) ? QMA(NP) ? PSPACE$ .

Future.

"We understand quantum complexity.  
as well as we understand classical complexity".

QMA ? qPCP

Future.

"We understand quantum complexity.  
as well as we understand classical complexity".

QMA ? qPCP

Future.

"We understand quantum complexity.  
as well as we understand classical complexity".

QMA ? qPCP



22-23

Future.

"We understand quantum complexity.  
as well as we understand classical complexity".

QMA ? qPCP

↓

NLTS  
Hamiltonians  
from good  
→  
qLDPC codes [ABN22]

Existence of family of statements and quantum proofs,  
such that any slightly noisy version of the proofs  
is still a proof and cannot be yielded by  
'weak' computations.

21-22

22-23

Future.

"We understand quantum complexity.  
as well as we understand classical complexity".

QMA ? qPCP

↓

Existence of family of statements and quantum proofs,  
such that any slightly noisy version of the proofs  
is still a proof and cannot be yielded by  
'weak' computations.

NLTS

Hamiltonians  
from good

qLDPC codes [ABN22]

good qLDPC →  
[Din+22], [PK21], [LZ22]

→

# Introduction.

The work assumes only a basic knowledge of linear algebra and combinatorics. So we believe that every computer science graduate will be able to enjoy reading it, understand the subject very well, and use it as a gateway for starting research in the field.

Bob is willing to send some message to Alice through





Bob is willing to send some message to Alice through a noisy channel in which bits might be flipped.



Bob is willing to send some message to Alice through a noisy channel in which bits might be flipped. By sending extra bits, i.e. duplicate any bit three times, B can ensure that A could still decode the original message in the presence of a single bit-flip.



Bob is willing to send some **state** to Alice through a noisy channel in which bits might be flipped. By sending extra bits, i.e duplicate any bit tree times, B can ensure that A could still decode the original **state** in the presence of a single bit-flip.



Bob is willing to send some **state** to Alice through a noisy channel in which bits might be flipped. By sending extra bits, i.e duplicate any bit three times, B can ensure that A could still decode the original **state** in the presence of a single bit-flip.



C



$$d(C) = \min_{x, y \in C} d(x, y)$$

Non formally, We call for the embedding of entities in a larger space a code. And the questions that we would like to ask are:

- Can we come up with a code that tolerates  $\epsilon$  bits flip?

Non formally, We call for the embedding of entities in a larger space a code. And the questions that we would like to ask are:

- Can we come up with a code that tolerates  $\epsilon$  bits flip?
- At the cost of at most  $\epsilon$  extra bits?

Non formally, We call for the embedding of entities in a larger space a code. And the questions that we would like to ask are:

- Can we come up with a code that tolerates  $\epsilon$  bits flip?
- At the cost of at most  $\epsilon$  extra bits?
- Can we ensure an efficient decoding (and checking) scheme?



Non formally, We call for the embedding of entities in a larger space a code. And the questions that we would like to ask are:

- Can we come up with a code that tolerates  $\epsilon$  bits flip?
- At the cost of at most  $\epsilon$  extra bits?
- Can we ensure an efficient decoding (and checking) scheme?
- In the asymptotic regime, when the size of the original message grows.

## Definition

Let  $n \in \mathbb{N}$  and  $\rho, \delta \in (0, 1)$ . We say that  $C$  is a **binary linear code** with parameters  $[n, \rho n, \delta n]$ . If  $C$  is a subspace of  $\mathbb{F}_2^n$ , and the dimension of  $C$  is at least  $\rho n$  and any pair of distinct elements in  $C$  differ in at least  $\delta n$  coordinates. We call to the vectors belong to  $C$  *codewords*, to  $\rho n$  the dimension of the code, and to  $\delta n$  the distance of the code.

## Definition

A **family of codes** is an infinite series of codes. Additionally, suppose the rates and relative distances converge into constant values  $\rho, \delta$ . In that case, we abuse the notation and call that family of codes a code with  $[n, \rho n, \delta n]$  for fixed  $\rho, \delta \in [0, 1)$ , and infinite integers  $n \in \mathbb{N}$ .

## Definition

We will say that a family of codes is a **good code** if its parameters converge into positive values.

## Definition

Let  $\Gamma$  be a graph and  $C_0$  be a “small” linear code with finite parameters  $[\Delta, \rho\Delta, \delta\Delta]$ . Let  $C = \mathcal{T}(\Gamma, C_0)$  be all the codewords which, for any vertex  $v \in \Gamma$ , the local view of  $v$  is a codeword of  $C_0$ . We say that  $C$  is a **Tanner code** of  $\Gamma, C_0$ . Notice that if  $C_0$  is a binary linear code, So  $C$  is.

## Coding.

Another example, the repetition code can be thought as the tanner graph defined by the parity code on the cycle graph.



parity check matrix of  $C_0$

$$\begin{bmatrix} 1 & 1 \end{bmatrix}$$

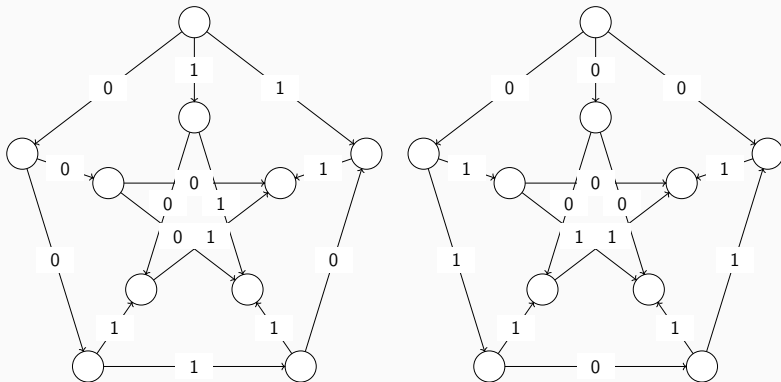


Parity check matrix of  $\mathcal{T}(\Gamma, C_0)$   
Each row associated with vertex check.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

# Tanner Codes.

Example, the parity code on the Peterson graph.



### Lemma

*Tanner codes have a rate of at least  $2\rho - 1$ .*

## Lemma

*Tanner codes have a rate of at least  $2\rho - 1$ .*

## Proof.

The dimension of the subspace is bounded by the dimension of the container minus the number of restrictions. So assuming non-degeneration of the small code restrictions, we have that any vertex count exactly  $(1 - \rho) \Delta$  restrictions. Hence,

$$\dim C \geq \frac{1}{2}n\Delta - (1 - \rho) \Delta n = \frac{1}{2}n\Delta (2\rho - 1)$$

Clearly, any small code with rate  $> \frac{1}{2}$  will yield a code with an asymptotically positive rate □



Note, that if the  $\Gamma$  is a family of  $\Delta$ -regular graphs then, the size (length, dim, and dis) of  $C_0$  is  $O(1)$  as  $n$  grows and the hamming weight of any row in the parity check matrix of  $\mathcal{T}(\Gamma, C_0)$  is finite. We say that a family of codes with a parity check matrices having a constant row weight is a Low Density Parity Check code (LDPC). LDPC can be viewed as the first local property and also has practical value as it implies a linear time algorithm for correctness verification.

## Definition

Denote by  $\lambda$  the second eigenvalue of the adjacency matrix of the  $\Delta$ -regular graph. For our uses, it will be satisfied to define expander as a graph  $G = (V, E)$  such that for any two subsets of vertices  $T, S \subset V$ , the number of edges between  $S$  and  $T$  is at most:

$$|E(S, T) - \frac{\Delta}{n}|S||T|| \leq \lambda \sqrt{|S||T|}$$

## Lemma

*Theorem, let  $C$  be the Tanner Code defined by the small code  $C_0 = [\Delta, \delta\Delta, \rho\Delta]$  such that  $\rho \geq \frac{1}{2}$  and the expander graph  $G$  such that  $\delta\Delta \geq \lambda$ .  $C$  is a good LDPC code.*

## Lemma

*Theorem, let  $C$  be the Tanner Code defined by the small code  $C_0 = [\Delta, \delta\Delta, \rho\Delta]$  such that  $\rho \geq \frac{1}{2}$  and the expander graph  $G$  such that  $\delta\Delta \geq \lambda$ .  $C$  is a good LDPC code.*

## Proof.

Fix a codeword  $x \in C$  and denote By  $S$  the support of  $x$  over the edges. Namely, a vertex  $v \in V$  belongs to  $S$  if it connects to nonzero edges regarding the assignment by  $x$ , Assume towards contradiction that  $|x| = o(n)$ . And notice that  $|S|$  is at most  $2|x|$ , Then by The Expander Mixing Lemma we have that:

$$\begin{aligned} \frac{E(S, S)}{|S|} &\leq \frac{\Delta}{n}|S| + \lambda \\ &\leq_{n \rightarrow \infty} o(1) + \lambda \end{aligned}$$



## Proof.

$$\begin{aligned}\frac{E(S, S)}{|S|} &\leq \frac{\Delta}{n}|S| + \lambda \\ &\leq_{n \rightarrow \infty} o(1) + \lambda\end{aligned}$$

Namely, for any such sublinear weight string,  $x$ , the average of nontrivial edges for the vertex is less than  $\lambda$ . So there must be at least one vertex  $v \in S$  that, on his local view, sets a string at a weight less than  $\lambda$ . By the definition of  $S$ , this string cannot be trivial. Combining the fact that any nontrivial codeword of the  $C_0$  is at weight at least  $\delta\Delta$ , we get a contradiction to the assumption that  $v$  is satisfied, videlicet,  $x$  can't be a codeword □

## Quantum In Our Presentation.

For presenting as simple as possible, we will refer to quantum state  $|\psi\rangle$  as a linear combination of classical states with  $\pm 1$  coefficients scaled by a normalization factor such the  $l_2$  is 1. For example, let  $|11\rangle$ ,  $|00\rangle$  and  $|01\rangle$  be classical states, then  $\frac{1}{\sqrt{3}}(|11\rangle + |00\rangle - |01\rangle)$  is a quantum state.

## Quantum In Our Presentation.

For presenting as simple as possible, we will refer to quantum state  $|\psi\rangle$  as a linear combination of classical states with  $\pm 1$  coefficients scaled by a normalization factor such that the  $l_2$  norm is 1. For example, let  $|11\rangle$ ,  $|00\rangle$  and  $|01\rangle$  be classical states, then  $\frac{1}{\sqrt{3}}(|11\rangle + |00\rangle - |01\rangle)$  is a quantum state.

1. bit flip  $X|0\rangle \rightarrow |1\rangle$ ,  $X|1\rangle \rightarrow |0\rangle$

## Quantum In Our Presentation.

For presenting as simple as possible, we will refer to quantum state  $|\psi\rangle$  as a linear combination of classical states with  $\pm 1$  coefficients scaled by a normalization factor such that the  $l_2$  norm is 1. For example, let  $|11\rangle$ ,  $|00\rangle$  and  $|01\rangle$  be classical states, then  $\frac{1}{\sqrt{3}}(|11\rangle + |00\rangle - |01\rangle)$  is a quantum state.

1. bit flip  $X|0\rangle \rightarrow |1\rangle$ ,  $X|1\rangle \rightarrow |0\rangle$
2. phase flip  $Z|0\rangle \rightarrow |0\rangle$ ,  $Z|1\rangle \rightarrow -|1\rangle$



# Quantum Error Correction Codes.

Observation,  $|0\rangle$  and  $|1\rangle$  can't both encoded to a single ket codeword.

The clouds perspective.

## Definition (CSS Code)

Let  $C_X, C_Z$  classical linear codes such that  $C_Z^\perp \subset C_X$  define the  $Q(C_X, C_Z)$  to be all the codewords with following structure:

$$|x\rangle := |x + C_Z^\perp\rangle = \frac{1}{\sqrt{|C_Z^\perp|}} \sum_{z \in C_Z^\perp} |x + z\rangle$$

## Quantum Error Correction Codes.

Observation,  $C_X, C_Z$  can't be both good codes and qLDPC codes.

Furthermore, if one is willing to has an qLDPC code, then  $H_X$  and  $H_Z$  can't be parity check matrices of good classical code as any column of  $H_Z^T$  is a codeword of  $C_X$ .

$$C_Z^\perp \subset C_X \Rightarrow H_X H_Z^T = 0$$

And by being an LDPC code, the rows wights of  $H_Z$  is bounded by constant. Therefore there is a codeword  $\in C_X$  which is also a row of  $H_Z$  that has a constant weight.

Observation, setting a small quantum code on a graph, in similar manner to tanner code construction doesn't give a CSS code. two adjoint vertices define checks that intersect in exactly one coordinate.

# Quantum Error Correction Codes.



## Definition ( $w$ -Robustness)

Let  $C_A$  and  $C_B$  be codes of length  $\Delta$  with minimum distance  $\delta_0\Delta$ .

$C = (C_A^\perp \otimes C_B^\perp)^\perp$  will be said to be  $w$ -robust if for any codeword  $c \in C$  of weight less than  $w$ , it follows that  $c$  can be decomposed into a sum of  $c = t + s$  such that  $t \in C_A \otimes \mathbb{F}^B$  and  $s \in \mathbb{F}^A \otimes C_B$ , where  $s$  and  $t$  are each supported on at most  $\frac{w}{\delta_0\Delta}$  rows and columns. For convenience, we will denote by  $B'$  ( $A'$ ) the rows (columns) supporting  $t$  ( $s$ ) and use the notation  $t \in C_A \otimes \mathbb{F}^{B'}$ .

## Quantum Error Correction Codes.

$$c \in \underbrace{(C_A^\perp \otimes C_B^\perp)} = \underbrace{t \in C_A \otimes \mathbb{F}^B} + \underbrace{s \in \mathbb{F}^A \otimes C_B}$$





# Quantum Error Correction Codes.



## Definition ( $p$ -Resistance to Puncturing.)

Let  $p, w$  be integers. We will say that the dual tensor code  $C_A \otimes \mathbb{F} + \mathbb{F} \otimes C_B$  is  $w$ -robust with  $p$ -resistance to puncturing, if the code obtained by removing (puncturing) a subset of at most  $p$  rows and columns is  $w$ -robust.

## Definition (Quantum Tanner Code.)

Let  $\Gamma$  be a group of size  $n$ . And let  $A, B$  be a two generator set of  $\Gamma$  such that if  $a \in A$  ( $B$ ) then also  $a^{-1} \in A$  ( $B^{-1}$ ) and that for any  $g \in \Gamma, a \in A, b \in B$  it holds that  $g \neq agb$ . Define the left-right Cayley complex to be the graph  $G = (\Gamma, E)$  obtained by taking the union of the two Cayley graphs generated by  $A$  and  $B$ . So the vertices pair  $u, v$  are set on a square diagonal only if there are  $a \in A$  and  $b \in B$  such that  $u = avb$ . We can assume that  $G$  is a bipartite graph (otherwise just take  $\Gamma' = \Gamma \times \mathbb{Z}_2$  and define the product to be  $a(u, \pm) = (au, \mp)$ ).

## Definition (Quantum Tanner Code.)

Now divide the graph into positive and negative vertices according to their coloring  $V_-$  and  $V_+$ . And define the positive graph to be  $G^+ = (V_+, E)$  and by  $G^- = (V_-, E)$  the negative graph, where  $E$  denotes the squares, put differently there is an edge between  $v$  and  $u$  in  $G^+$  if both vertices are positive and they are laid on the ends of a square's diagonal.

The quantum Tanner code is a CSS code, such that  $C_X$  is defined to be the classical Tanner code  $\mathcal{T}\left(G^+, (C_A^\perp \otimes C_B^\perp)^\perp\right)$  and  $C_Z$  is defined as  $\mathcal{T}\left(G^-, (C_A \otimes C_B)^\perp\right)$ . Note that in contrast to the classical Tanner code, in the quantum case it will be more convenient to think of codewords as assignments set on the squares and not on the edges.

## Good Quantum LDPC Codes.

The constructions of Quantum LDPC Codes with positive relative distance and rate are attributed to Dinur, Loubozky, Evra, Mosess, Pavel, Kalachev, Leverrier and Zemor [Din+22] [PK21] [LZ22].

## Good Quantum LDPC Codes.

The constructions of Quantum LDPC Codes with positive relative distance and rate are attributed to Dinur, Loubozky, Evra, Mosess, Pavel, Kalachev, Leverrier and Zemor [Din+22] [PK21] [LZ22]. We are about to give a proof following Zemor and Leverrier version.

## Good Quantum LDPC Codes.

The constructions of Quantum LDPC Codes with positive relative distance and rate are attributed to Dinur, Loubozky, Evra, Mosess, Pavel, Kalachev, Leverrier and Zemor [Din+22] [PK21] [LZ22]. We are about to give a proof following Zemor and Leverrier version.

Yet, the proof we present is not exactly the same, as we use a small code that requires satisfying a stronger assumption (the  $w$ -robustness property 13) relative to the original work. The reason why they had to use a weaker assumption is because the existence of codes satisfying the stronger one was proven a year later [KP22]. Relying on the stronger assumption allows us to simplify the proof even more and get rid of another requirement that the small code has to satisfy (The  $p$ -resistance to puncturing 15).

## Good Quantum LDPC Codes.

Recall our insight that for a pair of LDPC codes to define a good CSS code, they must both be poor codes in the sense that they must have a constant distance. Therefore, we understand that any codeword in  $C_X$  with small weight belongs to  $C_Z^\perp$ . To prove this, we will construct a proof such that if  $x \in C_X$  and  $|x|$  is small, then there is a small codeword  $z \in C_Z^\perp$  such that  $|x + z| < |x|$ ; by repeating this process recursively, it follows that  $x \in C_Z^\perp$ . To formulate this theorem, we will need to define more definitions.

The next two definitions are concerned with the properties of the small code that will be set on the edges. Using them, one can characterize cases in which a local view can be reduced by subtracting a codeword from the dual code.



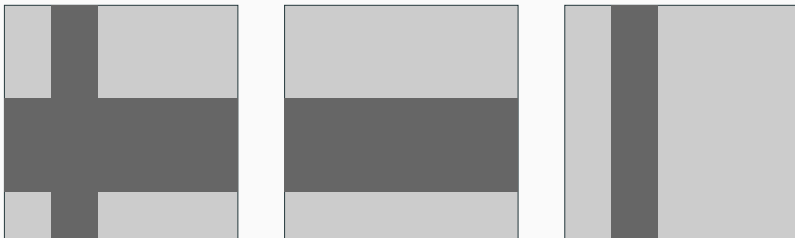
### Definition ( $w$ -Robustness)

Let  $C_A$  and  $C_B$  be codes of length  $\Delta$  with minimum distance  $\delta_0\Delta$ .

$C = (C_A^\perp \otimes C_B^\perp)^\perp$  will be said to be  $w$ -robust if for any codeword  $c \in C$  of weight less than  $w$ , it follows that  $c$  can be decomposed into a sum of  $c = t + s$  such that  $t \in C_A \otimes \mathbb{F}^B$  and  $s \in \mathbb{F}^A \otimes C_B$ , where  $s$  and  $t$  are each supported on at most  $\frac{w}{\delta_0\Delta}$  rows and columns. For convenience, we will denote by  $B'$  ( $A'$ ) the rows (columns) supporting  $t$  ( $s$ ) and use the notation  $t \in C_A \otimes \mathbb{F}^{B'}$ .

## Good Quantum LDPC Codes.

$$c \in \underbrace{(C_A^\perp \otimes C_B^\perp)^\perp}_{\text{dual tensor code}} = \underbrace{t \in C_A \otimes \mathbb{F}^B}_{\text{collection of rows}} + \underbrace{s \in \mathbb{F}^A \otimes C_B}_{\text{collection of columns}}$$



**Figure 2:**  $w$ -Robustness, Any low-weight codeword of the dual tensor code  $c$  can be decomposed into a sum  $t + s$ , where  $t$  is a collection of rows, each of which is a codeword in  $C_A$ , and similarly  $s$  is a collection of columns, each of which is a codeword of  $C_B$ .

The definition we gave for  $w$ -Robustness is identical to the one stated by Zemor and Leverrier, but we also included the decomposition property in the definition. We refer readers to the appendix section in [LZ22] for an existence proof of  $w$ -robustness codes for  $w = \Delta^{3/2-\varepsilon}$ ,  $\varepsilon > 0$ , through random construction. We note that the random construction also yields the Gilbert-Varshamov bound. Though, we need a  $w$ -robustness codes for  $\Delta^{3/2+\varepsilon}$  where  $\varepsilon$  is positive. For achieving that we use the theorem proven in [KP22]:

## Theorem

Fix  $\rho_A, \rho_B \in (0, 1)$ , and let  $\kappa$  be:

$$\kappa = \frac{1}{2} \min \left( \frac{1}{4} H_2^{-1} \left( \frac{\rho_A}{8} \right) H_2^{-1} \left( \frac{\rho_B}{8} \right), H_2^{-1} \left( \frac{\rho_A \rho_B}{8} \right) \right)$$

where  $H_2^{-1}$  denotes the inverse of the binary entropy function. Let  $C_A, C_B$  be  $\Delta$ -length and  $\rho_A \Delta, \rho_B \Delta$  codimension codes sampled uniformly at random. Then, with high probability as  $\Delta \rightarrow \infty$ , for any codeword of their dual tensor code  $c \in (C_A^\perp \otimes C_B^\perp)^\perp$ , there exists a decomposition of  $c$  into a sum of  $c = t + s$  such that  $t \in C_A \otimes \mathbb{F}^B$  and  $s \in \mathbb{F}^A \otimes C_B$ , where  $s$  and  $t$  are each supported on at most  $\frac{c}{\kappa \Delta}$  rows and columns. We call such codes  $\kappa$  product expanding.

## Good Quantum LDPC Codes.

Note that the fact that sampling succeeds with high probability implies that, with high probability, the codes that are sampled have a good distance, as well as their duals. By denoting  $\delta \leftarrow \min\{\kappa, \delta\}$ , we can say that, for any rate  $\rho$  and large enough  $\Delta$ , there exists  $\delta > 0$  such that  $(C_A^\perp \otimes C_B^\perp)^\perp$  is  $\Delta^{3/2+\varepsilon}$ -robust for  $\varepsilon < \frac{1}{2}$  and  $C_A, C_B, C_A^\perp, C_B^\perp$  have rate and relative distance of at least  $\rho$  and  $\delta$ , respectively.

### Definition ( $p$ -Resistance to Puncturing.)

Let  $p, w$  be integers. We will say that the dual tensor code  $C_A \otimes \mathbb{F} + \mathbb{F} \otimes C_B$  is  $w$ -robust with  $p$ -resistance to puncturing, if the code obtained by removing (puncturing) a subset of at most  $p$  rows and columns is  $w$ -robust.

Our proof does not utilize  $p$ -resistance to puncturing, yet it is a fundamental component in [LZ22]. Therefore, we will later indicate where and how precisely the  $p$ -resistance is being used. Now, we will define exactly what the code is.

## Good Quantum LDPC Codes.

### Definition (Quantum Tanner Code.)

Let  $\Gamma$  be a group at size  $n$ . And let  $A, B$  be a two generator set of  $\Gamma$  such that if  $a \in A$  ( $B$ ) then also  $a^{-1} \in A$  ( $B^{-1}$ ) and that for any  $g \in \Gamma, a \in A, b \in B$  it holds that  $g \neq agb$ . Define the left-right Cayley complex to be the graph  $G = (\Gamma, E)$  obtained by taking the union of the two Cayley graphs generated by  $A$  and  $B$ . So the vertices pair  $u, v$  are set on a square diagonal only if there are  $a \in A$  and  $b \in B$  such that  $u = avb$ . We can assume that  $G$  is a bipartite graph (otherwise just take  $\Gamma' = \Gamma \times \mathbb{Z}_2$  and define the product to be  $a(u, \pm) = (au, \mp)$ ).

Now divide the graph into positive and negative vertices according to their coloring  $V_-$  and  $V_+$ . And define the positive graph to be  $G^+ = (V_+, E)$  and by  $G^- = (V_-, E)$  the negative graph, where  $E$  denotes the squares, put differently there is an edge between  $v$  and  $u$  in  $G^+$  if both vertices are positive and they are laid on the ends of a square's diagonal.

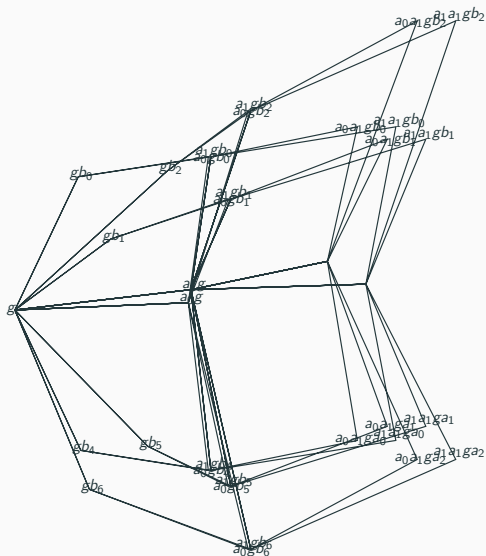
### Definition

The quantum Tanner code is a CSS code, such that  $C_X$  is defined to be the classical Tanner code  $\mathcal{T}\left(G^+, (C_A^\perp \otimes C_B^\perp)^\perp\right)$  and  $C_Z$  is defined as  $\mathcal{T}\left(G^-, (C_A \otimes C_B)^\perp\right)$ . Note that in contrast to the classical Tanner code, in the quantum case it will be more convenient to think of codewords as assignments set on the squares and not on the edges.

Note that any check of  $C_X$  can be thought of as multiplying one of the matrices in  $C_A^\perp \otimes C_B^\perp$  by the local view of some positive vertex. Similarly, the checks of  $C_Z$  are obtained by multiplying the matrices in  $C_A \otimes C_B$  in the local view of the negative vertices. As any two sibling positive and negative vertices share either a row or a column, it is easy to see that the checks commute. Therefore, by definition,  $H_X H_Z^\top = 0$ , which implies that the code is a CSS code.



# Good Quantum LDPC Codes.



Now we can state formally the theorem:

### Theorem

*For  $\varepsilon \in (0, \frac{1}{2})$ ,  $\delta_0 > 0$ , large enough  $\Delta$ , and small codes  $C_A, C_B$  with distance at least  $\delta_0 \Delta$  there exist constant  $\zeta > 0$  such if the dual tensor code of  $C_A, C_B$  is  $\Delta^{1\frac{1}{2}} + \varepsilon$ -robust then there exists an infinite family of square complexes for which the Tanner code  $\mathcal{T} \left( G^+, (C_A^\perp \otimes C_B^\perp)^\perp \right)$  defined by the complexes and the dual tensor code such that for any codeword  $c$  with weight less than  $\zeta n \Delta^2$  there exist a negative vertex in  $v \in V^-$  and code word in  $y \in C_A \otimes C_B$  supported only on the squares adjoint to  $v$  such that  $|c + y| < |c|$ .*

Observe that  $y \in C_Z^\perp \subset C_X$ , so  $c + y \in C_X$  and  $|c + y| < |c| < \zeta \cdot n\Delta^2$ . Therefore, by 18, there is another  $y_1 \in C_Z^\perp$  such that  $|c + y + y_1| < |c + y| < |c|$ . Repeating this process enough times yields a series of  $y, y_1, y_2, \dots, y_l$ , all of them in  $C_Z^\perp$ , such that:

$$|c + y + \dots + y_l| = 0 \Rightarrow c = y + y_1 + y_2 + \dots + y_l \Rightarrow c \in C_Z^\perp$$

## Good Quantum LDPC Codes.

### Claim

*The distance of the dual tensor code is at least  $\delta_0 \Delta$ .*

### Proof.

By the robustness property, any codeword of the dual tensor code with a weight less than  $\delta_0 \Delta$  is supported on at most one row. Let  $c$  be such a codeword and denote by  $i$  the number of the non-trivial row. Fix a  $c' \in C_A^\perp$  such that the  $i$ th coordinate of  $c'$  is non-zero and consider the multiplication of  $c$  with the codewords of  $C_A^\perp \otimes C_B^\perp$  of the following form:

$$J = \left\{ c' \otimes c_b : c_b \in C_B^\perp \right\}$$

□

### Proof.

So the  $i$ th row of any  $x \in J$  is a codeword of  $C_B^\perp$  and in total, collecting all the  $i$ th rows of codewords in  $J$  sums up to all the code words in  $C_B^\perp$ . On the other hand,  $c \cdot x = 0$  for all  $x \in J$ ; that is,  $c \cdot x = c_i \cdot c_b = 0$ . Thus we obtain that  $c_i \in C_B$  and therefore  $|c_i| \geq \delta_0 \Delta \Rightarrow |c| \geq \delta_0 \Delta$ , which is a contradiction.  $\square$

### Definition

Let  $S$  and  $S_-$  denote the positive and negative vertices that support the codeword  $c \in C_X$ , respectively. Furthermore, let  $S_e$  and  $S_n$  denote the exceptional and normal vertices, respectively, where the weight of the local view for any vertex in  $S_e$  is greater than  $\Delta^{3/2+\varepsilon}$ , and  $S_n$  is the complementary set of vertices. An edge in  $G$  will be said to be heavy if it supports more than  $\delta_0\Delta - \Delta^{\frac{1}{2}+\varepsilon}/\delta_0$  squares in  $G$ . Let  $T \subset S_-$  denote the negative vertices connected to  $S_n$  by at least one heavy edge. Additionally, let  $T_s \subset T$  denote the vertices in  $S_-$  that are surrounded by only normal vertices. Finally, for any pair of vertex subsets  $A, B$  such that  $A \subset V_+$  and  $B \subset V_-$ , let  $d_{B \rightarrow A}$  denote the average number of heavy edges leaving  $B$  and going to  $A$ .

## Claim

*for any  $\varepsilon \in (0, 1)$  and large enough  $\Delta$  it holds that  $|S| \leq \Delta^\varepsilon |S_-|$*

## Proof.

Suppose not, namely that  $|S| > \Delta^\varepsilon |S_-|$ , then  $|x|/|S_-| > \Delta^\varepsilon |x|/|S| > \Delta^\varepsilon \cdot \delta_0 \Delta$  But:

$$\frac{|x|}{|S_-|} = \frac{\Theta(E(S_-, S_-))}{|S_-|} \leq \Theta(\Delta^2) \frac{|S_-|}{n} + \Theta(\Delta) \xrightarrow{n \rightarrow \infty} \Theta(\Delta)$$



## Claim

*At least  $1 - \Delta^{-\frac{\epsilon}{4}}$  portion of the negative vertices adjoin to only normal vertices.*



### Proof.

Suppose through contradiction that for  $\Delta^{-p}$  portion of the negative vertices  $v_- \in V_-$  have at least one ( $\Delta^\gamma$ ) sibling in  $S_e$ . Therefore  $\Delta^{-p}|S_-| \leq \Delta|S_e|$  combining with 21 it follows that  $|S| \leq \Delta^{1+\varepsilon+p}|S_e|$  :

$$\begin{aligned}\Delta^{3/2+\varepsilon} &\leq \frac{E(S, S_e)}{|S_e|} = \Theta(\Delta^2) \frac{|S|}{n} + \Theta(\Delta) \sqrt{\frac{|S|}{|S_e|}} \\ &\leq \Theta(\Delta^2) \frac{|S|}{n} + \Theta(\Delta) \Theta\left(\Delta^{\frac{1+\varepsilon+p}{2}}\right)\end{aligned}$$

Thus we obtain contradiction for any  $p < \varepsilon/2$ . In particular for  $p = \varepsilon/4$  we obtain that at least  $1 - \Delta^{-\varepsilon/4}$  portion of the negative vertices are surrounded by only normal vertices. □

### Claim

*Let  $x$  be a codeword of  $(C_A^\perp \otimes C_B^\perp)^\perp$  and  $\xi < w$  such that  $d(x, \mathbb{F}^A \otimes C_B) + d(x, C_A \otimes \mathbb{F}^B) \leq \xi$ . Then  $d(x, C_A \otimes C_B) < 3\xi$ .*

### Proof.

Denote by  $R$  the closest codeword of  $C_A \otimes \mathbb{F}^B$  to  $x$ . Similarly, denote by  $C$  the closest codeword of  $\mathbb{F}^A \otimes C_B$  to  $x$ . Notice that  $C + R \in (C_A^\perp \otimes C_B^\perp)^\perp$ . In addition, the weight of  $C + R$  is bounded by:

$$\begin{aligned} |R + C| &= |x + (x + R) + x + (x + C)| \\ &\leq |(x + R)| + |(x + C)| \leq d(x, C_A \otimes \mathbb{F}^B) + d(x, \mathbb{F}^A \otimes C_B) \\ &\leq w \end{aligned}$$



## Good Quantum LDPC Codes.

### Proof.

Therefore, by the robustness property, there are  $r \in C_A \otimes \mathbb{F}^B$  and  $c \in \mathbb{F}^A \otimes C_B$  such that  $R + C = r + c$ . And  $r, c$  are supported on at most  $|R + C|/\delta_0\Delta$  rows and columns. (Here  $r$  and  $c$  play the role of  $s, t$  in 13.)

Now observe that on one hand  $C + c = R + r$ , and on the other hand  $C + c \in \mathbb{F}^A \otimes C_B$  and  $R + r \in C_A \otimes \mathbb{F}^B$ . Therefore,  $C + c \in C_A \otimes \mathbb{F}^B \cap \mathbb{F}^A \otimes C_B$ . Namely,  $C + c \in C_A \otimes C_B$ . Thus we have:

$$\begin{aligned} d(x, C_A \otimes C_B) &\leq d(x, C) + d(C, C_A \otimes C_B) \\ &\leq \xi + |c| \end{aligned}$$



### Proof.

And in the same way we obtain also that  $d(x, C_A \otimes C_B) \leq \xi + |r|$ . Since  $c, r$  are supported on at most  $|R + C|/\delta_0\Delta$  rows and columns, the weight of the string obtained by joining a single row of  $r$  with  $c$  grows by at least  $\delta_0\Delta - |R + C|/\delta_0\Delta > 0$ . Therefore,  $|c| < |c + r| = |R + C|$ . Thus, in total,  $d(x, C_A \otimes C_B) \leq 3\xi$ .  $\square$

### Claim

*Suppose that  $v \in T_s$ , Namely  $v$  is surrounded by only normal vertices. Then:*

$$d(c_v, C_A \otimes C_B) < \Theta\left(\Delta^{3/2+\varepsilon}\right)$$

## Good Quantum LDPC Codes.

### Proof.

By being surrounded only by normal vertices any row in the local view of  $v$  is codeword of  $C_A$  plus at most  $\Delta^{3/2+\varepsilon}/\Delta = \Delta^{\frac{1}{2}+\varepsilon}$  faults. So correcting the rows require flipping at most  $\Delta \cdot \Delta^{\frac{1}{2}+\varepsilon}$  bits in total. Thus  $d(c_v, C_A \otimes \mathbb{F}^B) < \Delta^{3/2+\varepsilon}$ . In same way we obtain that  $d(c_v, \mathbb{F}^A \otimes C_B) < \Delta^{3/2+\varepsilon}$ . Notice that, in particular,  $d(c_v, (C_A^\perp \otimes C_B^\perp)^\perp) \leq \Delta^{3/2+\varepsilon}$ .

Denote by  $y$  the closest codeword of  $(C_A^\perp \otimes C_B^\perp)^\perp$  to  $c_v$ . And observe that the distance between  $y$  to either  $C_A \otimes \mathbb{F}^B$  or  $\mathbb{F}^A \otimes C_B$  is at most  $2 \cdot \Delta^{3/2+\varepsilon}$ . To see it consider the decoding:

$$y \rightarrow x \rightarrow C_A \otimes \mathbb{F}^B$$

Therefore from 23 it follows that  $d(y, C_A \otimes C_B) < 3\xi$ . So  $d(x, C_A \otimes C_B) < \Delta^{3/2+\varepsilon} + 3\xi$ .



### Claim (The Technical Lemma)

Let  $A \subset S$  and  $B \subset S_-$  be subsets of the positive and negative vertices supported by a codeword  $x \in C_X$  such that  $|x| < \zeta n \Delta^2$  and  $\alpha \leq \Delta^2, \beta \leq \Delta$  are the minimum degrees in  $G^+, G$  induced by  $x$  (note that in  $G^+$  the edges are associated with the squares of the left-right Cayley graph). Assume the following conditions hold:

1.  $\beta = \frac{\delta}{4\sqrt{\Delta}}\alpha + \Theta(\Delta)$
2.  $B$  defined to be all the vertices connected to  $\bar{A}$  by at least one heavy edge.
3. Any vertex in  $\bar{A}$  has at least one heavy edge.

Then:  $d_{B \rightarrow \bar{A}} = \Omega(\Delta)$ .



### Proof.

By the given  $|S| \leq \frac{2|x|}{\delta_0 \Delta} \leq \zeta \frac{2n\Delta}{\delta}$  we have that  $|S|/n \leq \zeta \cdot \frac{2\Delta}{\delta}$ . Then by the Mixing Expander Lemma we have that:

$$\begin{aligned}\alpha|A| &\leq |E(A, S)| \leq \frac{\Delta^2}{n}|A||S| + 4\Delta\sqrt{|A||S|} \leq |A| \cdot \zeta \frac{2\Delta^3}{\delta} + 4\Delta\sqrt{|A||S|} \\ \Rightarrow \sqrt{|A|} \left( \alpha - \zeta \frac{2\Delta^3}{\delta} \right) &\leq 4\Delta\sqrt{|S|} \\ \Rightarrow |A| &\leq \left( \alpha - \zeta \frac{2\Delta^3}{\delta} \right)^{-2} \cdot 16\Delta^2|S|\end{aligned}$$



## Proof.

And by repeating the same calculation but consider  $B$  in the  $G$  graph we obtain:

$$\begin{aligned}\Rightarrow |B| &\leq \left( \beta - \zeta \frac{4 \cdot 2\Delta^2}{\delta} \right)^{-2} \cdot 16\Delta |S| \\ \Rightarrow |B| &\leq \left( \frac{\delta}{\sqrt{\Delta}} \alpha - \zeta \frac{4 \cdot 2\Delta^2}{\delta} \right)^{-2} \cdot 16\Delta |S| \\ &= \frac{\Delta}{\delta^2} \left( \alpha - 4 \cdot 2\zeta \frac{\Delta^{2\frac{1}{2}}}{\delta^2} \right)^{-2} \cdot 16\Delta |S|\end{aligned}$$

And for large enough  $\Delta$  the above is bounded by:

$$\left( \alpha - 4 \cdot 2\zeta \frac{\Delta^{2\frac{1}{2}}}{\delta^2} \right) \geq \left( \alpha - \zeta \frac{2\Delta^3}{\delta} \right) \Rightarrow |B| \leq \frac{1}{\delta^2} \left( \alpha - \zeta \frac{2\Delta^3}{\delta} \right)^{-2} \cdot 16\Delta^2 |S|$$

### Proof.

Now, choose  $\zeta$  such  $\left(\alpha - \zeta \frac{2\Delta^3}{\delta}\right) \geq 16^{\frac{1}{2}} \cdot 100\Delta^{1\frac{1}{2}}$  yields that:

$|A| \leq 10^{-4}\Delta^{-1}|S| \Rightarrow |\bar{A}| \geq (1 - 10^{-4}\Delta^{-1})|S|$ , And  $|B| \leq 10^{-4} \frac{|S|}{16\delta_0^2\Delta}$ . Conditions (2) and (3) guarantee that any vertex in  $\bar{A}$  is connected to at least one vertex of  $B$ . And therefore,  $B$  covers  $\bar{A}$ , that is,  $d_{B \rightarrow \bar{A}} \cdot |B| \geq |\bar{A}|$ , Hence:

$$d_{B \rightarrow \bar{A}} \geq \frac{|\bar{A}|}{|B|} \geq (1 - 10^{-4}\Delta^{-1}) 10^4 \cdot \delta_0^2\Delta = \Theta(\Delta)$$



### Claim

*$S_e$  and  $T$  satisfies the requirments of 25 with  $A = S_e$ ,  $B = T$ ,  $\alpha = \Delta^{3/2+\varepsilon}$  and  $\beta = \delta_0\Delta + \Delta^{\frac{1}{2}+\varepsilon}$ . That is, the average of havey edges form  $T$  to  $S_n$  is  $\Theta(\Delta)$ .*

### Proof.

Conditions (1) and (2) hold by definition of  $S_e$ ,  $T$  for values  $\alpha = \Delta^{3/2+\varepsilon}$  and  $\beta = \delta_0\Delta - \Delta^{\frac{1}{2}+\varepsilon}/\delta_0$ . It remains to show that any normal vertex has at least one heavy edge. By robustness there are  $t, s \in C_A \otimes \mathbb{F}^B, \mathbb{F}^B \otimes C_B$  such that  $t + s = c_v$ . Assume that any row of  $c_v$  has weight less than  $\delta_0\Delta - \Delta^{\frac{1}{2}+\varepsilon}/\delta_0$ . Pick an arbitrary row, and denote it by  $\tau$ . Now observe that by the fact that  $c_v$  has support on at most  $\Delta^{\frac{1}{2}+\varepsilon}/\delta_0$  columns, then  $\tau$  is at a distance of at most  $\Delta^{\frac{1}{2}+\varepsilon}/\delta_0$  from  $C_A$ . But, by assumption,  $|\tau| < \delta_0\Delta - \Delta^{\frac{1}{2}+\varepsilon}/\delta_0$  and therefore the closest codeword to  $\tau$  in  $C_A$  has weight less than  $\delta_0\Delta$ , in contradiction to the fact that the distance of  $C_A$  is at least  $\delta_0\Delta$ .  $\square$

### Claim

*There is a normal-surrounded vertex in  $v \in T_s$  in weight at least  $\Theta(\Delta^2)$ .*

## Proof.

We know from 26 that  $d_{T \rightarrow S_n}$  is linear in  $\Delta$ . Moreover 22 tell us that most of the vertices in  $S_-$  are surrounded only by normal vertices. Denote by  $\mathbf{E}[d(v)|v \in T_s]$  the expected degree of heavy edges connected to vertex in  $T_s$ . Using the conditional expectation formula we get:

$$\begin{aligned} d_{T \rightarrow S_n} &= \mathbf{E}[d(v)|v \in T_s] \Pr[v \in T_s] + \mathbf{E}[d(v)|v \in T/T_s] \Pr[v \in T/T_s] \\ &\leq \mathbf{E}[d(v)|v \in T_s] \Pr[v \in T_s] + \mathbf{E}[d(v)|v \in T/T_s] \Pr[v \in S_-/T_s] \\ &\leq \mathbf{E}[d(v)|v \in T_s] \cdot 1 + \Delta \cdot \Delta^{-\varepsilon/4} \\ &\Rightarrow \mathbf{E}[d(v)|v \in T_s] \geq d_{T \rightarrow S_n} - \Delta^{\frac{3}{4}\varepsilon} = \Theta(\Delta) \end{aligned}$$

□

### Proof.

Therefore there is at least a single vertex in  $T_s$  connected to  $\Theta(\Delta)$  heavy edges. Combining the fact that edge is heavy edge if there are at least  $\delta_0 \Delta - \Delta^{\frac{1}{2} + \varepsilon}$  non trivial bits on its squares we get the desired.  $\square$



## Good Quantum LDPC Codes.

### Remark

For small codes which are robust for  $w < \Delta^{3/2}$ , as in the original proof of [LZ22], 22 no longer holds. However, assuming the dual tensor code is also  $p$ -resistant to puncturing 15, one can still prove 27.

We are about to finish the proof of the theorem. Combining 27 and 24 we obtain the existence of a negative vertex which is both at distance  $\Theta(\Delta^{3/2+\varepsilon})$  from  $C_A \otimes C_B$  and weight at least  $\Theta(\Delta^2)$ . Denote by  $v \in T_s$  that vertex, by  $c_v$  its local view and by  $y \in C_A \otimes C_B$  the closest codeword to  $c_v$ . Subtracting  $y$  from  $c_v$  yields:

$$\begin{aligned} |c_v + y| &= d(c_v, y) = \Theta(\Delta^{3/2+\varepsilon}) < |c_v| \\ \Rightarrow |c + y| &< |c| \end{aligned}$$