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.

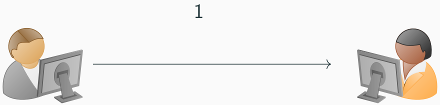
- Brif Review of Coding. Tanner and Expander codes.
- Quantum Error Correction Codes.

Today.

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

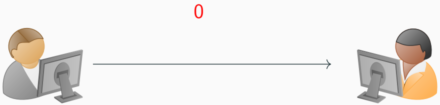
Classical Vs Quantum Encoding.

Classical:



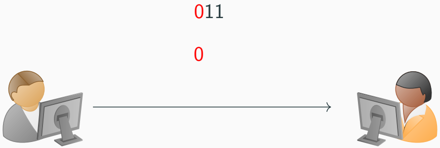
Classical Vs Quantum Encoding.

Classical:



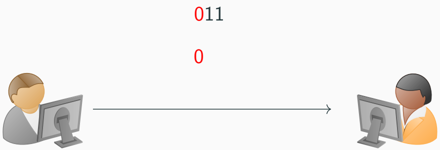
Classical Vs Quantum Encoding.

Classical:



Classical Vs Quantum Encoding.

Classical:



Classical Vs Quantum Encoding.

Classical:

$|{\color{red}0}11\rangle$

$|{\color{red}0}\rangle$

Classical Vs Quantum Encoding.

Classical:

$|011\rangle$

$|0\rangle$

Quantum:

$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$

Classical Vs Quantum Encoding.

Classical:

$|{\color{red}0}11\rangle$

$|{\color{red}0}\rangle$

Quantum:

$\frac{1}{\sqrt{2}}\left(|0\rangle {\color{red}-} |1\rangle\right)$

Classical Vs Quantum Encoding.

Classical:

$|{0}11\rangle$

$|0\rangle$

Quantum:

$\frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right)$

$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$

Classical Vs Quantum Encoding.

Classical:

$|011\rangle$

$|0\rangle$

Quantum:

$\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

The C.S Questions.

In the asymptotic regime, can we encode quantum states in codes robust against many errors, as our original massage grows? And in what costs?

Good Classical LDPC Code.

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 distinct elements in C differ in at least δn coordinates. We call to the vectors belong to C *codewords*, to ρn the dimension of the code, and to δn the distance of the code.

Good Classical LDPC Code.

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 distinct elements in C differ in at least δn coordinates. We call to the vectors belong to C *codewords*, to ρn the dimension of the code, and to δn the distance of the code.

Definition

A **family of codes** is an infinite series of codes..

Good Classical LDPC Code.

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 distinct elements in C differ in at least δn coordinates. We call to the vectors belong to C *codewords*, to ρn the dimension of the code, and to δn the distance of the code.

Definition

A **family of codes** is an infinite series of codes..

Definition

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

Good Classical LDPC Code.

Parity Check Matrix.

Code C is a linear subspace $\Rightarrow$ There is a matrix H such:

$$x \in C \Leftrightarrow Hx = 0$$

We will call H the parity check matrix.

Definition

A codes family will be called LDPC code if weight of any row (col) in H is $O(1)$.

Good Classical LDPC Code.

Example. Repetition code.

Let the Repetition code, $[n, 1, n]$ be the mapping $0 \to 0^n$ and $1 \to 1^n$.

Good Classical LDPC Code.

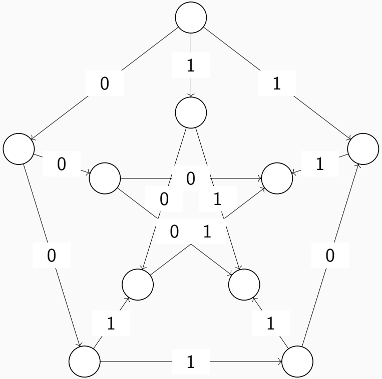
Technic for design LDPC families with positive rate.

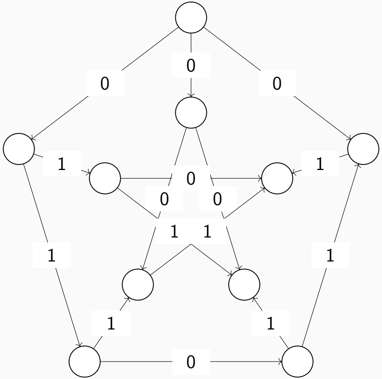
Definition

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.

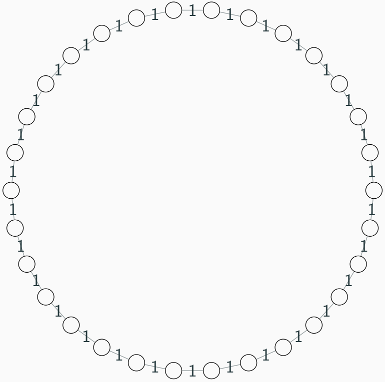
Good Classical LDPC Code.

Example, the parity code on the Peterson graph.

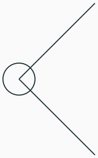




Another example, the repttion code can be thought as the tanner graph defind by the parity code on the cyle graph.



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



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

Good Classical LDPC Code.

Lemma

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

Good Classical LDPC Code.

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 $\square$

Good Classical LDPC Code.

Technic for design LDPC families with positive relative distance.

Good Classical LDPC Code.

Technic for design LDPC families with positive relative distance.

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 λ-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:

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

Good Classical LDPC Code.

Lemma

Using λ-Expander, the Tanner Code defined bit is a good LDPC code.

Good Classical LDPC Code.

Lemma

Using λ-Expander, the Tanner Code defined bit 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:

$$\begin{aligned} \text{bits seen by any } v \in S \leq & \text{ average degree of } v \in G \text{ restricted to } S \\ & = \frac{E(S,S)}{|S|} \leq \frac{\Delta}{n}|S| + \lambda \\ & \leq_{n \to \infty} o(1) + \lambda \end{aligned}$$

$\square$

Quantum Encoding.

Quantum Codes in Our Presentation.

C will be called $[n, k, d]$ Quantum Code if:

1. for all $|\psi\rangle, |\phi\rangle \in C \to \frac{1}{\sqrt{2}}(|\psi\rangle \pm |\phi\rangle) \in C$.
2. Let P be a tensor product of n matrices taken from the set $\{I, X, Z\}$ where X, Z are the Pauli matrices:

   $$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

   such, that less than $d/2$ of the elements in the product aren't identity. Then there is oneway mapping T such that $T[P|\psi\rangle] \to |\psi\rangle$ for any $|\psi\rangle \in C$.
3. There are k independents states in C.

Quantum Encoding.

Quantum Encoding.

Idea I - (Uncertainty) Clouds as States.

'claim'

Let C be quantum code with $d > 1$. Then there aren't two distinct $|\psi\rangle, |\phi\rangle \in C$ such that they both supported only a single classical state (bit string).

Idea I - (Uncertainty) Clouds as States.

'claim'

Let C be quantum code with $d > 1$. Then there aren't two distinct $|\psi\rangle, |\phi\rangle \in C$ such that they both supported only a single classical state (bit string).

Proof.

Assume through contradiction, $x, y \in \mathbb{F}_2^n$ such that $|\psi\rangle = |x\rangle$ and $|\phi\rangle = |y\rangle$. Let $i \in [n]$ be a coordinate such $x_i \neq y_i$ and consider the codewords: $|\pm\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle \pm |\phi\rangle)$. Now observes that applying the $P = I_0 \otimes I_1..I_{i-1} \otimes Z_i \otimes I_{i+1}..$, maps $P|+\rangle \to |-\rangle$. Hence the distance of C is less than one. $\square$

CSS Code.

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:

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

CSS Code.

CSS.

We think about the base of Q (generators) as the generators of $C_X / C_Z^{\perp}$, and it is easy to see that:

1. $\dim Q = \dim C_X - \dim C_Z^{\perp}$.
2. The distance of Q is the lightest codeword of C_X (C_Z) doesn't belong to $C_Z^{\perp}$ ($C_X^{\perp}$).
3. Denote by H_X, H_Z the parity check matrices of the classic codes, The rows of H_Z are in $C_Z^{\perp} \Rightarrow$ are also in $C_X \rightarrow H_X H_Z^{\top} = 0$. We will say that Q is LDPC if any rows of both H_X, H_Z have at most $O(1)$ weight.

'Idea II' - Tanner Checks are 'Too Much' Interdependence.

'claim'

Let C_1, C_2 be codes at length Δ and let G be Δ-reg Graph. $\mathcal{T}(G, C_1), \mathcal{T}(G, C_2)$ don't define a CSS.

'Idea II' - Tanner Checks are 'Too Much' Interdependence.

'claim'

Let C_1, C_2 be codes at length Δ and let G be Δ-reg Graph. $\mathcal{T}(G, C_1), \mathcal{T}(G, C_2)$ don't define a CSS.

Proof.

Draw on the board. $\square$

'Idea III' - Impossibility of Both C_X, C_Z being Good.

'claim'

C_X, C_Z can't be both good LDPC and define a CSS.

'Idea III' - Impossibility of Both C_X, C_Z being Good.

'claim'

C_X, C_Z can't be both good LDPC and define a CSS.

Proof.

Let C_X, C_Z define a CSS, and assume they both LDPC. Hence $H_X H_Z^\top = 0 \Rightarrow$ the rows of H_Z are codewords of C_X. Therefore there are codewords in C_X at $O(1)$ weight. $\square$

Quantum Tanner Code Construction.

Proving Strategy.

Classical

- Assuming x is low weight codeword.
- Using the graph expansion we show the existences of vertices with low weight local view.

Quantum.

- Assuming x is low weight codeword.

Proving Strategy.

Classical

- Assuming x is low weight codeword.
- Using the graph expansion we show the existences of vertices with low weight local view.

Quantum.

- Assuming x is low weight codeword.
- Using the graph expansion to show the existences of vertex u in the negative graph with high weight local view. Yet, surrounded by only positive vertices with low weigh local view.

Proving Strategy.

Classical

- Assuming x is low weight codeword.
- Using the graph expansion we show the existences of vertices with low weight local view.

Quantum.

- Assuming x is low weight codeword.
- Using the graph expansion to show the existences of vertex u in the negative graph with high weight local view. Yet, surrounded by only positive vertices with low weigh local view.
- Assuming a property on the small code, $\rightarrow$ there is a codeword c in $C_Z^{\perp}$ supported only on u's squares such that $|c + x| < |x|$.

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

Quantum Tanner Code.

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