construction of asymptotically good quantum LDPC codes

Gilles Zémor, joint work with Anthony Leverrier

Bordeaux Mathematics Institute

October 2023, Najac

Quantum (CSS) codes

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_X \\ \mathbf{H}_Z \end{bmatrix}$$

Two matrices $\mathbf{H}_X, \mathbf{H}_Z$ with orthogonal row spaces.

Dimension of code is: $n - \dim \mathbf{H}_X - \dim \mathbf{H}_Z$.

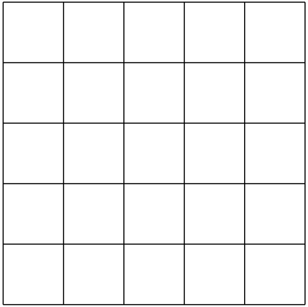
Minimum distance d_X defined as minimum weight of binary error $\mathbf{e}_X$ orthogonal to rows of $\mathbf{H}_X$ and *not in row-space of* $\mathbf{H}_Z$.

Distance d_Z defined similarly. Minimum distance of quantum code is:

$$d = \min(d_X, d_Z).$$

We are interested in $\mathbf{H}_X, \mathbf{H}_Z$ *low-density*. Quantum LDPC codes.

Example: Kitaev toric code.



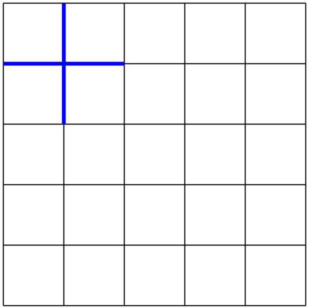
$$\mathbf{H}_X = \begin{bmatrix} \quad \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} \quad \end{bmatrix}$$

$\mathbf{H}_X$: rows consist of elementary cocycles.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

Example: Kitaev toric code.



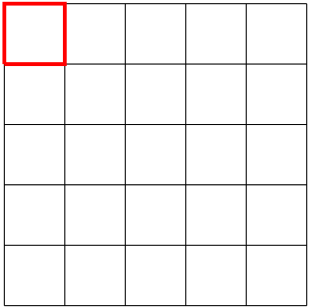
$$\mathbf{H}_X = \begin{bmatrix} 111100 \quad \cdots & & \\ & & \\ & & \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$$

$\mathbf{H}_X$: rows consist of elementary cocycles.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

Example: Kitaev toric code.



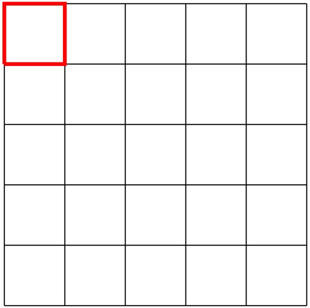
$$\mathbf{H}_X = \begin{bmatrix} {\color{blue}111100 \; \cdots} \\ \\ \\ \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} {\color{red}001111 \; \cdots} \\ \\ \\ \end{bmatrix}$$

$\mathbf{H}_X$: rows consist of elementary cocycles.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

Example: Kitaev toric code.



$$\mathbf{H}_X = \begin{bmatrix} 111100 \cdots & \\ & \\ & \end{bmatrix}$$

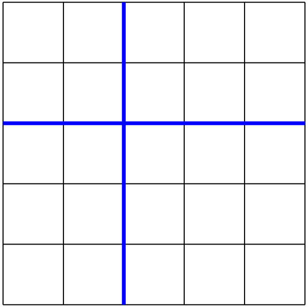
$$\mathbf{H}_Z = \begin{bmatrix} 001111 \cdots & \\ & \\ & \end{bmatrix}$$

$\mathbf{H}_X$: rows consist of elementary cocycles.

$\mathbf{H}_Z$: rows consist of elementary cycles (faces).

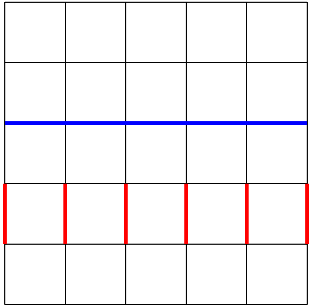
Dimension: $k = n - \dim \mathbf{H}_X - \dim \mathbf{H}_Z = \dim \ker \sigma_X / \operatorname{Im} \sigma_Z = 2$. $\mathbb{F}_2$-homology of torus.

Kitaev's toric code, minimum distance



Homologically non-trivial cycles.

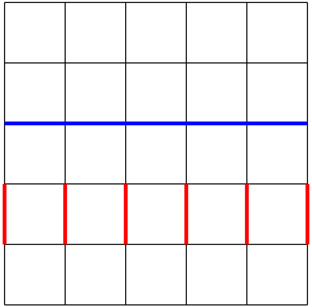
Kitaev's toric code, minimum distance



Homologically non-trivial cycles.

and cocycles

Kitaev's toric code, minimum distance



Homologically non-trivial cycles.

and cocycles

We obtain the quantum code's parameters

$$[[2m^2, 2, m]] \qquad d = \sqrt{n/2}.$$

Issues: raise the dimension, raise the minimum distance.

Context: minimum distance beyond $\sqrt{n}$

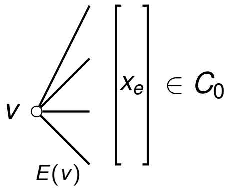
- Freedman, Luo, Meyer 2002. $d \geq \sqrt{n} \log^{1/4} n$.
- Evra, Kaufman, Z, 2020. $d \geq \sqrt{n} \log n$.
- Kaufman, Tessler, 2020. $d \geq \sqrt{n} \log^k n$.
- Hastings, Haah, O'Donnell, 2020 $d \geq n^{0.6}$.
- Panteleev, Kalachev, 2021 $d \geq n/logn$.
- Panteleev, Kalachev, 2022, asymptotically good quantum LDPC codes.
- Leverrier, Z, 2022. Quantum Tanner codes.

Classical Tanner code.

Ingredients.

1. A regular graph (V, E) of degree Δ.
2. A code C_0 of length Δ.

Code is space of functions $x : E \to \mathbb{F}_2$ such that for every vertex $v \in V$, x restricted to $E(v)$ is in C_0.



Sipser-Spielman 1996. *Expander codes.*

A codeword is a subgraph with minimum degree equal to minimum distance of C_0.

If the graph is an expander then all such subgraphs must be large – by definition of expansion.

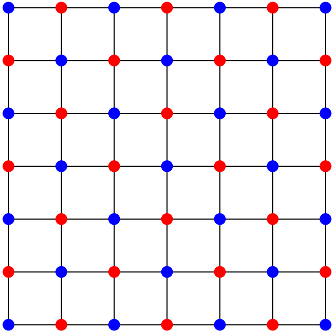
Tanner codes

Can one do a quantum version of a Tanner code ?

Say bipartite graph: one set of vertices carries X-checks (generators), the other set the Z-checks.

Issue. Two neighbouring vertices typically share just one edge: in which case two checks on the two vertices are either disjoint or not orthogonal.

QLDPC codes, Kitaev toric code. Square complex version

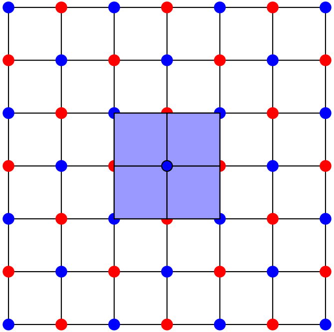


$$\mathbf{H}_X = \begin{bmatrix} \\ \\ \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} \\ \\ \end{bmatrix}$$

- Qubits are on squares !
- One set of vertices for X equations, one set of vertices for Z equations

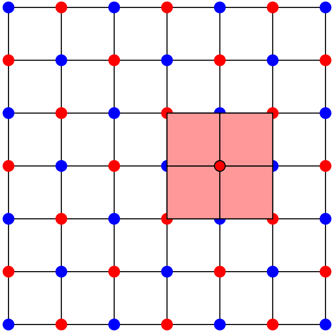
QLDPC codes, Kitaev toric code. Square complex version



$$\mathbf{H}_X = \begin{bmatrix} 111100 \cdots & \\ & \\ & \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} & \\ & \\ & \end{bmatrix}$$

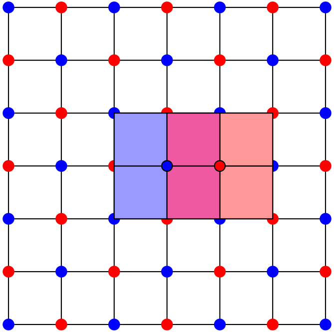
QLDPC codes, Kitaev toric code. Square complex version



$$\mathbf{H}_X = \begin{bmatrix} 111100 \cdots \\ \\ \\ \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} 001111 \cdots \\ \\ \\ \end{bmatrix}$$

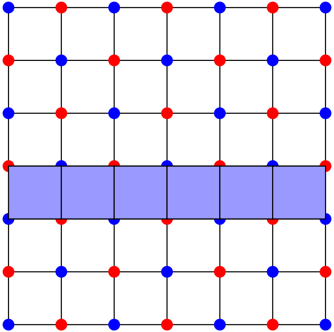
QLDPC codes, Kitaev toric code. Square complex version



$$\mathbf{H}_X = \begin{bmatrix} 111100 \cdots \\ \\ \\ \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} 001111 \cdots \\ \\ \\ \end{bmatrix}$$

QLDPC codes, Kitaev toric code. Square complex version



$$\mathbf{H}_X = \begin{bmatrix} \quad \end{bmatrix}$$

$$\mathbf{H}_Z = \begin{bmatrix} \quad \end{bmatrix}$$

$[[N, 2, \sqrt{N}]]$ code

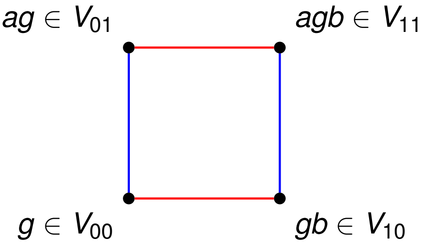
Generalize to left-right Cayley complex

Left-right complex from Dinur, Evra, Livne, Lubotzky, Mozes 2022, used to construct locally testable codes with constant rate, distance, and locality.

Form two Cayley graphs Cay(G, A) and Cay(G, B) over a group G.

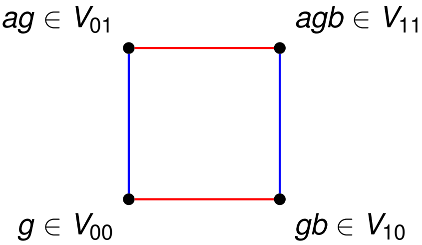
The left-right Cayley complex

Four copies of G. $V_{00}, V_{10}, V_{01}, V_{11}$. $A = A^{-1}, B = B^{-1}$.

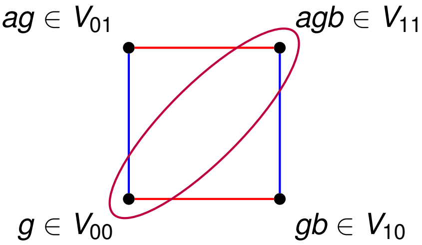


$|A| = |B| = \Delta$, so every vertex v incident to $|Q(v)| = \Delta^2$ squares.

The graphs $\mathcal{G}_0^\square$ and $\mathcal{G}_1^\square$

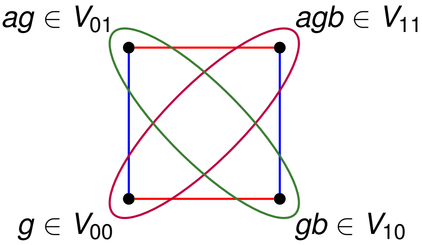


The graphs $\mathcal{G}_0^{\square}$ and $\mathcal{G}_1^{\square}$



Throw away $V_1 = V_{10} \cup V_{01}$: squares are downgraded to edges, we have a graph $\mathcal{G}_0^{\square}$ over vertex set $V_0 = V_{00} \cup V_{11}$.

The graphs $\mathcal{G}_0^\square$ and $\mathcal{G}_1^\square$



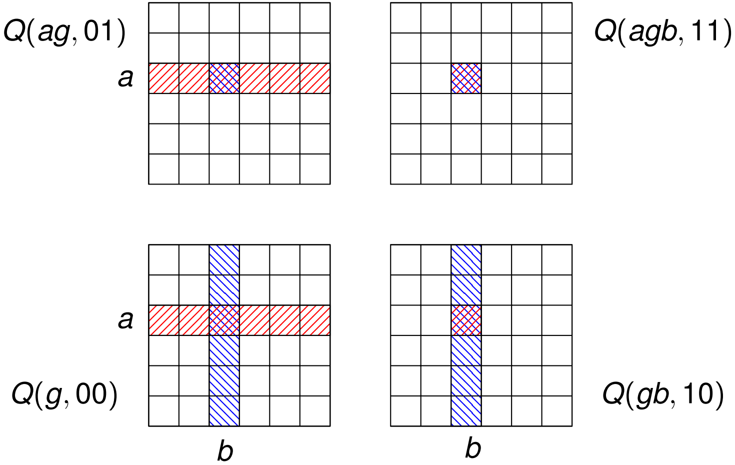
Throw away $V_1 = V_{10} \cup V_{01}$: squares are downgraded to edges, we have a graph $\mathcal{G}_0^\square$ over vertex set $V_0 = V_{00} \cup V_{11}$.

Throw away V_0, we have $\mathcal{G}_1^\square$.

Two graphs, ***that share the same edge set.*** Degree: Δ^2.

Q-neighbourhoods

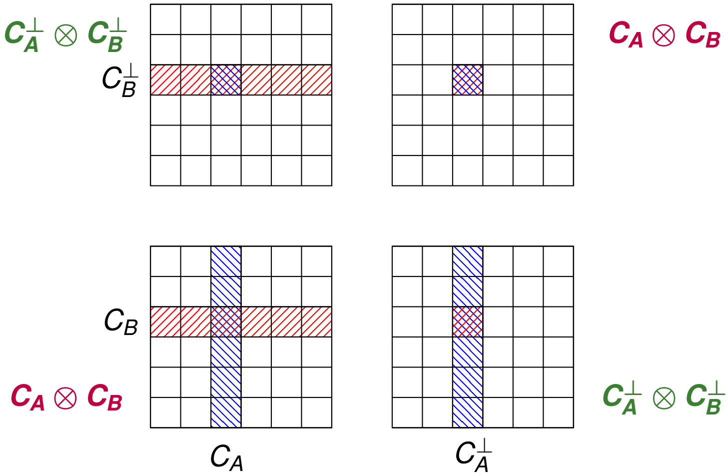
The set $Q(v)$ of squares $\{g, ag, gb, agb\}$incident to g can be labelled $A \times B$.



Quantum Tanner codes, Leverrier-Z 2022

Bits on squares.

Two sets of constraints, $\boldsymbol{C_A} \otimes \boldsymbol{C_B}$ on V_0 and $\boldsymbol{C_A^\perp} \otimes \boldsymbol{C_B^\perp}$ on V_1.



Generalises Kitaev Code

Kitaev case: $|A| = |B| = 2$.

$C_A = C_B = C_A^{\perp} = C_B^{\perp} = \{[00], [11]\}$.

Every check equation has the form:

1	1
1	1

Tanner code view

$\mathcal{C}_0$ is Tanner code on $\mathcal{G}_0^\square$ and $\mathcal{C}_1$ is Tanner code on $\mathcal{G}_1^\square$ with inner codes

$$(C_A \otimes C_B)^\perp = C_A^\perp \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B^\perp$$

$$(C_A^\perp \otimes C_B^\perp)^\perp = C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B.$$

Rate of quantum code: if C_A and C_B have rates ρ and $1-\rho$, then quantum code has rate $(1-2\rho)^2$.

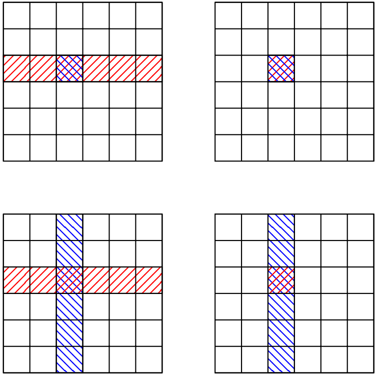
Minimum distance: minimum weight of word of $\mathcal{C}_1$ that is not in $\mathcal{C}_0^\perp$.

Proved to be linear in length n if Cayley graphs $\mathrm{Cay}(G, A)$ and $\mathrm{Cay}(G, B)$ are sufficiently expanding.

Minimum distance

Tanner codeword that is not sum of generators.

$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$



$C_A \otimes C_B$

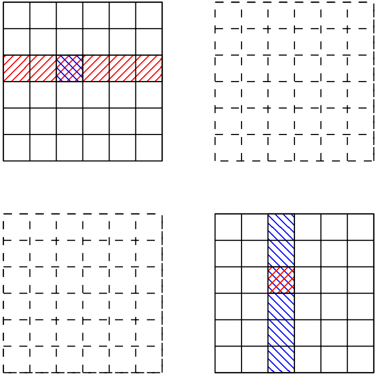
$C_A \otimes C_B$

$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$

Minimum distance argument for quantum code

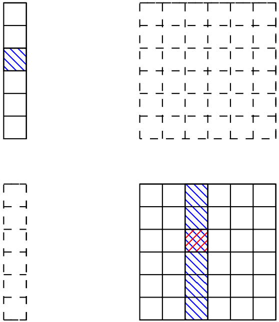
Expansion in $\mathcal{G}_1^{\square}$ implies that most local views have small weight. (Almost) single columns or rows.

$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$



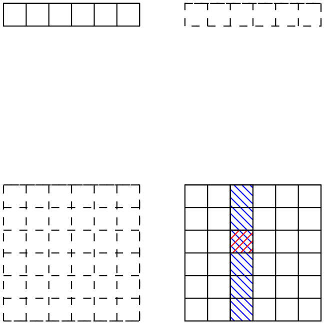
$C_A \otimes \mathbb{F}_2^B + \mathbb{F}_2^A \otimes C_B$

Minimum distance argument



Collapse local views to single column: recover Cayley graph Cay(G, A).

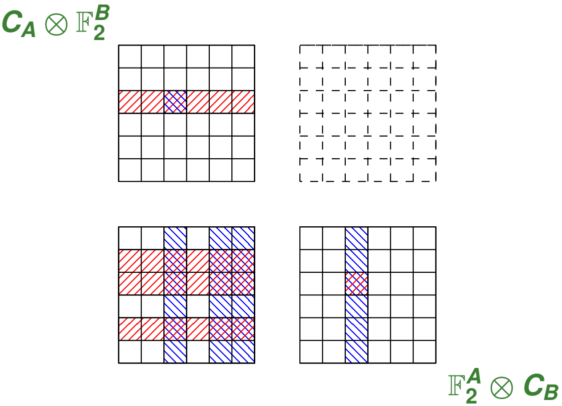
Minimum distance argument



Collapse local views to single column: recover Cayley graph Cay(G, A).

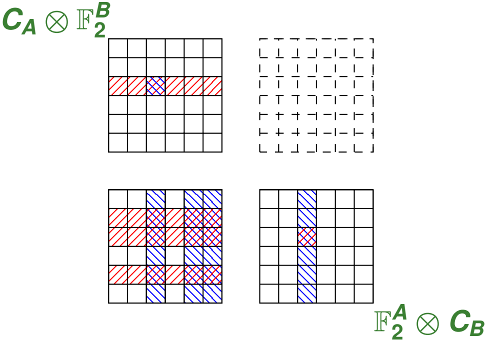
And Cayley graph Cay(G, B).

Minimum distance argument



Single row (column) codewords from local views on $v \in V_1$ *cluster* on local views of V_0. Because of expansion in $\mathrm{Cay}(G, A), \mathrm{Cay}(G, B)$.

Minimum distance argument

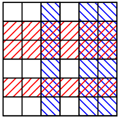


Such a local view of x is close to $\mathbb{F}_2^A \otimes C_B$ and to $C_A \otimes \mathbb{F}_2^B$.

Therefore close to codeword of $C_A \otimes C_B$.
Add it to x and decrease its weight.

Iterate and obtain that x is sum of generators.

Robustness



Close to $\mathbb{F}_2^A \otimes C_B$ and close to $C_A \otimes \mathbb{F}_2^B$ implies close to $C_A \otimes C_B$.

Robustness of tensor code.

Equivalently, for dual tensor codeword $x = c + r$, $c \in C_A \otimes \mathbb{F}_2^B$, $r \in \mathbb{F}_2^A \otimes C_B$,

$$|x| \geq \kappa\Delta(\|c\| + \|r\|) \quad \| \ \| \text{ number of columns/rows}$$

Robustness is equivalent to local testability of tensor code

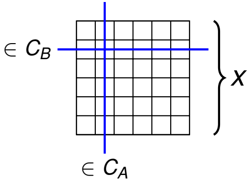
Test whether y is close to $C_A \otimes C_B$ by testing closeness to C_A and C_B on a few random rows/columns.

gives answer ‘close’ only when y close to $c \in C_A \otimes \mathbb{F}_2^B$ and close to $r \in \mathbb{F}_2^A \otimes C_B$. But then $r + c$ has small weight so by robustness equals $r' + c'$ with $\|c\|$ and $\|r\|$ small.

So y close to $c + c' = r + r' \in C_A \otimes C_B$.

Robustness of tensor/dual-tensor codes

$|x| \geq \kappa\Delta(\|c\| + \|r\|)$ $\quad$ $\|\ \|$ number of columns/rows



First known to hold when $|x| \ll \Delta^{3/2}$ for randomly chosen codes C_A, C_B. Now without any condition on $|x|$.

Gives minimum distance linear in length n, and also decoding in linear time.

Extended to parallel decoding.

Robustness vs decoding

- Gu, Pattison, Tang, 2022: improved robustness and decoding of LZ codes
- Dinur, Hsieh, Lin, Vidick, 2022: complete robustness and decoding of dual construction of PK codes
- Leverrier, Z, 2022: decoding LZ codes with reduced robustness
- Kalachev, Panteleev 2022: complete robustness

Problem: obtain robust tensor codes $C_A \otimes C_B$ for $\dim C_A + \dim C_B \geq \Delta$.
Replace random choice by constructions ??

For $\dim C_A + \dim C_B \leq \Delta$, Reed-Solomon codes (Polishchuk, Spielman, 1994).
(Not robust for higher rates).

Connection to (classical) locally testable codes

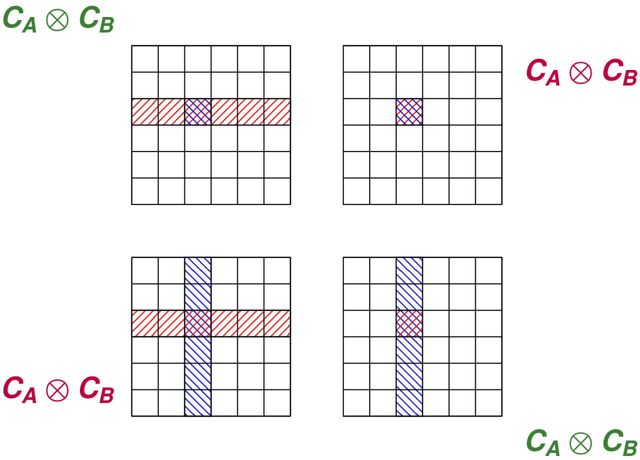
If a code is LDPC then the syndrome $\sigma(\mathbf{e})$ of a low-weight vector $\mathbf{e}$ is low-weight

Converse ?

Locally testable means that a syndrome $\sigma(\mathbf{x})$ is low-weight *iff* it is the syndrome of a low-weight vector $\sigma(\mathbf{x}) = \sigma(\mathbf{e})$.

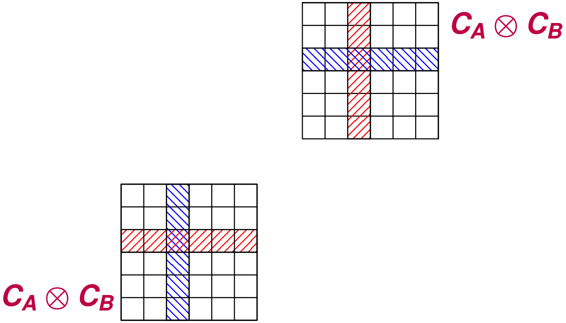
The Dinur et al code.

Tanner code on $\mathcal{G}_1^{\square}$ with inner code $C_A \otimes C_B$. Note: also Tanner code on $\mathcal{G}_0^{\square}$, so *redundant checks* !



Test

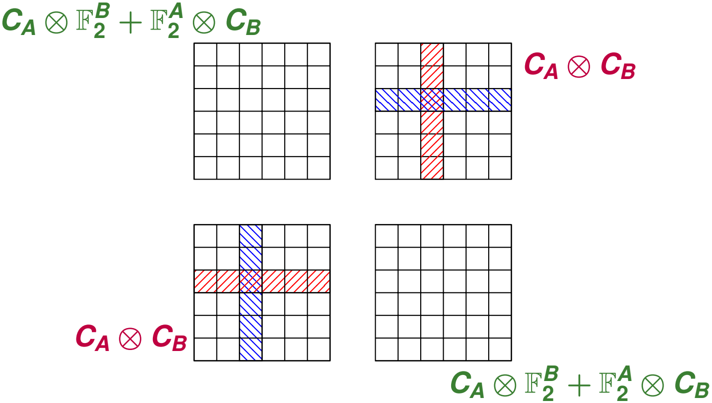
To test vector x, sample some local views and test whether belong to $C_A \otimes C_B$.



Suppose few local views of x not in $C_A \otimes C_B$. Choose the closest local view in $C_A \otimes C_B$ and sum them all: *mismatch vector* Z.

Mismatch vector Z is sum of generators

(if the quantum code has large distance).
So there is a Tanner codeword close to x.



Other developments and open problems

- Hopkins, Lin 2022. Application to sum of squares approximation
- Anshu, Breukmann, Nirkhe, 2022. Proof of NLTS conjecture.

Open problems:

Alternatives to the left-right Cayley complex ?

locally testable quantum LDPC code ?