From classical to good quantum LDPC codes.

D. Ponarovsky[1]

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.

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

Today.

- Brif Review of Coding. Tanner and Expander codes.
- Quantum Error Correction Codes.
- Good Classical Locally Testabile Codes and Good Qauntum 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

$\downarrow$

22-23

NLTS

Hamiltonians

from good

qLDPC codes [ABN22] $\rightarrow$

Future.

"We understand quantum complexity.

as well as we understand classical complexity".

QMA ? qPCP

$\downarrow$

Exsitance of family of statmensts and quantum proofs,

such that any slightly noisy version of the proofs

is still a proof and cann't be yilded by

'weak' computations.

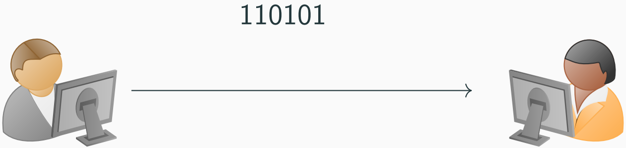
21-22		22-23		Future.
				"We understand quantum complexity. as well as we understand classical complexity". QMA ? qPCP $\downarrow$
good qLDPC [Din+22], [PK21], [LZ22]	$\rightarrow$	NLTS Hamiltonians from good qLDPC codes [ABN22]	$\rightarrow$	Exsitance of family of statmensts and quantum proofs, such that any slightly noisy version of the proofs is still a proof and cann't be yilded by 'weak' computations.

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.

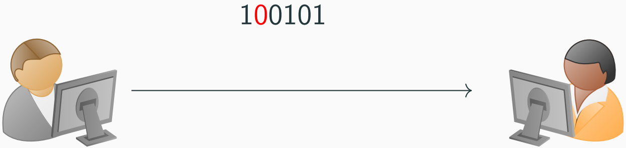
Coding.

Bob is willing to send some message to Alice through



Coding.

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



Coding.

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

100101110101110101

100101

Coding.

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

100101110101110101

100101

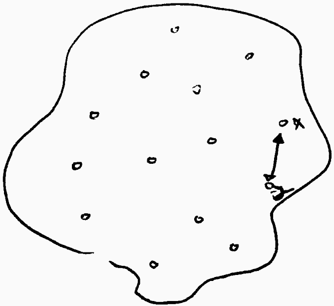
Coding.

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

$$|100101110101110101\rangle$$
$$|100101\rangle$$

Coding.

C



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

Coding.

Non formally, We call for the embedding of entitis 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 $*$ bits flip?

Coding.

Non formally, We call for the embedding of entitis 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 $*$ bits flip?
- At the cost of at most $*$ extra bits?

Coding.

Non formally, We call for the embedding of entitis 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 $*$ bits flip?
- At the cost of at most $*$ extra bits?
- Can we ensure an efficient decoding (and checking) sechme?

Coding.

Non formally, We call for the embedding of entitis 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 $*$ bits flip?
- At the cost of at most $*$ extra bits?
- Can we ensure an efficient decoding (and checking) sechme?
- In the assymptotic regime, when the size of the original message grows.

Coding.

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 ρn and any pair of distinict elements in C differ in at least δn coordinates. We call to the vectors belong to C *codewords*, to ρn the diminsion of the code, and to δn the distance of the code.

Coding.

Definition

A **family of codes** is an infinite series of codes. Additionally, suppose the rates and relative distances converge into constant values ρ, δ. 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.

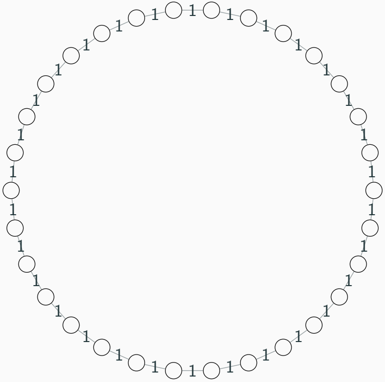
Tanner Codes.

Definition

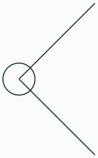
Let Γ be a graph and C_0 be a "small" linear code with finate parameters $[\Delta, \rho\Delta, \delta\Delta]$. Let $C = \mathcal{T}(\Gamma, C_0)$ be all the codewords which, for any vertex $v \in \Gamma$, the local view of v is a codeword of C_0. We say that C is a **Tanner code** of Γ, C_0. Notice that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

Coding.

Another example, the repttion code can be thought as the tanner graph defind by the parity code on the cyle graph.

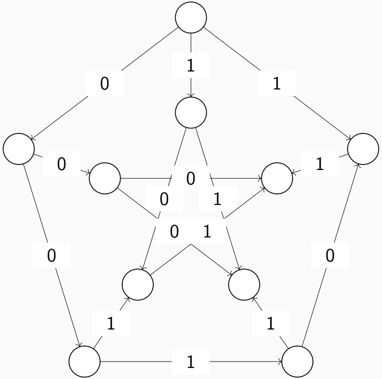


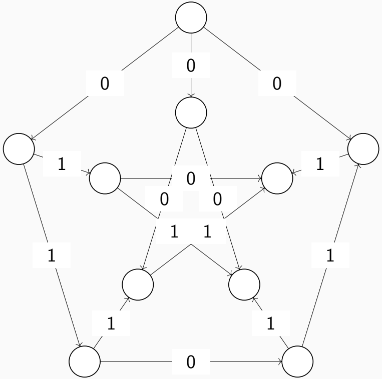
$$\overbrace{\begin{bmatrix} 1 & 1 \end{bmatrix}}^{\text{parity check matrix of } C_0}$$



$$\overbrace{\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}}^{\substack{\text{Parity check matrix of } \mathcal{T}(\Gamma, C_0) \\ \text{Each row associated with vertex check.}}}$$

Example, the parity code on the Peterson graph.





Coding.

Lemma

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

Coding.

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 $\square$

Coding.

Note, that if the Γ is a family of Δ-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 chack matrix of $\mathcal{T}(\Gamma, C_0)$ is finte. We say that a family of codes with a parity cheack matrices having a constant row weight is a Low Density Parity Check code (LDPC). LDPC can be view as the first local property and also has practical value as it implies a linear time algorithm for correctness verification.

Coding.

Definition

Denote by λ the second eigenvalue of the adjacency matrix of the Δ-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:

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

Codeing.

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.

Codeing.

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 Mixining Lemma we have that:

$$\frac{E(S,S)}{|S|} \leq \frac{\Delta}{n}|S| + \lambda$$

$$\leq_{n\to\infty} o(1) + \lambda$$

□

Coding.

Proof.

$$\frac{E(S,S)}{|S|} \leq \frac{\Delta}{n}|S| + \lambda$$
$$\leq_{n\to\infty} o(1) + \lambda$$

Namely, for any such sublinear weight string, x, the average of nontrivial edges for the vertex is less than λ. So there must be at least one vertex $v \in S$ that, on his local view, sets a string at a weight less than λ. 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 $\square$

Quantum In Our Presentation.

For presanting as simple as possible, we will refer to quantum state $|\psi\rangle$ as a linear combination of classical states with ± 1 coffeicents 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 presanting as simple as possible, we will refer to quantum state $|\psi\rangle$ as a linear combination of classical states with ± 1 coffeicents 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.

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

Quantum In Our Presentation.

For presanting as simple as possible, we will refer to quantum state $|\psi\rangle$ as a linear combination of classical states with ± 1 coffeicents 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.

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 $|1\rangle$ cann't both encoded to a single ket codeword.

Quantum Error Correction Codes.

The clouds perspective.

Definition (CSS Code)

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

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

Quantum Error Correction Codes.

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

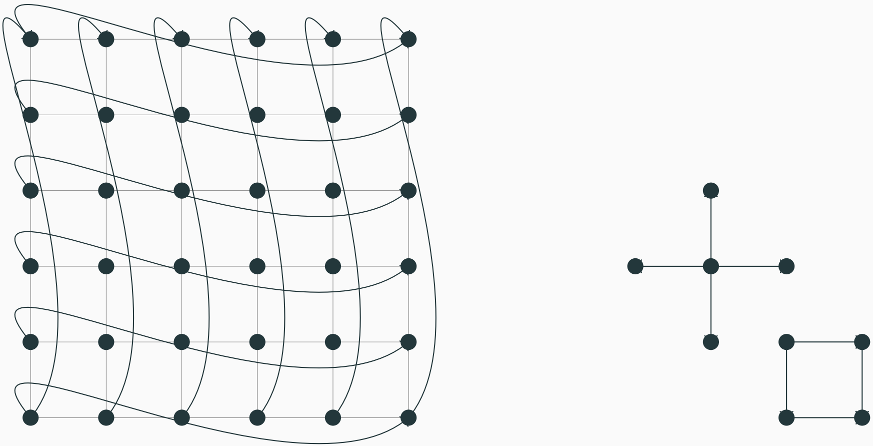
Furthermore, if one is willing to has an qLDPC code, then H_X and H_Z can't be parity check matrices of good classical code as any column of $H_z^\top$ is a codeword of C_X.

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

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 qauntum 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 excactly one coordinate.

Quantum Error Correction Codes.



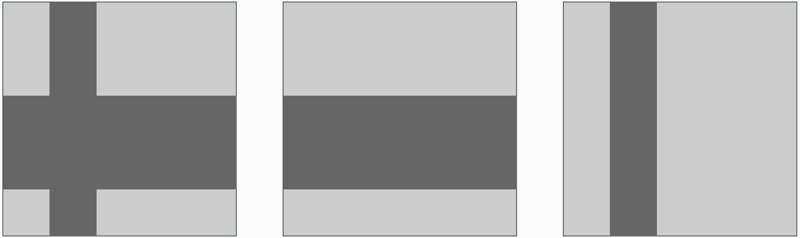
Quantum Error Correction Codes.

Definition (w-Robustness)

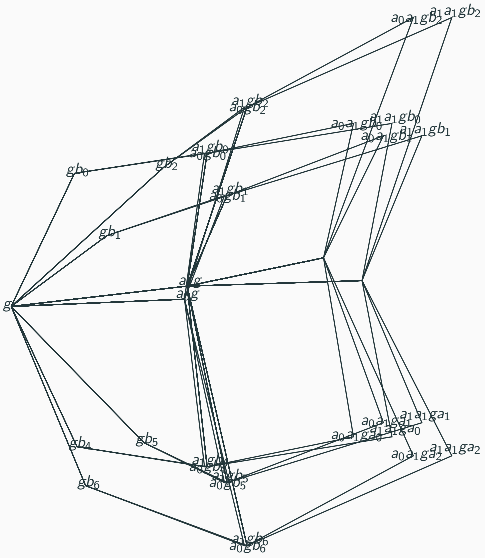
Let C_A and C_B be codes of length Δ with minimum distance $\delta_0\Delta$. $C = \left(C_A^\perp \otimes C_B^\perp\right)^\perp$ will be said to be w-robust if for any codeword $c \in C$ of weight less than w, it follows that c can be decomposed into a sum of $c = t + s$ such that $t \in C_A \otimes \mathbb{F}^B$ 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.

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



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 Γ be a group at size n. And let A, B be a two generator set of Γ 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 $a(u, \pm) = (au, \mp)$).

Quantum Error Correction Codes.

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.

The existence of good quantum LDPC codes and locally testable codes (LTCs) was considered an open problem for roughly two decades. Although they seemed to be related only by containing the word "code" in their names, they were proven to exist by the same construction. They first appeared in [Din+22] as good locally testable codes and not long after that in [PK21], in which they also extended and derived the result to obtain the quantum code. We emphasize that even though they developed the same codes, their proofs are not similar at all. Here, we follow the [LZ22] work, which simplifies the original proof and does not rely on any concept more complicated than what we have already seen in the previous chapters. They also coined the term "Quantum Tanner Codes" referring to the fact that C_X and C_Z are classical Tanner codes. 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

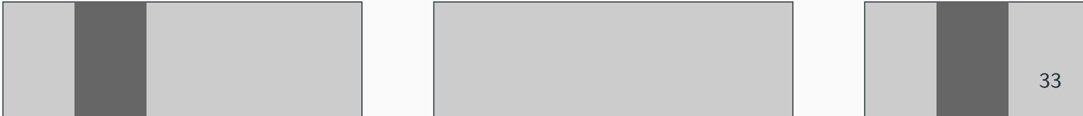
Recall our insight that for a pair of LDPC codes to define a good CSS code, they must both be poor codes in the sense that they must have a constant distance. Therefore, we understand that any codeword in C_X with small weight belongs to $C_Z^{\perp}$. To prove this, we will construct a proof such that 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 Δ with minimum distance $\delta_0\Delta$.
$C = \left(C_A^\perp \otimes C_B^\perp\right)^\perp$ 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 $t \in C_A \otimes \mathbb{F}^{B'}$.

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



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 ε is positive. For achiving that we use the theorem proven in [KP22]:

Theorem

Fix $\rho_A, \rho_B \in (0,1)$, and let κ 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 Δ-length and $\rho_A\Delta, \rho_B\Delta$ codimension codes sampled uniformly at random. Then, with high probability as $\Delta \to \infty$, for any codeword of their dual tensor code $c \in \left(C_A^\perp \otimes C_B^\perp\right)^\perp$, 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 κ product expanding.

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 ρ and large enough Δ, there exists $\delta > 0$ such that $\left(C_A^\perp \otimes C_B^\perp\right)^\perp$ 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 ρ and δ, 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.

Definition (Quantum Tanner Code.)

Let Γ be a group at size n. And let A, B be a two generator set of Γ 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.

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

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.

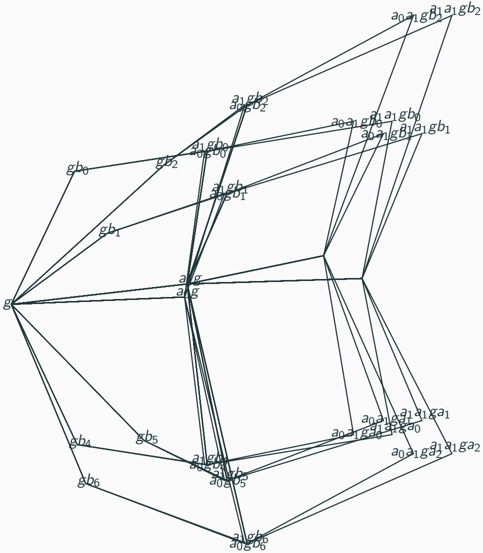


Figure 3: Local environment of a square complex.

Now we can state formally the theorem:

Theorem

For $\varepsilon \in \left(0, \frac{1}{2}\right)$, $\delta_0 > 0$, large enough Δ, 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 weigh 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 squers 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 17, 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 $y, y_1, y_2, \ldots, y_l$, all of them in $C_Z^\perp$, such that:

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

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 ith 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:

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

So the ith row of any $x \in J$ is a codeword of $C_B^\perp$ and in total, collecting all the ith 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. □

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 $d_{B\to A}$ denote the average number of heavy edges leaving B and going to A.

Claim

for any $\varepsilon \in (0,1)$ *and large enough* Δ *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:

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

$\square$

Claim

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

Proof.

Suppose through contradiction that for Δ^{-p} portion of the negative vertices $v_- \in V_-$ have at least one (Δ^γ) sibling in S_e. Therefore $\Delta^{-p}|S_-| \leq \Delta|S_e|$ combining with 20 it follows that $|S| \leq \Delta^{1+\varepsilon+p}|S_e|$:

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

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 surounded by only normal vertices. $\square$

Claim

Let x be a codeword of $\left(C_A^{\perp} \otimes C_B^{\perp}\right)^{\perp}$ 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 $C + R \in \left(C_A^\perp \otimes C_B^\perp\right)^\perp$. In addition, the weight of $C + R$ is bounded by:

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

□

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:

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

$\square$

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 surounded by only normal vertices. Then:

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

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 $d\left(c_v, C_A \otimes \mathbb{F}^B\right) < \Delta^{3/2+\varepsilon}$. In same way we obtain that $d\left(c_v, \mathbb{F}^A \otimes C_B\right) < \Delta^{3/2+\varepsilon}$. Noitce that, in parituclar, $d(c_v, (C_A^\perp \otimes C_B^\perp)^\perp) \leq \Delta^{3/2+\varepsilon}$.

Denote by y the closest codeword of $\left(C_A^\perp \otimes C_B^\perp\right)^\perp$ to c_v. And observes 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:

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

Therefore form 22 it follows that $d\left(y, C_A \otimes C_B\right) < 3\xi$, So $d\left(x, C_A \otimes C_B\right) < \Delta^{3/2+\varepsilon} + 3\xi$. $\square$

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

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:

$$\alpha|A| \leq |E(A,S)| \leq \frac{\Delta^2}{n}|A||S| + 4\Delta\sqrt{|A||S|} \leq |A| \cdot \zeta \frac{2\Delta^3}{\delta} + 4\Delta\sqrt{|A||S|}$$

$$\Rightarrow \sqrt{|A|}\left(\alpha - \zeta\frac{2\Delta^3}{\delta}\right) \leq 4\Delta\sqrt{|S|}$$

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

□

Proof.

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

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

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

$$= \frac{\Delta}{\delta^2}\left(\alpha - 4\cdot 2\zeta\frac{\Delta^{2\frac{1}{2}}}{\delta^2}\right)^{-2} \cdot 16\Delta|S|$$

And for large enugh Δ the above is bounded by:

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

$\square$

Proof.

Now, choose ζ such $\left(\alpha - \zeta\frac{2\Delta^3}{\delta}\right) \geq 16^{\frac{1}{2}} \cdot 100\Delta^{1\frac{1}{2}}$ yields that:
$|A| \leq 10^{-4}\Delta^{-1}|S| \Rightarrow |\bar{A}| \geq \left(1 - 10^{-4}\Delta^{-1}\right)|S|$, And $|B| \leq 10^{-4}\frac{|S|}{16\delta_0^2\Delta}$. Conditions (2) and (3) garunte that any vertex in $\bar{A}$ is connected to at least on vertex of B. And therfore, B covers $\bar{A}$, that is, $d_{B\to\bar{A}} \cdot |B| \geq \bar{A}$, Hence:

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

□

Claim

S_e and T satisfies the requrirments of 24 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 τ. Now observe that by the fact that c_v has support on at most $\Delta^{\frac{1}{2}+\varepsilon}/\delta_0$ columns, then τ 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 τ 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-surounded vertex in $v \in T_s$ in weight at least $\Theta\left(\Delta^2\right)$.

Proof.

We know from 25 that $d_{T \to S_n}$ is linear in Δ. Morever 21 tell us that most of the vertices in S_- are surrounded only by normal vertices. Denote by $\mathbf{E}\left[d(v) | v \in T_s\right]$ the expected degree of heavy edges connected to vertex in T_s. Using the conditional expection formula we get:

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

□

Proof.

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

Remark

For small codes which are robust for $w < \Delta^{3/2}$, as in the original proof of [LZ22], 21 no longer holds. However, assuming the dual tensor code is also p-resistant to puncturing 15, one can still prove 26.

We are about to finish the proof of the theorem. Combining 26 and 23 we obtain the the existnes of a negative vertex which is both at distance $\Theta\left(\Delta^{3/2+\varepsilon}\right)$ form $C_A \otimes C_B$ and weight at least $\Theta\left(\Delta^2\right)$. Denote by $v \in T_s$ that vertex, by c_v it's local view and by $y \in C_A \otimes C_B$ the closest codeword to c_v. Subtructing y from c_v yilds:

$$|c_v + y| = d\left(c_v, y\right) = \Theta\left(\Delta^{3/2+\varepsilon}\right) < |c_v|$$
$$\Rightarrow |c + y| < |c|$$