From calassical to quantum good 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.
- Quantum Error Correction Codes.

Today.

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

Future.

"We understand quantum complexity".

BQP ? QMA? PSPACE.

Future.

”We understand quantum complexity”.

BQP ? QMA? PSPACE.

Future.

"We understand quantum complexity".

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

Future.

"We understand quantum complexity.
as well as we understand classical complexity".
BQP ? QMA? 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
$\downarrow$

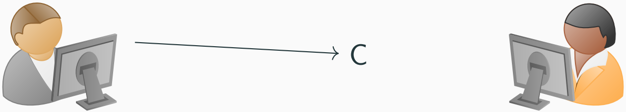
22-23		Future.
NLTS Hamiltonians from good qLDPC codes	$\rightarrow$	"We understand quantum complexity. as well as we understand classical complexity". QMA ? qPCP $\downarrow$ Family of witness (Quantum states) that can't approximate by "weak" machines.

21-22		22-23		Future.
				"We understand quantum complexity. as well as we understand classical complexity".
				QMA ? qPCP
				$\downarrow$
good qLDPC	$\rightarrow$	NLTS Hamiltonians from good qLDPC codes	$\rightarrow$	Family of witness (Quantum states) that can't approximate by "weak" machines.

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.



Coding.

Can we come up with a code that tolerates $*$ bits flip?

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. In addition, we call the vectors belong to C *codewords* and define the distance of C to be the minimal number of different bits between any codewords pair of C.

Coding.

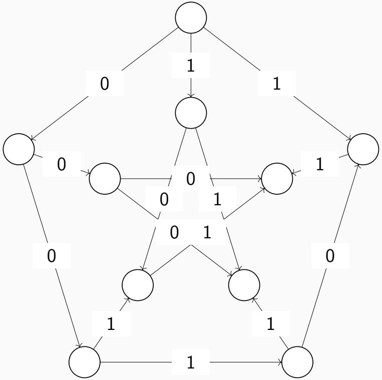
Definition

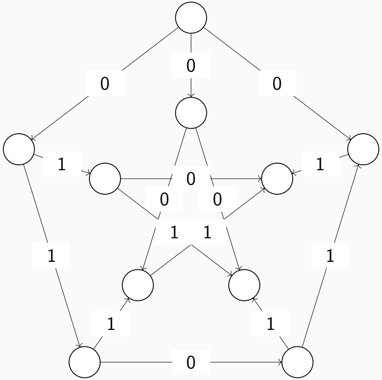
A **family of codes** is an infinite series of codes. Additionally, suppose the rates and relative distances converge into constant values ρ, δ. In that case, we abuse the notation and call that family of codes a code with $[n, \rho n, \delta n]$ for fixed $\rho, \delta \in [0, 1)$, and infinite integers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

Definition

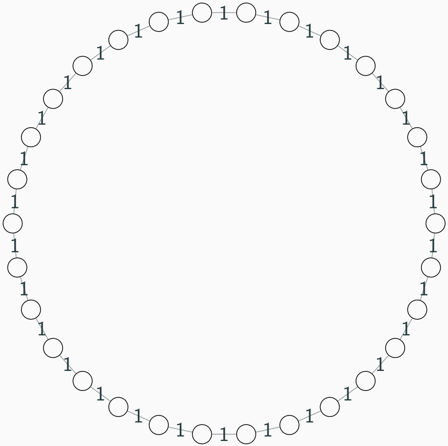
We will say that a family of codes is a **good code** if its parameters converge into positive values.

Coding.





Coding.



Quantum Error Correction Codes.

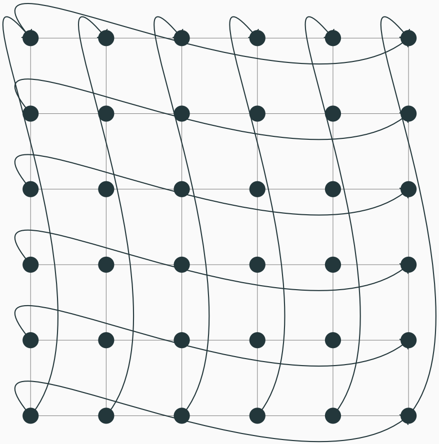
Quantum Error Correction Codes.

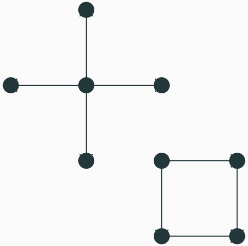
Definition (CSS Code)

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 code words 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.



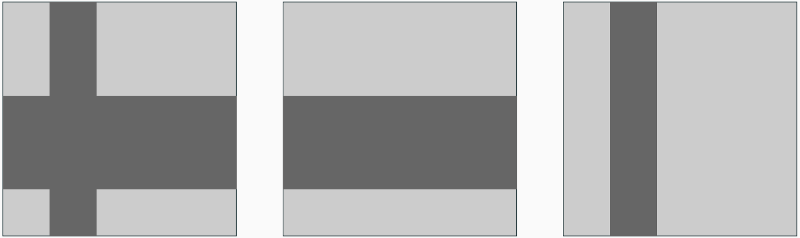


Definition (w-Robustness)

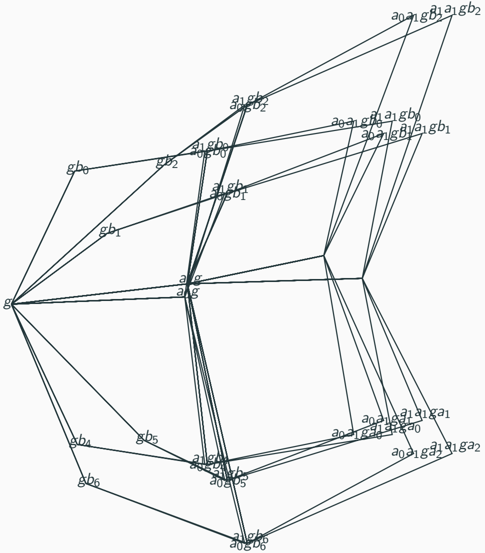
Let C_A and C_B be codes of length Δ with minimum distance $\delta_0\Delta$. $C = \left(C_A^{\perp} \otimes C_B^{\perp}\right)^{\perp}$ will be said to be w-robust if for any codeword $c \in C$ of weight less than w, it follows that c can be decomposed into a sum of $c = t + s$ such that $t \in C_A \otimes \mathbb{F}^B$ 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 $t \in C_A \otimes \mathbb{F}^{B'}$.

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.



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 $\mathcal{T}\left(G^+, (C_A^\perp \otimes C_B^\perp)^\perp\right)$ 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.

Quantum Error Correction Codes.