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
↓

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.

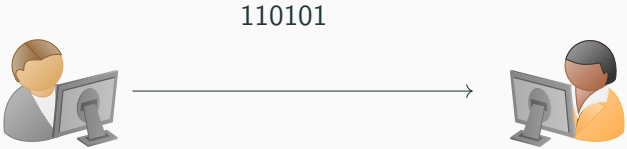
21-22	22-23	Future.
good qLDPC [Din+22], [PK21], [LZ22]	NLTS Hamiltonians from good qLDPC codes [ABN22]	"We understand quantum complexity. as well as we understand classical complexity". QMA ? qPCP ↓ Exsitance of family of statmensts and quantum proofs, such that any slightly noisy version of the proofs 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

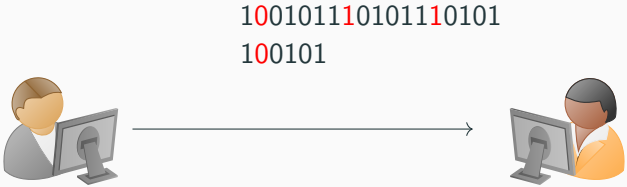


Coding.

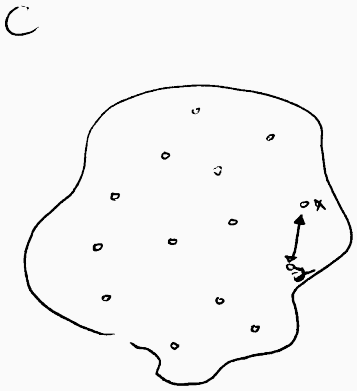
Bob is willing to send some message to Alice through a noisy chanell in which bits might be fliped.

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.



Coding.



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

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.

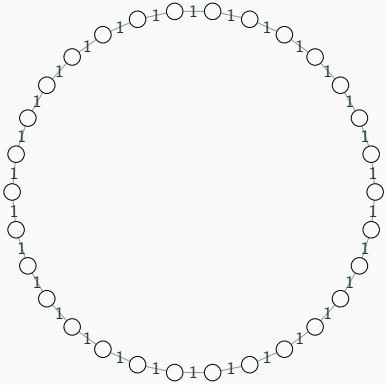
Tanner Codes.

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.

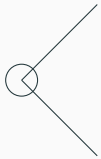
Coding.

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



parity check matrix of C_0

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

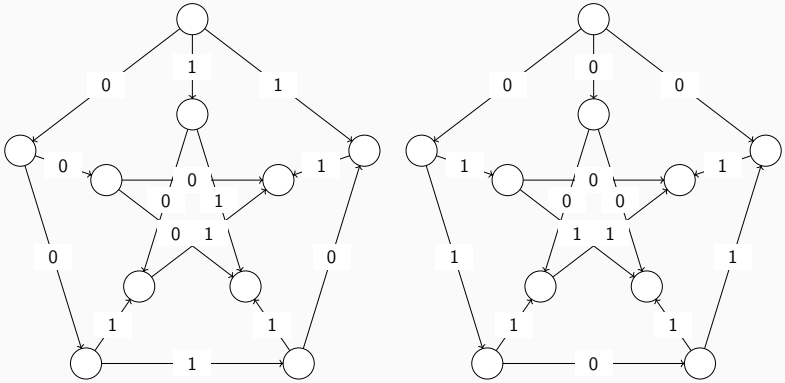


Parity check matrix of $\mathcal{T}(\Gamma, C_0)$
Each row associated with vertex check.

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

Tanner Codes.

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.

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:

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

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 Mixining Lemma we have that:

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

□

Proof.

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

Namely, for any such sublinear weight string, x, the average of nontrivial edges for the vertex is less than 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 □

Quantum Error Correction Codes.

Back to the quantum noise.

So in the quntum setting any state can be a superpostion of classical states.

Quantum Noise.

$$|110101\rangle + |010100\rangle + |011110\rangle$$

Quantum Noise.

$$|110101\rangle + |010100\rangle + |011110\rangle$$

Quantum Noise.

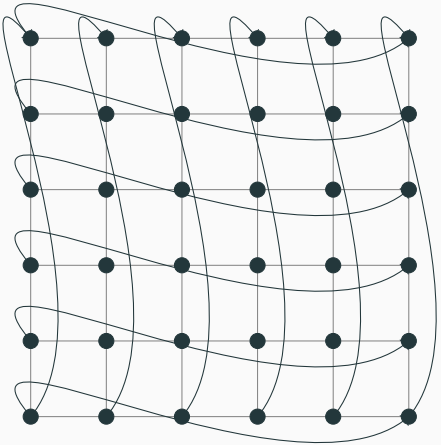
$$|010101\rangle + |110100\rangle - |111110\rangle$$
$$|110101\rangle + |010100\rangle + |011110\rangle$$

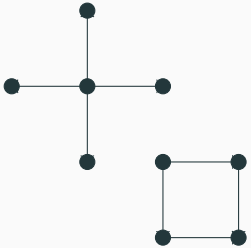
Definition (CSS Code)

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:

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

Quantum Error Correction Codes.

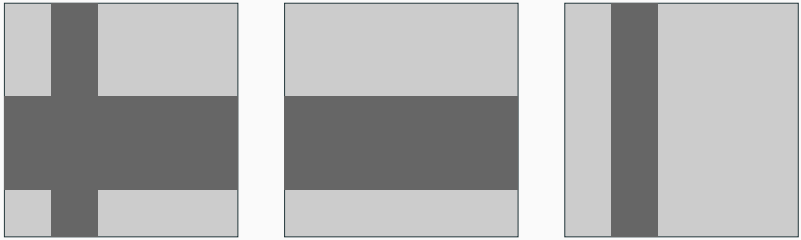




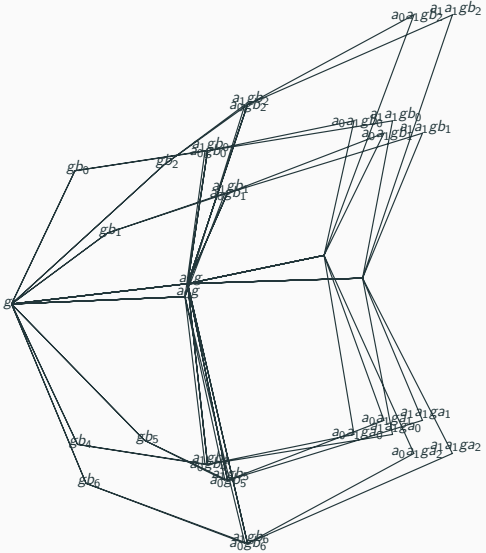
Definition (w-Robustness)

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 $t \in C_A \otimes \mathbb{F}^{B'}$.

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



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 $a\,(u, \pm) = (au, \mp)$).

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 $\mathcal{T}\left(G^+, \left(C_A^\perp \otimes C_B^\perp\right)^\perp\right)$ and C_Z is defined as $\mathcal{T}\left(G^-, \left(C_A \otimes C_B\right)^\perp\right)$. 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.

Quantum Error Correction Codes.