Quantum LDPC codes
Lecture 4

Nicolas Delfosse
Microsoft

PCMI Summer School 2023
July 28th 2023

Overview

- Brief overview of quantum Tanner code
- Conclusion: Should we abandon surface codes?

Quantum Tanner codes

Some constructions of QLDPC codes

Topological codes:

- 1997: Kitaev. $d = \Omega(\sqrt{n})$ but $k = 1$.
- 2002: Freedman, Meyer, Luo $d = \Omega\left(\sqrt{n\sqrt{\log n}}\right)$
- 2009: Bravyi, Poulin, Terhal bound: $kd^2 \leq$ constant $\times$ n

Hypergraph-product codes and generalizations:

- 2009: Tillich, Zémor. HGP with $k \propto n$ $d = \Omega(\sqrt{n})$
- 2013: Bravyi, Hastings. Homological products
- 2020: Hastings, Haah, O'Donnell: Fiber bundle codes $d = \Omega\left(\frac{n^{\frac{3}{5}}}{polylog}\right)$
- 2020: Panteleev, Kalachev: Lifted products $d = n^{1-\varepsilon}/\log n$
- 2020: Breuckmann and Eberhardt: Balanced products $d = \Omega(n^{\frac{3}{5}})$

Decoder for good LDPC codes

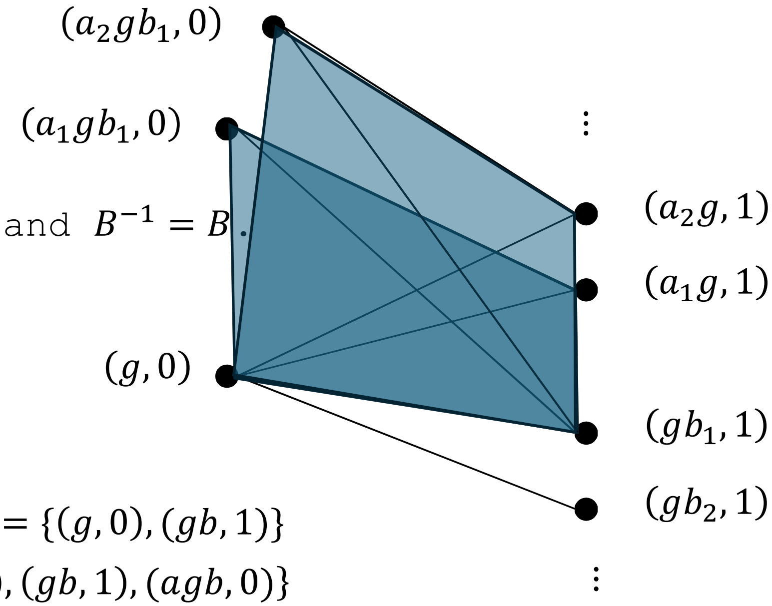
Good LDPC codes:

- 2021: Panteleev and Kalachev. Good QLDPC codes
- 2021: Dinur, Evra, Livne, Lubotzky, and Mozes. LTC codes
- 2022: Leverrier, Zémor

Linear time decoders for quantum Tanner codes:

- 2022: Gu, Pattison, Tang
- 2022: Dinur, Hsieh, Lin, VIdick
- 2022: Leverrier, Zémor

Left-Right Cayley Complex



Input:

- A finite group G
- Two subsets A, B of G such that $A^{-1} = A$ and $B^{-1} = B$.

Output:

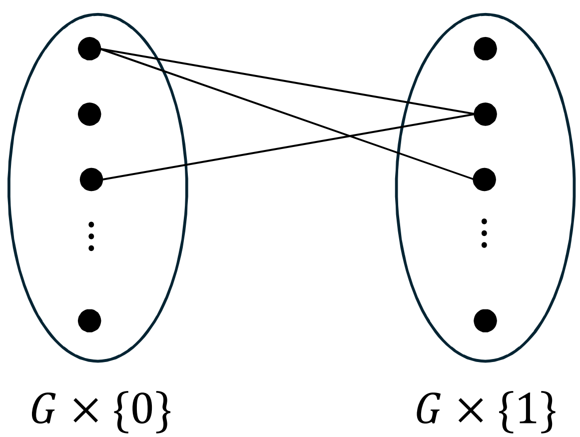
A complex $X = (V, E, F)$ where:

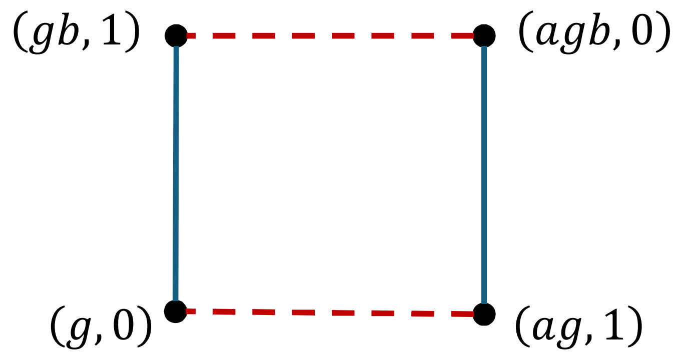
- $V = V_0 \cup V_1$ where $V_i = G \times \{i\}$
- $E = E_A \cup E_B$ where $E_A = \{(g,0),(ag,1)\}$ and $E_B = \{(g,0),(gb,1)\}$
- $F =$ set of squares $f(g,a,b) \coloneqq \{(g,0),(ag,1),(gb,1),(agb,0)\}$

Local structure

$G = \{g_1, g_2, \dots\}$
$A = \{a_1, a_2, \dots\} \subseteq G$
$B = \{b_1, b_2, \dots\} \subseteq G$

$V =$





Type A edge:

$a \times \cdot$

Type B edge:

$\cdot \times b$

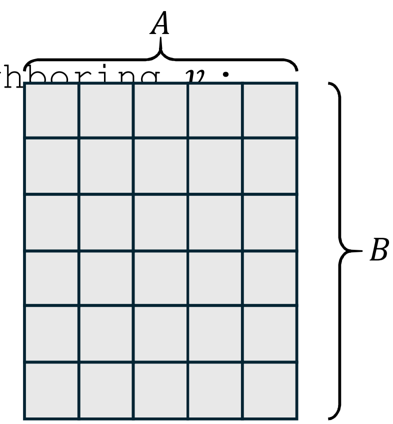
Neighborhood of a vertex

Consider $v = (g, 0)$

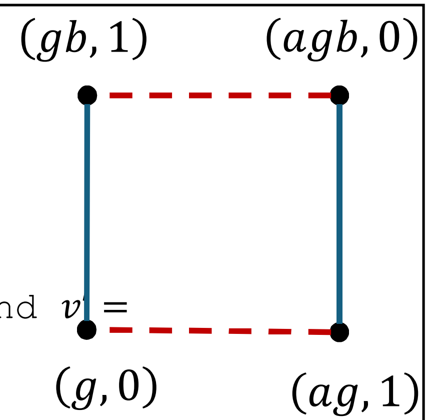
- Neighboring vertices: $(ag, 1)$ with $a \in A$ and $(gb, 1)$ for $b \in B$
- Neighboring faces: $\{(g,0),(ag,1),(gb,1),(agb,0)\}$ for each pair $(a,b) \in A \times$ B.

Abstract representation the faces neighboring v:

$F(v) = A \times B =$



Intersection of two neighborhoods



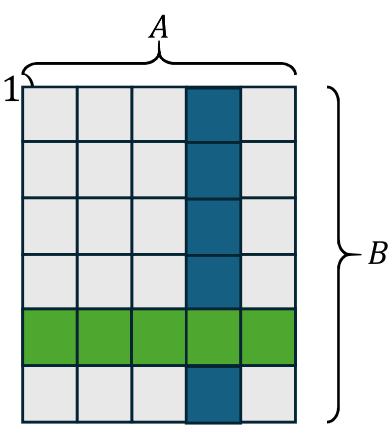
Question. What is $F(v) \cap F(v')$ for two vertices $v = (g,0)$ and $v' = (g',1)$?

- If $F(v) \cap F(v') \neq \emptyset$, then v and v' must share an edge.
- Why?

- If they share a type A edge: $v = (g,0)$ and $v' = (ag,1)$
- Then $F(v) \cap F(v')$ is the set of faces:

  $\{(g,0),(ag,1),(gb,1),(agb,0)\}$ for $b \in B$

$F(v) \cap F(v') = B =$



- If they share a type B edge:

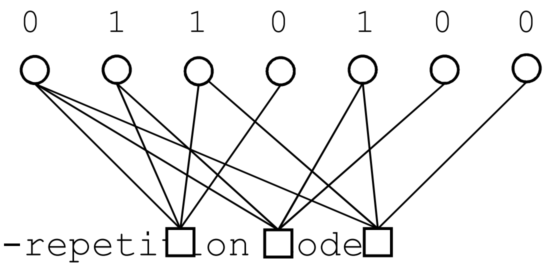
Tensor codes of two classical codes

Def. A codeword of $C_1 \otimes C_2$ is bitstring forming a $n_1 \times n_2$ matrix x such that

- each column of x is in C_1,
- each row of x is in C_2,

Ex.

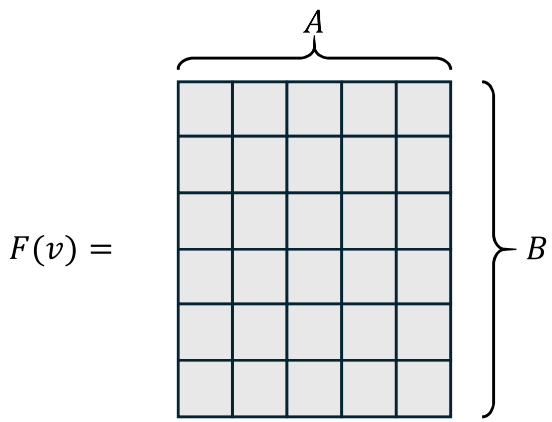
$$\begin{matrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{matrix}$$



is in the product of the Hamming code and the 3-repetition code

Prop. The code $C_1 \otimes C_2$ has parameters $[n_1 n_2,\ k_1 k_2]$.

Definition of quantum Tanner codes



- Select a finite group G.
- Select $A, B \subseteq G$ such that $A^{-1} = A$ and $B^{-1} = B$.
- Select two codes C_A and C_B with length $|A|$ and $|B|$.

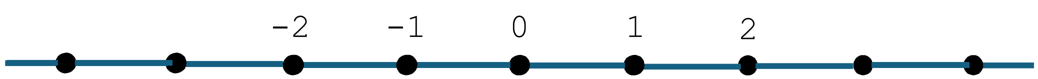
- Place a qubit on each face of the left-right Cayley complex (V, E, F)
- For each $v = (g, 0)$, for each $c \in C_A \otimes C_B$, define a X generator on $F(v)$ acting on the support of c.
- For each $v = (g, 1)$, for each $c \in C_A^{\perp} \otimes C_B^{\perp}$, define a Z generator on $F(v)$ acting on the support of c.

Prop. The generators commute because $F(v) \cap F(v')$ is either empty, or a row of $F(v)$ or a column of $F(v)$.

The sets must satisfy the TNC condition for all a, g, b: $ag \neq gb$

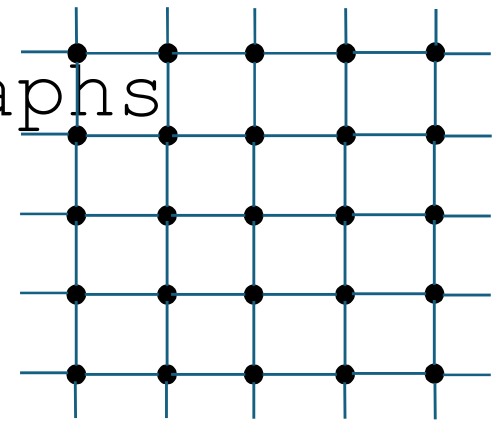
Example of Cayley graphs

- $G = \mathbb{Z}$,
- $A = \{\pm 1\}$

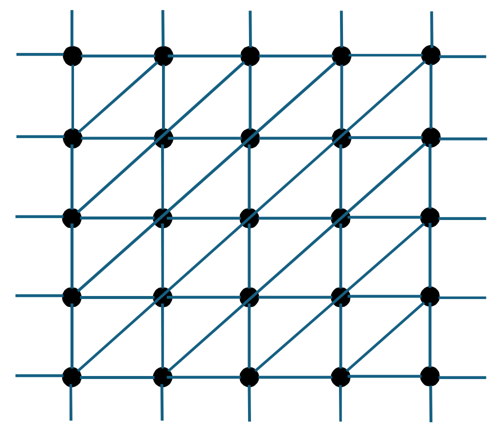


Example of Cayley graphs

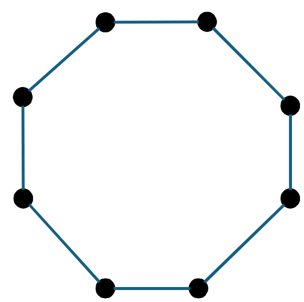
- $G = \mathbb{Z}^2, A = \{(\pm 1,0), (0, \pm 1)\}$



- $G = \mathbb{Z}^2, A = \{(\pm 1,0), (0, \pm 1), (\pm 1, \pm 1)\}$



- $G = \mathbb{Z}_8, A = \{\pm 3\}$



Why do we need $A = A^{-1}$?

Double cover of a Cayley graph

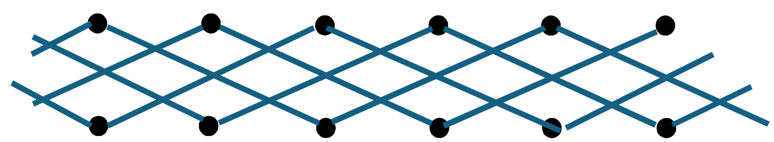
It is the graph with

- $V = V_0 \cup V_1$ with $V_0 = G \times \{0\}$ and $V_1 = G \times \{1\}$
- Two types of edges: $\{(g, 0), (ag, 1)\}$ and $\{(g, 1), (ag, 0)\}$

Ex. $G = \mathbb{Z}, A = \{\pm 2\}$

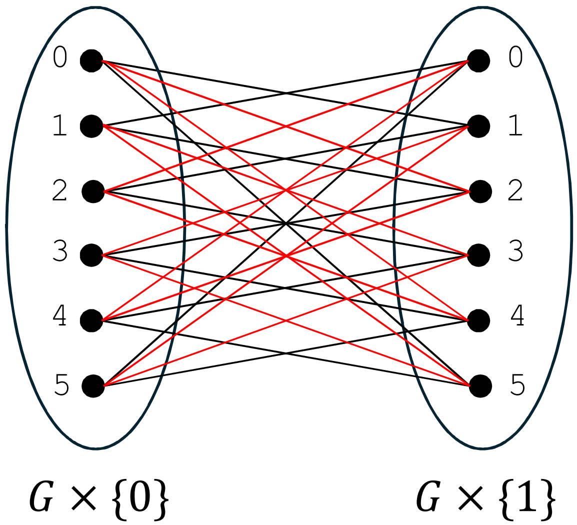
$G \times \{0\} =$

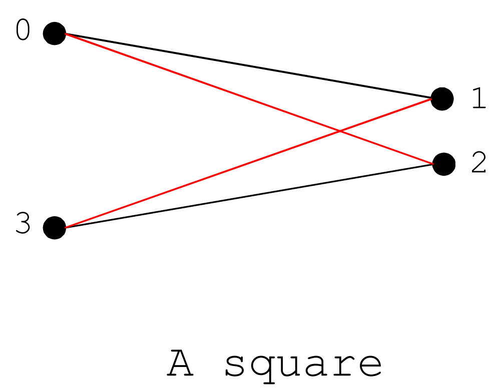
$G \times \{1\} =$



Example

$G = \mathbb{Z}_6, \mathrm{A} = \{\pm 1\}, B = \{\pm 2\}$





Example - $G = \mathbb{Z}_9$

$G = \mathbb{Z}_9, A = \{\pm 1\}, B = \{\pm 2\}$

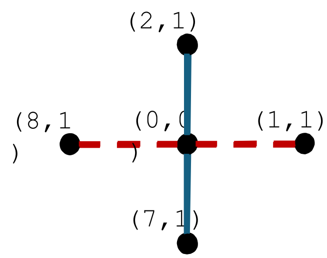
Type A edge:

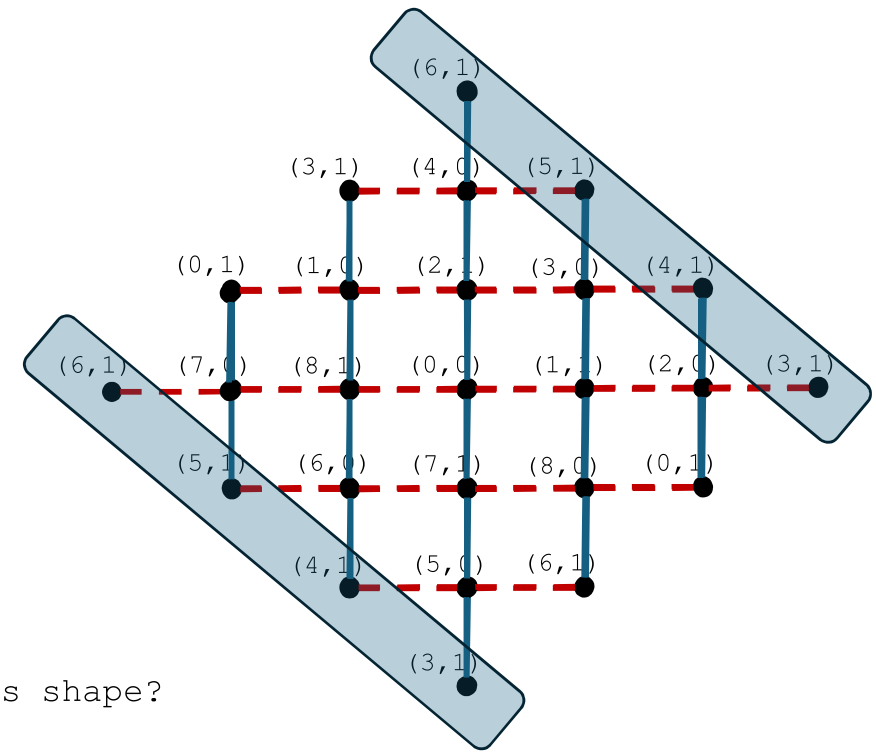
$(+1, \text{flip})$

$(-1, \text{flip})$

Type B edge:

$(+2, \text{flip})$ $(-2, \text{flip})$

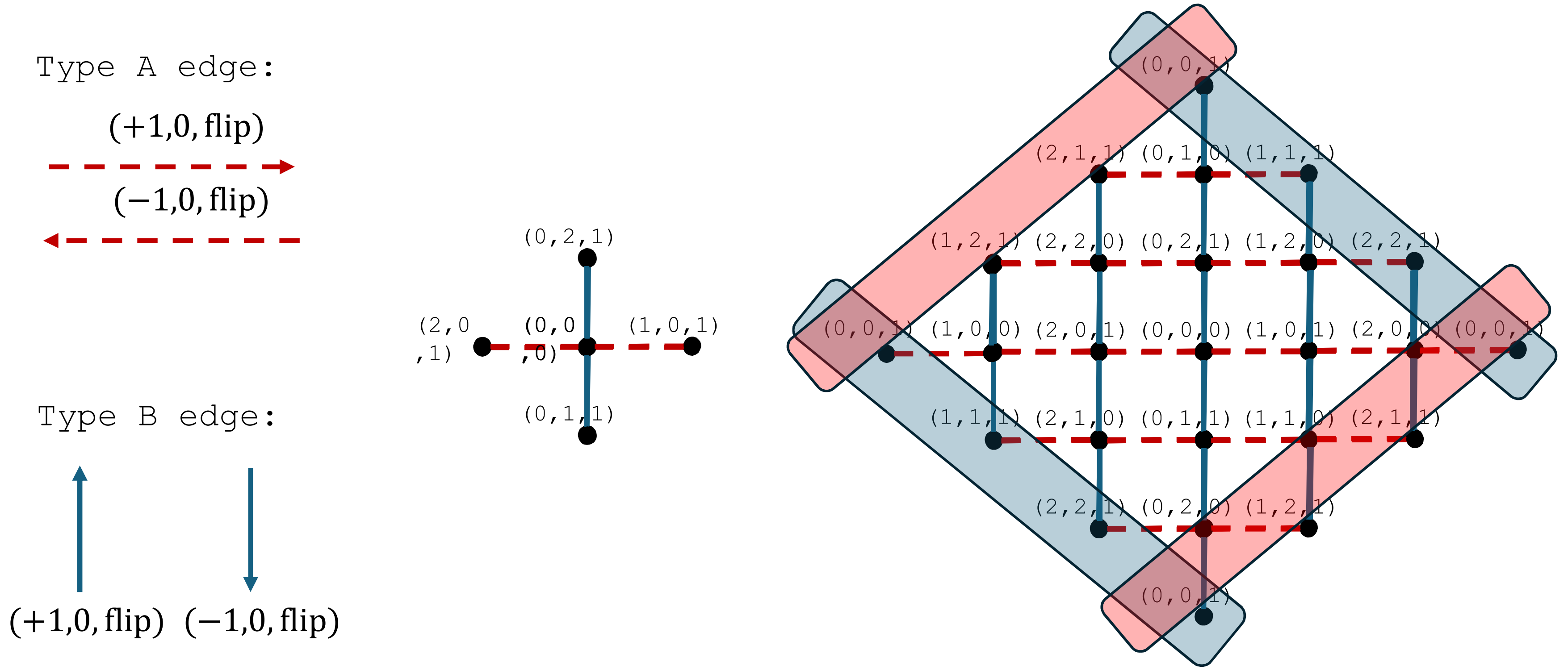




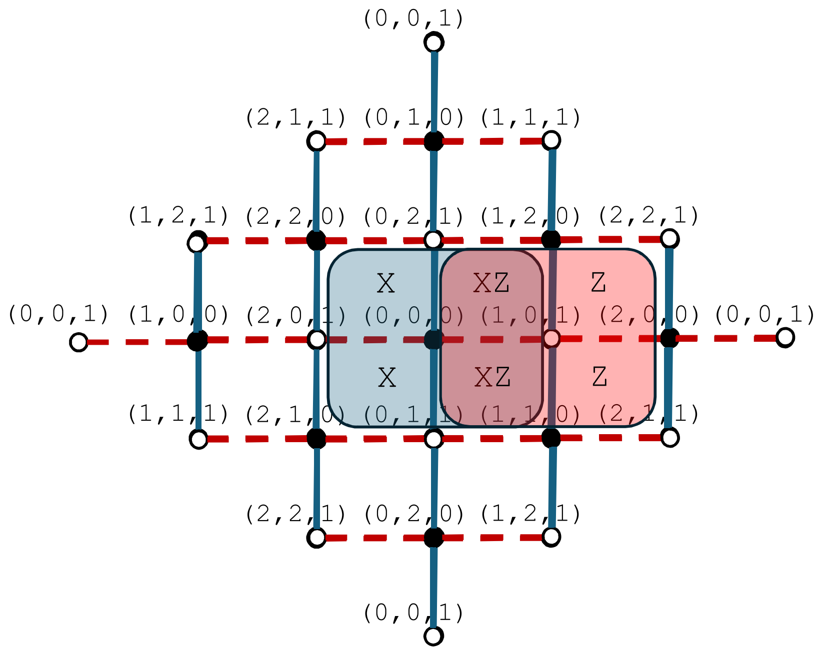
What is this shape?

Example - $G = \mathbb{Z}_3 \times \mathbb{Z}_3$

$G = \mathbb{Z}_3 \times \mathbb{Z}_3, A = \{(\pm 1, 0)\}, B = \{(0, \pm 1)\}$



Example - $G = \mathbb{Z}_3 \times \mathbb{Z}_3$



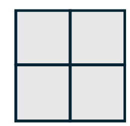
We recover the toric code.

Construction:

- Qubits are on faces
- For $v = (g, 0)$, $c \in C_A \otimes C_B$, define a X generator on $F(v)$ acting on the support of c.
- For $v = (g, 1)$, $c \in C_A^{\perp} \otimes C_B^{\perp}$, define a Z generator on $F(v)$ acting on the support of c.

● $= (g, 0) =$ X stabilizer generators

$F(v) = A \times B =$



We need to a tensor code $C_A \otimes C_B$ on $A \times B$:

$\Rightarrow C_A = C_B = \{00, 11\}$

$C_A \otimes C_B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

$\Rightarrow$ X stabilizer generator: $\begin{bmatrix} X & X \\ X & X \end{bmatrix}$

How to get good LDPC codes

Take:

- $G = \mathrm{PSL}_2(q^i)$
- C_A = random code
- C_B = random code

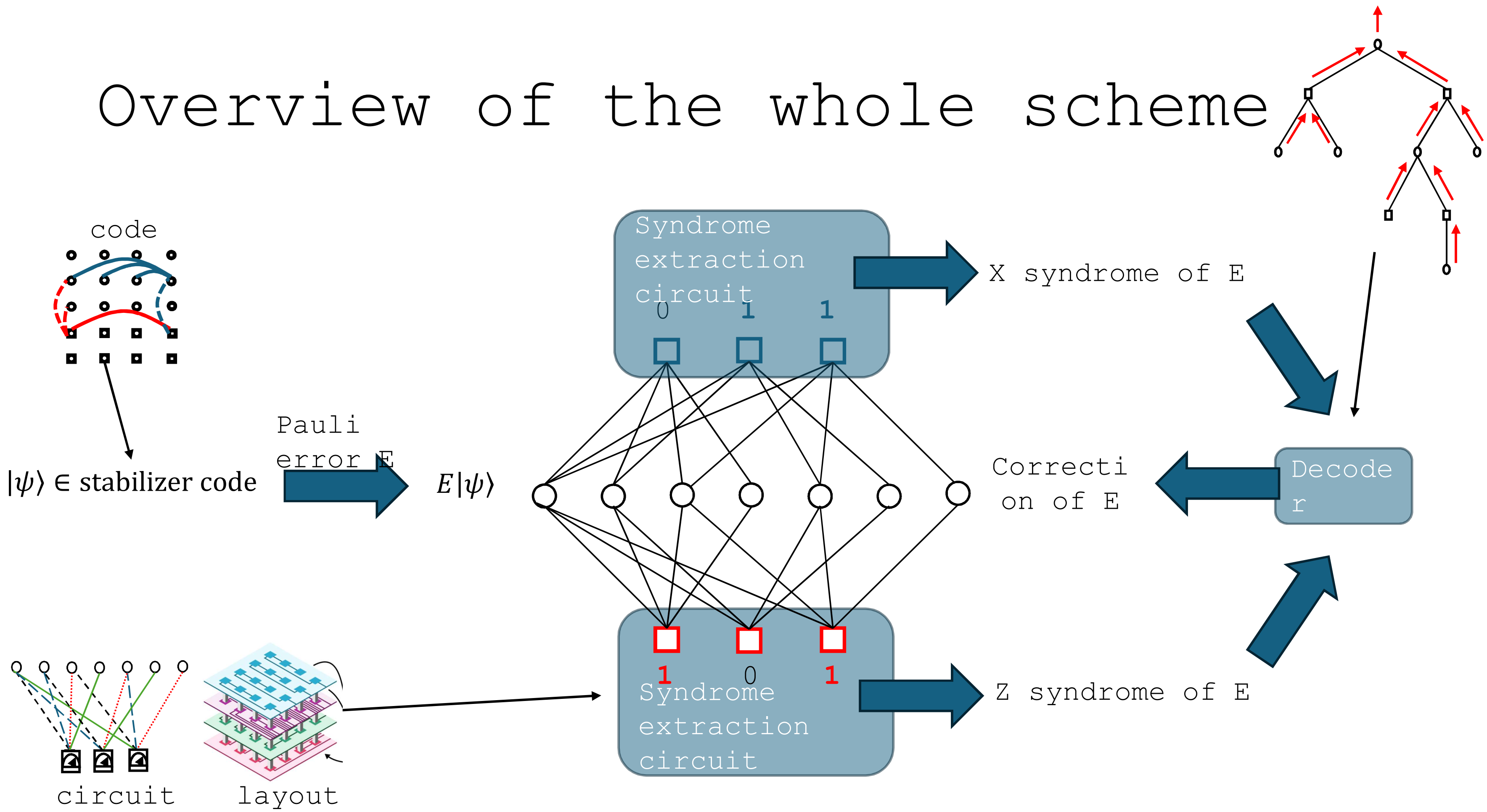
This leads to a family of good quantum LDPC codes.

Question:

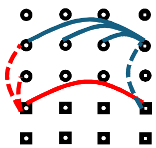
Should we all replace our codes by good quantum LDPC codes?

Conclusion

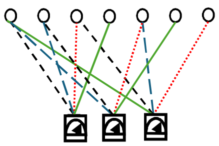
Overview of the whole scheme



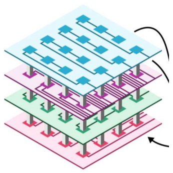
Overview of the whole scheme



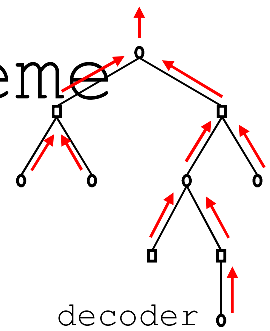
code



circuit



layout



decoder

Select two random Tanner graphs with
- 4s bits with degree 3.
- 3s checks with degree 4.
- girth ≥ 8

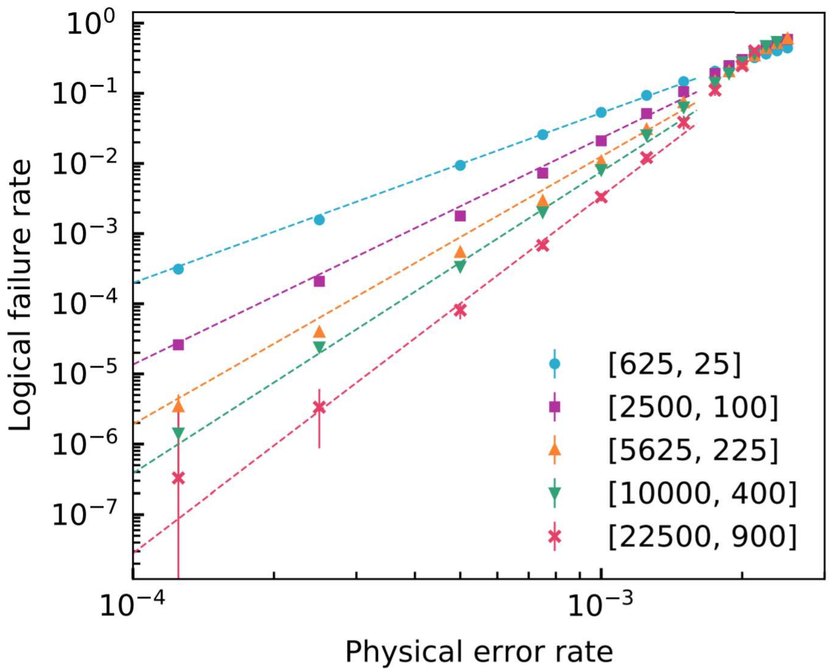
Construct their HGP.
- Estimate the performance of the HGP code using the SSF decoder.
- Select the best HGP

- Compute the Tanner graph T of the code.
- Compute an edge coloration of T
- Construct the color-based syndrome extraction circuit.

- Compute a layered decomposition of the Tanner graph.
- Compute an edge coloration of T
- Construct the color-based syndrome extraction circuit.

- We use BP for decoding in a single shot manner.
- We estimate the logical error rate over 10 rounds of syndrome extraction.
- To check if a logical error occurs, we use SSF decoder to correct the residual

Numerical results



Noise threshold:

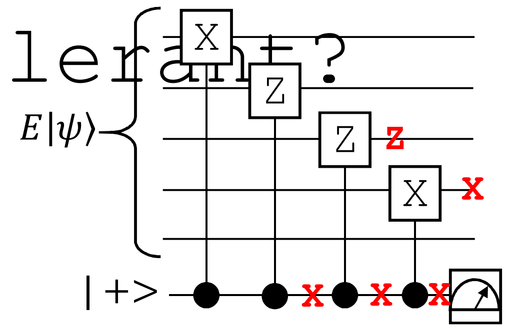
0.28% (instead of 0.7% for surface codes)

physical qubits per logical qubit:

49 (instead of thousands for surface codes)

Logical failure rate	10^{-9}	10^{-12}	10^{-15}
Logical qubits	1600	6400	18 496
Surface code physical qubits	387 200	2 880 000	13 354 112
HGP code physical qubits	78 400	313 600	906 304
Improvement using HGP codes	4.94×	9.18×	14.73×

Is our scheme fault-tolerant?



Syndrome extraction:

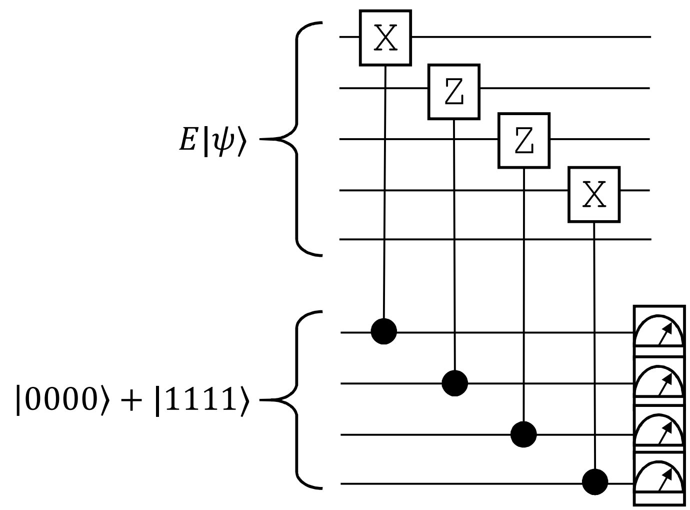
- What is this circuit?
- Are there ‘bad’ faults for this circuit?
- What is the effect of a X fault on the ancilla qubit?
- Can we avoid that?
- Should we avoid that?

Decoder:

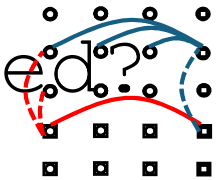
- BP corrects each qubits independently based on marginal probability. Is it a problem?
- The decoder uses noisy syndrome data. Is it a problem?

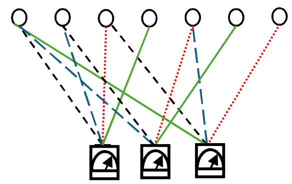
Conclusion:

- Practical FT ≠ Theoretical FT

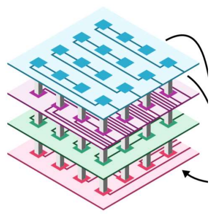


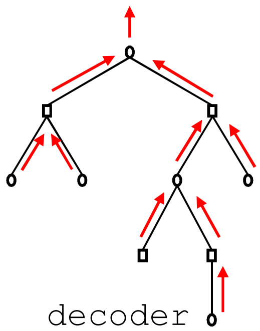
What could be improved?





1. Improve the code:
   - linear distance,
   - reduced code length,
   - denser family.
2. Improve the circuit:
   - the circuit is not FT (reduced distance).
3. Improve the decoder:
   - better logical error rate,
   - linear complexity,
   - hardware optimization.
4. Improve the simulation:
   - Refine the numerical estimate of the logical error rate.
   - Simulate longer lifetime.





What about computation?

- 2013: Gottesman - Fault-Tolerant Quantum Computation with constant overhead.
- Other proposals for fault-tolerant logical gates in QLDPC codes[1,2,3,4].

(c)

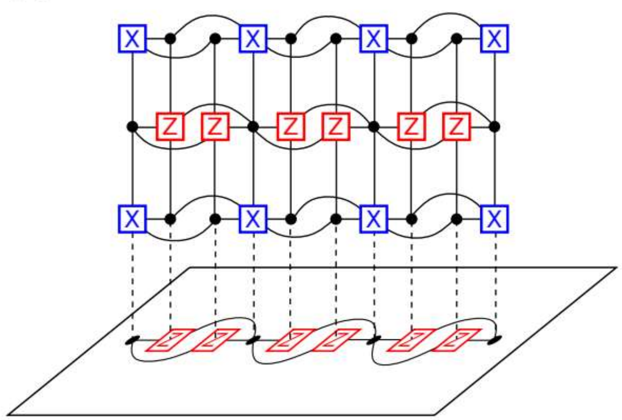
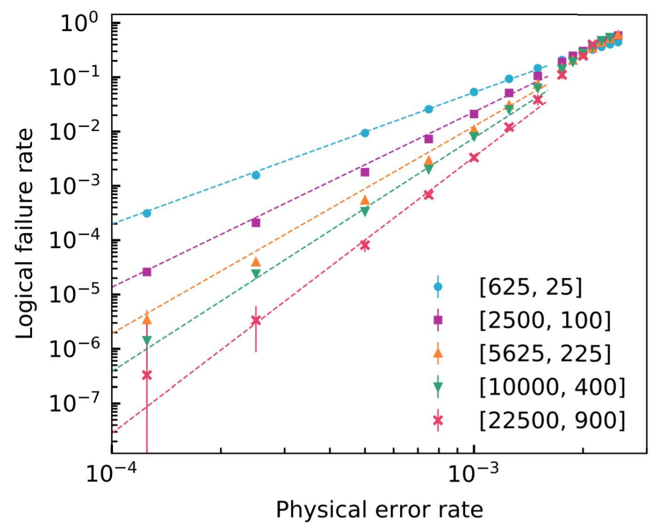


Figure from ref 3.

1. Jochym-O'Connor, arxiv:1807.09783
2. Krishna, Poulin, arxiv:1909.07424
3. Cohen, Kim, Bartlett, Brown, arxiv: 2110.10794
4. Breuckmann, Burton, arxiv:2202.06647

What could go wrong with this approach?

- Noise could be correlated.
- Noise could be non-Pauli.
- We may be unable to build sufficiently reliable hardware (need $p = 10^4$).
- The blocks could be too big (we need $n = 900{,}000$).
- The decoder could be too slow.
- Fault-tolerant operations may be expensive.
- We may be unable to build the required long-range connections.
- We may need too many long-range connections.
- Building insulated layers of long-range connections may be hard.



Logical failure rate	10^{-9}	10^{-12}	10^{-15}
Logical qubits	1600	6400	18 496
Surface code physical qubits	387 200	2 880 000	13 354 112
HGP code physical qubits	78 400	313 600	906 304
Improvement using HGP codes	4.94×	9.18×	14.73×

Other encoding strategies

Now what?

Should we abandon surface codes?

Hyperbolic codes:

- Higgott, Breuckmann (2020)
- Breuckmann, Vuillot, Campbell, Krishna, Terhal (2017)

Floquet codes:

- Haah, Hastings (2021)

Spacetime code:

- Delfosse, Paetznick (2023)

Appendix - History of classical LDPC codes

Brief (and biased) history

- Asymptotic results: Shannon (1940’s)
  - Channel capacity: If we use a channel an infinite number of times, what is the maximum number of bits of information that we can send per use of the channel?
  - Basic idea: Random codes are optimal.
  - Problem: How to encode? How to decode?

- Birth of modern coding: Elias and Gallager (1960’s)
  - Linear codes perform as well as random codes but encoding is easy.
  - Convolutional codes too.
  - Erasure channel as a toy model.
  - LDPC codes.

Brief (and biased) history

- The comeback of modern coding: Berrou, Mackay, Neal, Richardson, Urbanke, Shorkollahi, … (1990’s):
  - Turbo codes
  - LDPC codes
  - Decoding is easy! But is it optimal?
- Capacity achieving codes.
  - Proofs for the erasure channel first.
  - Irregular LDPC codes.
  - Spatially-coupled codes achieve capacity (Kudekar, Richardson, Urbanke 2013).
- Today LDPC codes are in your cell phone, your laptop, your WiFi…

How far are we from the classical story?

Classical goal:

- Achieve capacity with a linear time decoder.

Def. The capacity of a channel N is the maximum rate $\frac{k}{n}$ of a family of codes with vanishing logical error rate.

Quantum goal:

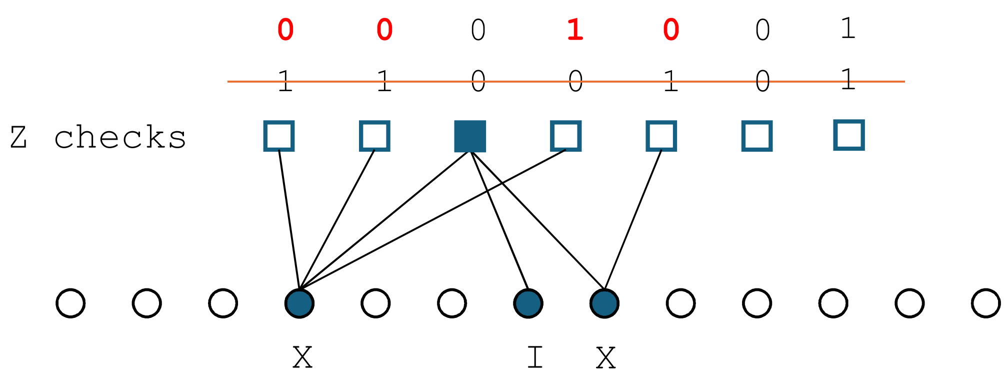
- Achieve capacity?
- Build a fault-tolerant quantum computer?

We can still learn form the classical case: For instance, starting with the erasure channel.

Appendix - Small Set Flip (SSF) decoder

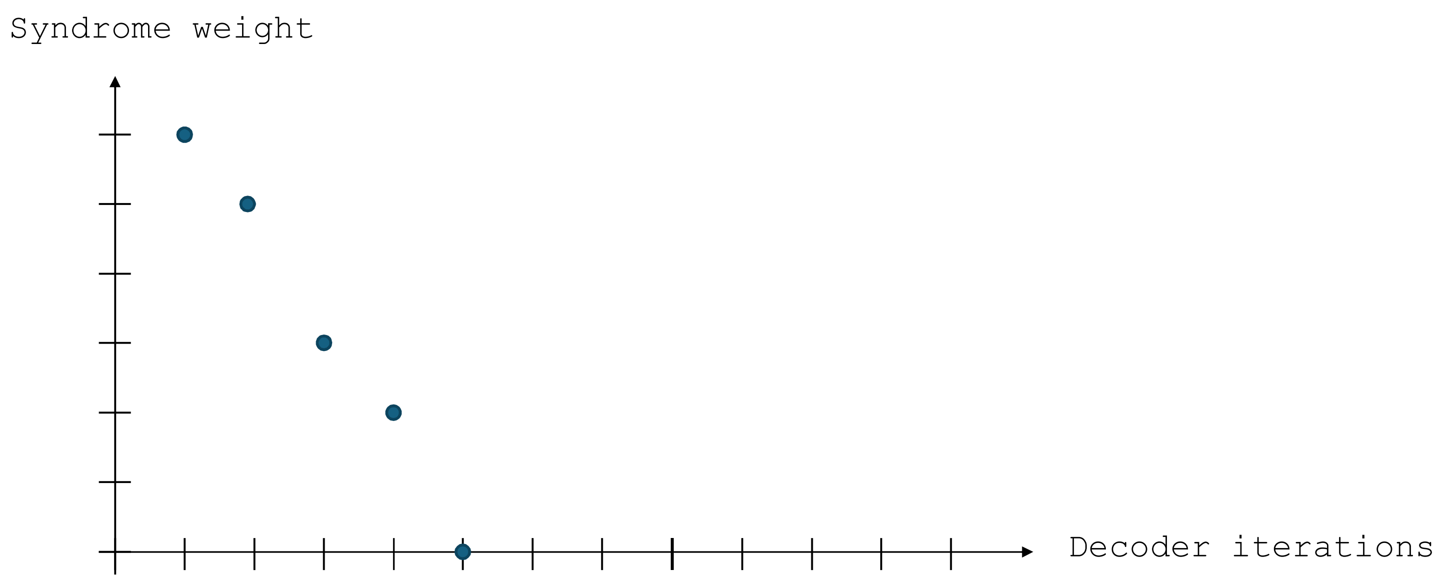
Leverrier, Tillich, Zémor - arXiv:1504.00822 (2015)

Small Set Flip decoder – Basic idea



1. Select a Z check
2. Select an error E_X inside the Z check that reduces the syndrome weight.
3. Update the syndrome

Small Set Flip decoder – Basic idea



Leverrier, Tillich, Zémor – arXiv:1504.00822 (2015)

Small set flip decoder

Def: A *critical generator* g is a Z stabilizer generator that contains a X error that reduces the weight of the syndrome.

Input: A syndrome value $s_c = 0$ or 1 for each Z check node.

Output: A correction for X errors.

1. While there exists a critical generator g:
2. Select an error $E_X(g)$ included in g such that $\frac{weight\ reduction}{|E_X(g)|}$ is maximum.
3. Update the syndrome: Add s($E_X(g)$) to the syndrome.
4. Return the product of all the $E_X(g)$.

Theorem. [Leverrier, Tillich, Zémor, 2015]. Under some conditions about the expansion of the two input graphs, *the small set flip decoder for HGP codes corrects any set of* $O(\sqrt{\ }$

Small set flip decoder - Complexity

Complexity: $O(2^w n)$

Notation:

- n = code length.
- w = max. degree of a check (max. weight of a stabilizer generator).

Remark:

- Linear-time complexity for bounded degree Tanner graphs.
- May be slow in practice for large w.