

Title: Homological Product Codes

Date: Nov 27, 2013 04:00 PM

URL: <http://pirsa.org/13110091>

Abstract: Quantum codes with low-weight stabilizers known as LDPC codes have been actively studied recently due to their potential applications in fault-tolerant quantum computing. However, all families of quantum LDPC codes known to this date suffer from a poor distance scaling limited by the square-root of the code length. This is in a sharp contrast with the classical case where good families of LDPC codes are known that combine constant encoding rate and linear distance. Here we propose the first family of good quantum codes with low-weight stabilizers. The new codes have a constant encoding rate, linear distance, and stabilizers acting on at most square root of  $n$  qubits, where  $n$  is the code length. For comparison, all previously known families of good quantum codes have stabilizers of linear weight. Our proof combines two techniques: randomized constructions of good quantum codes and the homological product operation from algebraic topology. We conjecture that similar methods can produce good stabilizer codes with stabilizer weight  $n^a$  for any  $a > 0$ . Finally, we apply the homological product to construct new small codes with low-weight stabilizers.  
This is a joint work with Matthew Hastings.

# Homological Product Codes

Sergey Bravyi

IBM Watson Research Center

joint work with

Matthew Hastings

Microsoft Station Q

arXiv:1311.0885

Perimeter Institute  
Nov. 27, 2013

# OUTLINE

1. Quantum LDPC codes
2. Boundary operators and homological product
3. Tillich & Zemor construction
4. Homological product of two random codes
5. Open problems

**Quantum code:** a linear subspace  $C$  of  $n$ -qubit system such that all states in  $C$  are locally indistinguishable

**Main quantum applications:** reliable memory and computing, communication over a noisy channel, secret sharing

CSS codes: the codespace  $C$  is a common eigenspace of Pauli stabilizers. Each stabilizer is a product of  $X$  or  $Z$ .

CSS codes: the codespace  $C$  is a common eigenspace of Pauli stabilizers. Each stabilizer is a product of X or Z.

Example:

$$S_1 = X_1 X_2 X_3 \quad S_2 = X_3 X_4 X_5 \quad T_1 = Z_1 Z_3 Z_4 \quad T_2 = X_2 X_3 X_5$$

$$C = \{ \psi : S_i \psi = \psi, \quad T_j \psi = \psi \text{ for all } i, j \}$$

Qubits

1

2

3

4

5

## Why do we care about LDPC ?

- Simple fault-tolerant syndrome readout circuits
- LDPC codes with a distance growing faster than  $\log(n)$  have a constant error threshold for stochastic error models [2,3].
- Toy models of local Hamiltonians with topologically ordered ground states [1]
- Classical LDPC codes are widely used in modern communication protocols

[1] Kitaev, quant-ph/9707021 (Ann. Phys. 303, p.2, 2003)

[2] Kovalev and Pryadko, arxiv:1208.2317 (PRA 87, 020304, 2013)

[3] Gottesman, arxiv:1310.2984

## Why do we care about LDPC ?

- Simple fault-tolerant syndrome readout circuits
- LDPC codes with a distance growing faster than  $\log(n)$  have a constant error threshold for stochastic error models [2,3].
- Toy models of local Hamiltonians with topologically ordered ground states [1]
- Classical LDPC codes are widely used in modern communication protocols

[1] Kitaev, quant-ph/9707021 (Ann. Phys. 303, p.2, 2003)

[2] Kovalev and Pryadko, arxiv:1208.2317 (PRA 87, 020304, 2013)

[3] Gottesman, arxiv:1310.2984

Big open question: existence of **GOOD LDPC codes**.

Desired properties:

- Tanner graph has bounded degree:  $W = O(1)$
- Constant encoding rate:  $k/n = \Omega(1)$
- Constant relative distance:  $d/n = \Omega(1)$

## Previous work

	k	d	W
2D Surface Codes (SC) [1]	$O(1)$	$n^{1/2}$	4
2D Hyperbolic SC [2]	$\Omega(n)$	$\log(n)$	$O(1)$
3D Generalized SC [3]	$O(1)$	$(n \log n)^{1/2}$	$O(1)$
Hypergraph Product Codes [4] (almost good)	$\Omega(n)$	$n^{1/2}$	$O(1)$
Good Quantum Codes [5] (not LDPC)	$\Omega(n)$	$\Omega(n)$	$\Omega(n)$

[1] Kitaev (1997)

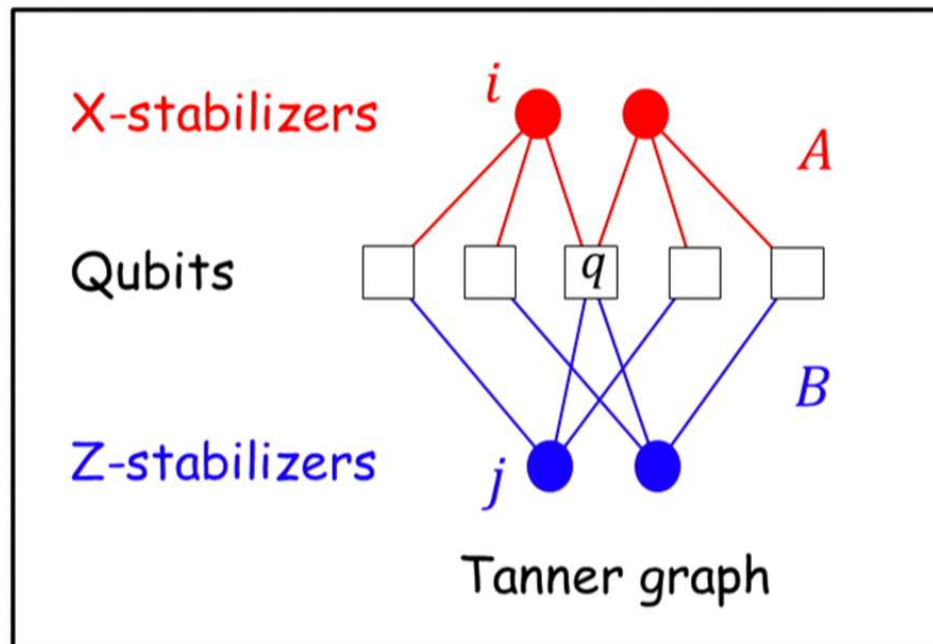
[2] Zemor (2009); Delfosse (2013)

[3] Freedman, Meyer, Luo (2002)

[4] Tillich, Zemor (2009); Kovalev, Pryadko (2012);  
Freedman, Hastings (2013)

[5] Calderbank, Shor (1996); Ashikhmin et al (2000);  
Brown, Fawzi (2013)

Describe the Tanner graph by a pair of binary adjacency matrices  $A$  and  $B$



Connect  $i$  and  $q$  if  $A_{i,q} = 1$

Connect  $j$  and  $q$  if  $B_{j,q} = 1$

**Definition:**

A binary square matrix  $\delta$  is called a **boundary operator** if

$$\delta^2 = 0 \pmod{2}$$

Any boundary operator  $\delta$  defines a quantum CSS code with the adjacency matrices  $\delta$  and  $\delta^T$

$$\text{CSS}(\delta): \quad A = \delta \quad B = \delta^T$$

**X-stabilizers** = rows of  $\delta$       **Z-stabilizers** = columns of  $\delta$

$$AB^T = \delta^2 = 0 \pmod{2}$$

Example:

$$\delta =$$

1	1	1		
		1	1	1
1	1		1	1
1	1	1		
		1	1	1

Example:

$\delta =$

1	1	1		
		1	1	1
1	1		1	1
1	1	1		
		1	1	1

$\rightarrow S_1 = X_1 X_2 X_3$   
 $\rightarrow S_2 = X_3 X_4 X_5$

Parameters of the code  $CSS(\delta)$ :

Number of physical qubits:  $n = \text{size}(\delta)$

Parameters of the code  $CSS(\delta)$ :

Number of physical qubits:  $n = \text{size}(\delta)$

Number of logical qubits:

$$k = \dim(\ker(\delta)) - \dim(\text{im}(\delta))$$

Distance  $d$  is the smallest of X-distance and Z-distance:

$$d^Z = \min\{ \text{wt}(f) : f \in \ker(\delta) \setminus \text{im}(\delta) \}$$

Parameters of the code  $CSS(\delta)$ :

Number of physical qubits:  $n = \text{size}(\delta)$

Number of logical qubits:

$$k = \dim(\ker(\delta)) - \dim(\text{im}(\delta))$$

Distance  $d$  is the smallest of X-distance and Z-distance:

$$d^Z = \min\{ \text{wt}(f) : f \in \ker(\delta) \setminus \text{im}(\delta) \}$$

$$d^X = \min\{ \text{wt}(f) : f \in \ker(\delta^T) \setminus \text{im}(\delta^T) \}$$

Maximum degree  $W$  = maximum weight of rows  
and columns of  $\delta$

Parameters of the code  $CSS(\delta)$ :

Number of physical qubits:  $n = \text{size}(\delta)$

Number of logical qubits:

$$k = \dim(\ker(\delta)) - \dim(\text{im}(\delta))$$

Distance  $d$  is the smallest of X-distance and Z-distance:

$$d^Z = \min\{ \text{wt}(f) : f \in \ker(\delta) \setminus \text{im}(\delta) \}$$

$$d^X = \min\{ \text{wt}(f) : f \in \ker(\delta^T) \setminus \text{im}(\delta^T) \}$$

Maximum degree  $W$  = maximum weight of rows  
and columns of  $\delta$

Input boundary  
operators



Output boundary  
operator

$$\Delta = \delta_1 \otimes I + I \otimes \delta_2$$

Input boundary operator  $\delta_a$  acts on a space  $C_a$ ,  $a = 1, 2$

Operator  $\Delta$  acts on the tensor product  $C_1 \otimes C_2$

$$\Delta^2 = (\delta_1)^2 \otimes I + 2 \delta_1 \otimes \delta_2 + I \otimes (\delta_2)^2 = 0 \pmod{2}$$

Input boundary  
operators



Output boundary  
operator

$$\Delta = \delta_1 \otimes I + I \otimes \delta_2$$

Input boundary operator  $\delta_a$  acts on a space  $C_a$ ,  $a = 1, 2$

Operator  $\Delta$  acts on the tensor product  $C_1 \otimes C_2$

$$\Delta^2 = (\delta_1)^2 \otimes I + 2 \delta_1 \otimes \delta_2 + I \otimes (\delta_2)^2 = 0 \pmod{2}$$

What are parameters of the output code ?



$$CSS(\delta_a) = [[n_a, k_a, d_a]], \text{ maximum degree } W_a$$

$$CSS(\Delta) = [[n, k, d]], \text{ maximum degree } W$$

$$n = n_1 n_2 \text{ (we take a tensor product of spaces)}$$

What are parameters of the output code ?



$$CSS(\delta_a) = [[n_a, k_a, d_a]], \text{ maximum degree } W_a$$

$$CSS(\Delta) = [[n, k, d]], \text{ maximum degree } W$$

$$n = n_1 n_2 \text{ (we take a tensor product of spaces)}$$

$$k = k_1 k_2 \text{ (by Kunneth theorem)}$$

$$W \leq W_1 + W_2 \text{ (taking a tensor product with the identity operator does not change row or column weight; use triangle inequality)}$$

**Distance of the output code:** only lower and upper bounds.

Recall two types of distances for Z-errors and X-errors:

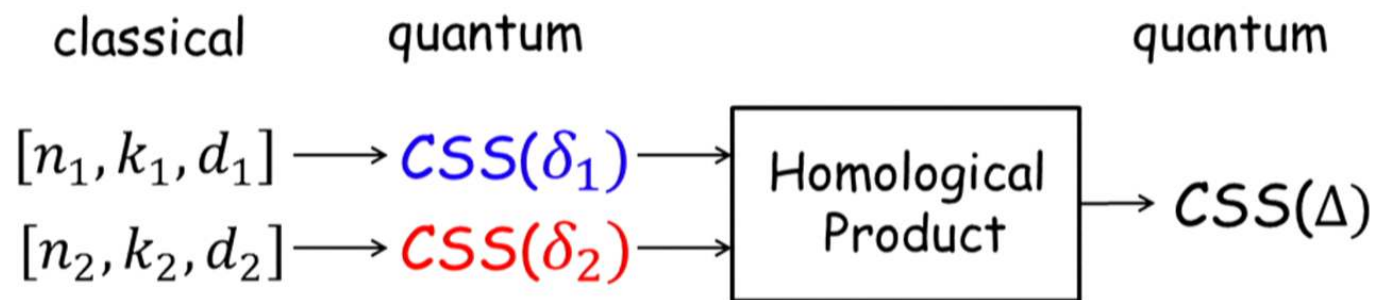
$$d^Z = \min\{ \text{wt}(f) : f \in \ker(\delta) \setminus \text{im}(\delta) \}$$

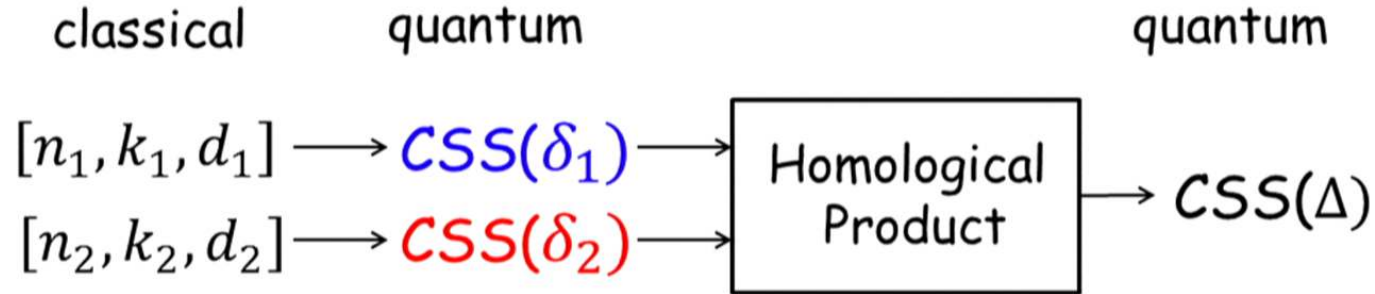
$$d^X = \min\{ \text{wt}(f) : f \in \ker(\delta^T) \setminus \text{im}(\delta^T) \}$$

**Lemma 1:**

$$\max[d_1^Z, d_2^Z] \leq d^Z \leq d_1^Z d_2^Z$$

$$\max[d_1^X, d_2^X] \leq d^X \leq d_1^X d_2^X$$





1<sup>st</sup> classical code: **Z-stabilizers** + **dummy X-stabilizers**

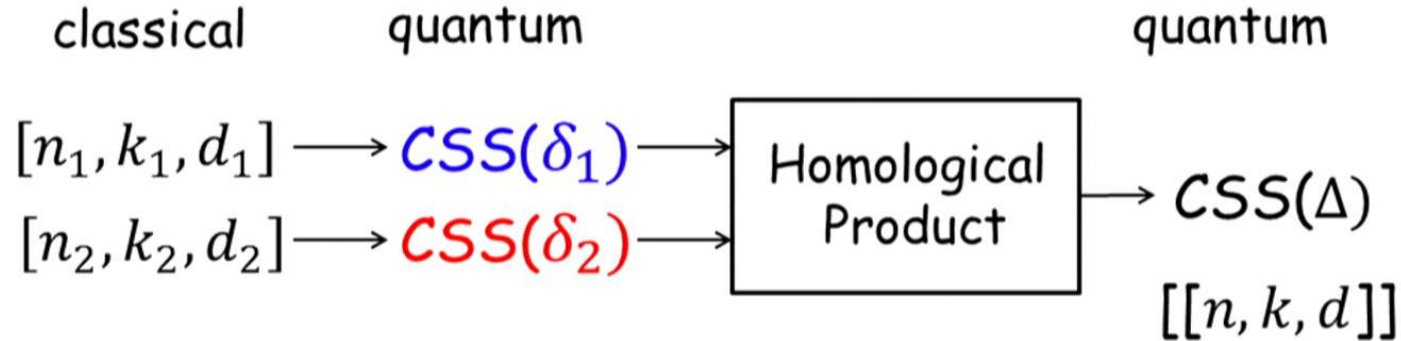
$CSS(\delta_1)$  has  $k_1$  logical qubits and distances

$$d_1^X = d_1 \quad d_1^Z = 1 \quad \text{Max degree} = W_1$$

2<sup>nd</sup> classical code: **X-stabilizers** + **dummy Z-stabilizers**

$CSS(\delta_2)$  has  $k_2$  logical qubits and distances

$$d_2^X = 1 \quad d_2^Z = d_2 \quad \text{Max degree} = W_2$$



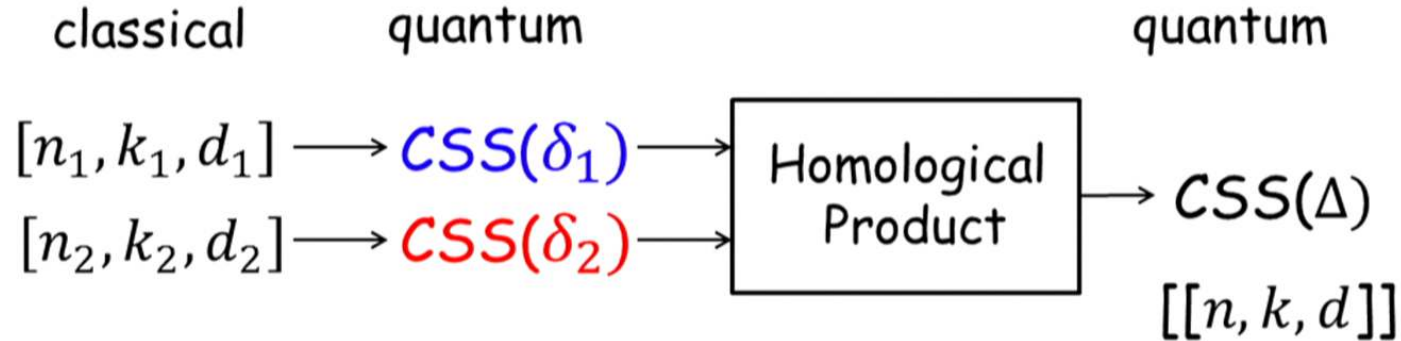
$$n = O(n_1 n_2)$$

$$k = k_1 k_2$$

$$d = \min [d^X, d^Z] = \min[d_1, d_2]$$

$$\text{Max degree: } W \leq W_1 + W_2$$

Choose inputs as good classical LDPC with  $n_1 = n_2$   
 Then  $k$  is linear in  $n$ ;  $d$  is linear in  $\sqrt{n}$  and  $W = O(1)$



$$n = O(n_1 n_2)$$

$$k = k_1 k_2$$

$$d = \min [d^X, d^Z] = \min[d_1, d_2]$$

$$\text{Max degree: } W \leq W_1 + W_2$$

Choose inputs as good classical LDPC with  $n_1 = n_2$

Then  $k$  is linear in  $n$ ;  $d$  is linear in  $\sqrt{n}$  and  $W = O(1)$

The output is quantum "almost good" LDPC

# OUTLINE

1. Quantum LDPC codes
2. Boundary operators and homological product
3. Tillich & Zemor construction
4. Homological product of two random codes
5. Open problems

## Why do we need randomness ?



Matching lower and upper bounds on the output distance.



Large gap between the lower and the upper bounds. Use randomness to derive stronger lower bounds which are valid only in a "typical case".

## Why do we need randomness ?



Matching lower and upper bounds on the output distance.



Large gap between the lower and the upper bounds. Use randomness to derive stronger lower bounds which are valid only in a "typical case".

## Some terminology:

Cycles	$\ker(\delta)$
Trivial Cycles	$\text{im}(\delta)$
Nontrivial Cycles	$\ker(\delta) \setminus \text{im}(\delta)$

### Some terminology:

Cycles	$\ker(\delta)$
Trivial Cycles	$\text{im}(\delta)$
Nontrivial Cycles	$\ker(\delta) \setminus \text{im}(\delta)$

Cocycles: same as cycles, but use  $\delta^T$  instead of  $\delta$

Distance of  $\text{CSS}(\delta)$  = minimum weight  
of a nontrivial cycle or cocycle.

Define **canonical boundary operator** with a fixed size  $M$  and a fixed homological dimension  $H$

$$\hat{\delta} = \begin{array}{|c|c|c|} \hline 0 & 0 & 0 \\ \hline 0 & 0 & \mathbf{I} \\ \hline 0 & 0 & 0 \\ \hline \end{array} \quad \begin{array}{l} \text{size}(\hat{\delta}) = M \\ H(\hat{\delta}) = H \end{array}$$

**Random ensemble** of boundary operators:

$$\delta = U\hat{\delta}U^{-1}$$

Here  $U$  is random invertible matrix picked uniformly.

Homological product of two random boundary operators:

$$\Delta = \delta_1 \otimes I + I \otimes \delta_2$$

$$\delta_1 = U \widehat{\delta}_1 U^{-1} \quad \delta_2 = V \widehat{\delta}_2 V^{-1}$$

Here  $U, V$  are random independent invertible matrices

The product code  $CSS(\Delta)$  has  $n = M^2$  physical qubits.

For any constant  $c > 0$  define a "low-weight" event:

$$E_c = \{\exists f \in \ker(\Delta) \setminus \text{im}(\Delta) : \text{wt}(f) < cM^2\}$$

It suffices to show that  $\Pr[E_c] < 1/2$  for small enough constants  $c, r > 0$  and for all large enough  $M$

$$\Delta = (U \otimes V) \hat{\Delta} (U^{-1} \otimes V^{-1})$$



Canonical bipartite boundary operator

$$\hat{\Delta} = \widehat{\delta}_1 \otimes I + I \otimes \widehat{\delta}_2$$

$$\ker(\Delta) = (U \otimes V) \ker(\hat{\Delta})$$

$$\text{im}(\Delta) = (U \otimes V) \text{im}(\hat{\Delta})$$

$$E_c = \{\exists f \in \ker(\Delta) \setminus \text{im}(\Delta) : \text{wt}(f) < cM^2\}$$

$$\Pr[E_c] \leq \sum_{R \geq 1} \Gamma(R) \cdot P(R)$$

$\Gamma(R)$  is the number of rank-  $R$  matrices in  $\ker(\hat{\Delta}) \setminus \text{im}(\hat{\Delta})$

$P(R)$  is the probability that a random rank-  $R$  matrix of size  $M$  has weight less than  $cM^2$

## Why the union bound fails ?

Intuition: if one of the input codes is bad, the product code has exponentially many low-weight cycles.

$$f = f_1 \otimes f_2 \quad \text{wt}(f) = \text{wt}(f_1) \cdot \text{wt}(f_2)$$

$$\text{wt}(f_1) < cM \quad \Longrightarrow \quad \text{wt}(f) < cM^2 \quad \text{for all } f_2$$

**Solution:** impose a stronger version of “low-weight” condition which cannot be satisfied if only one of the input codes is bad.

**Definition:**

A matrix  $f$  of size  $M$  has **Uniform Low Weight** with a constant  $c$  iff **each row** and **each column** of  $f$  has **weight at most  $cM$**

For any constant  $c > 0$  define a ULW event:

$$E'_c = \{ \exists f \in \ker(\Delta) \setminus 0 : f \text{ has ULW}(c) \}$$

**Pigeonhole principle:**

if  $f$  is a matrix of size  $M$  with weight at most  $cM^2$  then  $f$  contains a submatrix  $f'$  of size  $M'$  which has  $ULW(c')$

$$M' \approx M \text{ and } c' \approx c$$

$$E'_{c,\gamma} = \{ \exists f \in \ker(\Delta) \setminus 0 : f_\gamma \text{ has ULW}(c) \}$$

$$\Pr[E'_{c,\gamma}] \leq \sum_{R \geq 1} \Gamma(R) \cdot P(R)$$

the sum is exponentially small in  $M$  ... 😊

$\Gamma(R)$  is the number of rank- $R$  submatrices  $f_\gamma$  that can be extended to a cycle  $f \in \ker(\Delta)$

$P(R)$  is the probability that a random rank- $R$  matrix of size  $M'$  has ULW( $c$ )

These quantities are (slightly less) easy to compute 😊

## Open Problems

- Does the product of two random codes achieves quantum Gilbert-Varshamov bound ?
- Prove that the product of  $m$  random codes is good (whp) for  $m=O(1)$ . This implies existence of good quantum codes with  $W = n^\varepsilon$  for any  $\varepsilon > 0$
- Can we reduce stabilizer weight from  $n^\varepsilon$  to  $O(1)$  without harming the distance too much ? Construct quantum LDPC codes with a super-sqrt distance.
- Can we describe encoding circuits for  $m$ -fold homological product codes as MERA ?

## Open Problems

- Does the product of two random codes achieves quantum Gilbert-Varshamov bound ?
- Prove that the product of  $m$  random codes is good (whp) for  $m=O(1)$ . This implies existence of good quantum codes with  $W = n^\varepsilon$  for any  $\varepsilon > 0$
- Can we reduce stabilizer weight from  $n^\varepsilon$  to  $O(1)$  without harming the distance too much ? Construct quantum LDPC codes with a super-sqrt distance.
- Can we describe encoding circuits for  $m$ -fold homological product codes as MERA ?

## Open Problems

- Does the product of two random codes achieves quantum Gilbert-Varshamov bound ?
- Prove that the product of  $m$  random codes is good (whp) for  $m=O(1)$ . This implies existence of good quantum codes with  $W = n^\varepsilon$  for any  $\varepsilon > 0$
- Can we reduce stabilizer weight from  $n^\varepsilon$  to  $O(1)$  without harming the distance too much ? Construct quantum LDPC codes with a super-sqrt distance.
- Can we describe encoding circuits for  $m$ -fold homological product codes as MERA ?

## Open Problems

- Does the product of two random codes achieves quantum Gilbert-Varshamov bound ?
- Prove that the product of  $m$  random codes is good (whp) for  $m=O(1)$ . This implies existence of good quantum codes with  $W = n^\varepsilon$  for any  $\varepsilon > 0$
- Can we reduce stabilizer weight from  $n^\varepsilon$  to  $O(1)$  without harming the distance too much ? Construct quantum LDPC codes with a super-sqrt distance.
- Can we describe encoding circuits for  $m$ -fold homological product codes as MERA ?

## Open Problems

- Does the product of two random codes achieves quantum Gilbert-Varshamov bound ?
- Prove that the product of  $m$  random codes is good (whp) for  $m=O(1)$ . This implies existence of good quantum codes with  $W = n^\varepsilon$  for any  $\varepsilon > 0$
- Can we reduce stabilizer weight from  $n^\varepsilon$  to  $O(1)$  without harming the distance too much ? Construct quantum LDPC codes with a super-sqrt distance.
- Can we describe encoding circuits for  $m$ -fold homological product codes as MERA ?