

# Locality of Small-Set-Flip Decoder.

David Ponnarovsky

July 3, 2025

# Introduction

## Last Time:

- ▶ Quantum Expanders + original fault tolerance gives an almost  $\mathbf{QNC}_1 = \text{noisy-}\mathbf{QNC}_1$ .
- ▶ Michael: Error decomposition into clustering happens in any LDPC code + local decoder that achieves error reduction w.h.p. exists for the  $4D$ -toric.
- ▶ Dorit: The error reduction statement should be checked, particularly, what's the structure of such a lemma when the decoding circuit is subjected to noise.

## Today:

- ▶ More about Noise,  $p$ -local noise  $\leftrightarrow^1 (p', q')$ -initial error per correction cycle.
- ▶ Formal statement, of the decoding theorem.
- ▶ A bit on the locality of the algorithm.

---

<sup>1</sup>When using the LDPC codes

# Nosiy Circuit.



## $(p', q)$ -Simplified Model.

### Definition (Local Stochastic Noise.)

Denote by  $E$  the subset of faulty qubits. We say that an error model behaves according to the local stochastic noise if:

$$\Pr[|E| = t] \leq O(p^t)$$

for some  $p \in (0, 1)$ . For example, a depolarizing channel is a local stochastic noise.

### Definition

Let  $p', q \in (0, 1)$  and let  $C$  be an error correction code. The decoding problem in the  $(p', q)$ -**Simplified Model** is defined as finding (a correction to) error  $E$ , promised the qubits are subjected to local stochastic noise  $p$ , and given syndrome measurement subjected to local stochastic noise  $q$ . We will denote by  $D$  the faulty syndrome bits.

## $(p', q)$ -Simplified Model.

### Claim.

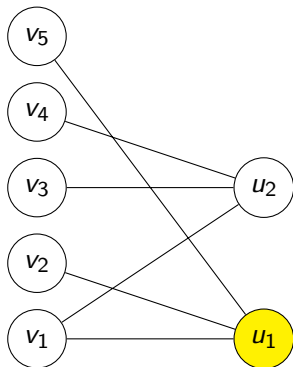
Assume that  $C$  is an LDPC code, and let  $D$  be a decoding algorithm which first measures the syndrome and then decode (guess a correction).

Then, for any  $p \in (0, 1)$ , there are  $p', q \in (0, 1)$  (functions of  $p$  and the 'locality'<sup>2</sup> of  $C$ ) such that the running of  $D$  according to the standard  $p$ -noise is equivalent to its running when subjected to the  $(p', q)$ -Simplified Model. [gottesman2014]

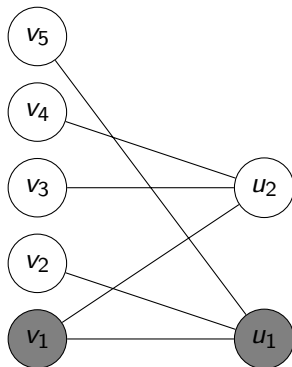
---

<sup>2</sup>degree in the Tanner graph of  $C$ .

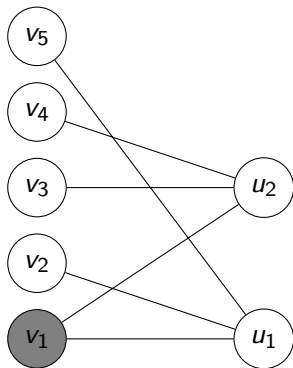
standard model,  $t = 0$



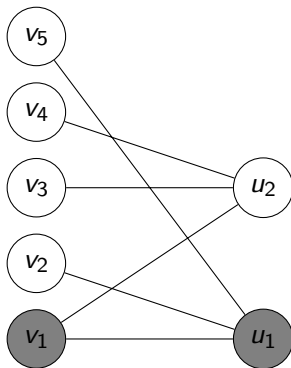
simplified  $(p', q)$ -model



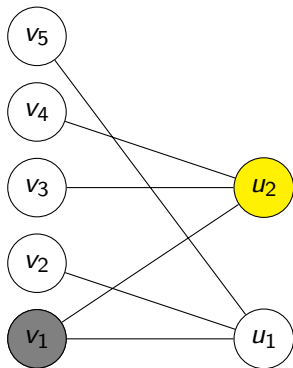
standard model,  $t = 1$



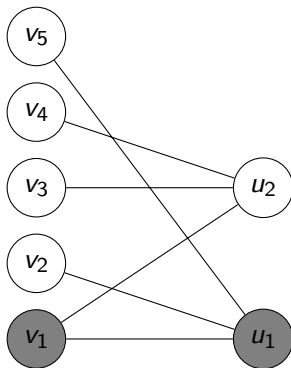
simplified  $(p', q)$ -model



standard model,  $t = 2$



simplified  $(p', q)$ -model





# Reducing error formal statement.

## Claim.

There exist two non-zero constants  $p_1, p_2 > 0$  such that the following holds. Suppose the pair  $(E, D)$  satisfies a local stochastic noise model with parameter  $(p_{\text{phs}}, p_{\text{syn}})$  where  $p_{\text{phs}} < p_1, p_{\text{syn}} < p_2$ . If we run the parallel decoder with constant number of steps  $f_0$ , then there exists a random variable  $E' \subset V_Q$  (qubits) with a local stochastic distribution with parameter  $p' = p_1^c$  (for some constant  $c$ ) and such that:

$$\Pr \left[ E' \neq E \otimes \hat{E} \right] \leq e^{\Theta(\sqrt{n})}$$

Where  $\hat{E}$  is the estimated error computed by the decoder.


## Decoder. (Simplified version).

Look for a 'small set'  $F$  of qubits such that:

1.  $F$  contained in the support of some  $X$ -type stabilizer.
2.  $F$  touched many unsatisfied  $Z$ -type stabilizer. Or, flipping  $F$ , decrease the  $Z$ -type syndrome.

For parallelizing the decoder, we color the check nodes in the Tanner graph such that no two checks of the same color share a bit.<sup>3</sup> Then, in the  $i$ th iteration, we look in parallel over all  $X$ -type stabilizers at the  $i$ th color.

---

<sup>3</sup>Since the code is LDPC, we can do it with  $O(1)$  colors. 

# Locality.

## Definition (Execution Support.)

Denote by  $U = E \cup F_1 \cup F_2, \dots, F_m$  the execution support, the combination of faulty qubits and the qubits flipped by the decoder.

## Claim.

For any set  $K \subset U$  with  $\Gamma_Q(K) \cap \Gamma_Q(U/K) = \emptyset$  there is a valid execution of the Decoder, on the input  $(E \cap K, D \cap \Gamma_X(K))$  whose output is  $\hat{E} \cap K$  and whose support is  $U \cap K$ .

4

---

<sup>4</sup>An execution might change upon the order of the small set being chosen, yet notice that for small errors, the algorithm is always correct.

## Definition

$\alpha$ -subset, and  $\text{MaxConn}_\alpha$ . (Simplified<sup>5</sup>) Let  $G$  be a graph. Let  $X, Y \subset \mathcal{V}$  and  $\alpha \in (0, 1]$ .  $X$  is said to be an  $\alpha$ -subset of  $Y$  if  $|X \cap Y| \geq \alpha|X|$ . In addition we define:

$$\text{MaxConn}_\alpha(Y) = \max \{|X| : X \text{ is connected in } G \text{ and is an } \alpha \text{ subset of } Y\}$$

Notice that if  $X$  is an  $\alpha$ -subset of  $Y$  then:

$$|X| \leq \frac{1}{\alpha} |Y|$$

---

<sup>5</sup>In the original, the graph is the syndorm graph

**Lemma 5.18** ( $\alpha$ -percolation, [38]). *We use the notations of Section 5.1.1.*

*Let  $\alpha \in (0, 1]$  then there exists a threshold  $p_{\text{th}} = p_{\text{th}}(\alpha) > 0$  such that for any  $t \in \mathbb{N}^*$ , for any  $p_{\text{phys}} < p_{\text{th}}$  and for any  $p_{\text{synd}} < p_{\text{th}}$  the following holds. If an error  $(E, D)$  is chosen according to a local stochastic noise with parameter  $(p_{\text{phys}}, p_{\text{synd}})$  then:*

$$\mathbb{P}\left[\text{MaxConn}_\alpha(E \cup D) \geq t\right] \leq C|\mathcal{V}| \left(\frac{\max(p_{\text{phys}}, p_{\text{synd}})}{p_{\text{th}}}\right)^{\alpha t},$$

*where  $C = C(p, \alpha)$  is independent of  $t$ .*

**Figure:** Formal statement, error reduction using the Small-set-flip parallel decoder.

So with probability  $1 - e^{-\gamma\sqrt{n}}$  we have that  $\text{MaxConn}_\alpha(E) < \gamma\sqrt{n}$ .

# The Decoding Algorithm.

First notice that the repetition code could be defined as Tanner code, for any  $\Delta$ -regular graph  $G$  and local code  $C_0$  which is the repetition over  $\Delta$  bits.

In particular  $G$  could be a bipartite expander graph. Denote the right and the left vertices subsets by  $V^-$  and  $V^+$ .

## Decoding:

For  $\Omega(\log n)$  iterations, do:

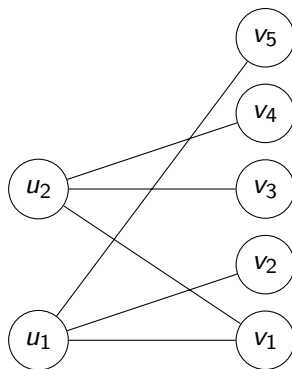
1. In every even iteration, all the vertices in  $V^+$  'correct' their local view based on the majority.
2. In every odd iteration, all the vertices in  $V^-$  'correct' their local view based on the majority.

For having a constant depth error reduction procedure, it's enough to run the decoding above for two iterations.

# The Decoding Algorithm.

**Data:**  $x \in \mathbb{F}_2^n$

```
1 for  $v \in V^+$  do
2    $x'_v \leftarrow$ 
      $\arg \min \{y \in C_0 : |y + x|_v|\}$ 
3 end
4 for  $v \in V^-$  do
5    $x'_v \leftarrow$ 
      $\arg \min \{y \in C_0 : |y + x|_v|\}$ 
6 end
7 return  $x$ 
```



# The Decoding Algorithm.

## Proof.

Denote by  $S^{(0)} \subset V^+$  and  $T^{(0)} \subset V^-$  the subsets of left and right vertices adjacent to the error. And denote by  $T^{(1)} \subset T^{(0)}$  the right vertices such any of them is connect by at least  $\frac{1}{2}\Delta$  edges to vertices at  $S^{(0)}$ .

Note that that any vertex in  $V^- / T^{(1)}$  has on his local view less than  $\frac{1}{2}\Delta$  faulty bits, So it corrects into his 'right' (codeword in  $C_0$ ) local view in the first right correction round.

Therefore after the right correction round the error is set only on  $T^{(1)}$ 's neighbourhood, namely at size at most  $\Delta|T^{(1)}|$ . We will show:

$$\Delta|T^{(1)}| \leq \text{constant} \cdot |e|$$



Using the expansion property we get an upper bound on  $T^{(1)}$  size:

$$\begin{aligned}\frac{1}{2}\Delta|T^{(1)}| &\leq \Delta \frac{|T^{(1)}||S^{(0)}|}{n} + \lambda\sqrt{|T^{(1)}||S^{(0)}|} \\ \left(\frac{1}{2}\Delta - \frac{|S^{(0)}|}{n}\Delta\right)|T^{(1)}| &\leq \lambda\sqrt{|T^{(1)}||S^{(0)}|} \\ \Delta^2|T^{(1)}| &\leq \left(\frac{1}{2} - \frac{|S^{(0)}|}{n}\right)^{-2} \lambda^2|S^{(0)}|\end{aligned}$$

Since any left vertex adjoins to at least single faulty bit we have that  $|S^{(0)}| \leq |e|$ . Combining with the inequality above we get:




$$\Delta|T^{(1)}| \leq \left(\frac{1}{2} - \frac{|e|}{n}\right)^{-2} \lambda^2 \frac{|e|}{\Delta}$$

Hence for  $|e|/n \leq \beta = \frac{1}{2} - \sqrt{\frac{2\lambda^2}{\Delta}}$  it holds that  $\Delta|T^{(1)}| \leq \frac{1}{2}|e|$ .<sup>6</sup>

<sup>6</sup>Reminder for David!!! Explain why  $\lambda^2/\Delta \geq 1$ , and to describe how to correct the proof.

# The French's Construction.

Tillich and Zemor 2014 Leverrier, Tillich, and Zemor 2015  
GrosPELLIER 2019

-  Tillich, Jean-Pierre and Gilles Zemor (Feb. 2014). “Quantum LDPC Codes With Positive Rate and Minimum Distance Proportional to the Square Root of the Blocklength”. In: *IEEE Transactions on Information Theory* 60.2, pp. 1193–1202. DOI: 10.1109/tit.2013.2292061. URL: <https://doi.org/10.1109%2Ftit.2013.2292061>.
-  Leverrier, Anthony, Jean-Pierre Tillich, and Gilles Zemor (Oct. 2015). “Quantum Expander Codes”. In: *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*. IEEE. DOI: 10.1109/focs.2015.55. URL: <https://doi.org/10.1109%2Ffocs.2015.55>.
-  GrosPELLIER, Antoine (Nov. 2019). “Constant time decoding of quantum expander codes and application to fault-tolerant quantum computation”. *Theses. Sorbonne Université*. URL: <https://theses.hal.science/tel-03364419>.

# The French's Construction.

## French gadgets.

- ▶ Encoded states and magic preparation (via original fault tolerance).
- ▶ Hypergraph product code. (Quantum Expander Codes).  
 $[[n, \Theta(n), \Theta(\sqrt{n})]]$ .

## Theorem <sup>7</sup>

There exists a threshold  $p_0$  such that the following holds. Let  $p < p_0$ , let  $\delta > 0$  and let  $D$  be a circuit with  $m$  qubits, with  $T$  time steps and  $|D|$  locations. We assume that the output of  $D$  is a quantum state  $|\psi\rangle$ .

Then there exists another circuit  $D'$  whose output is  $|\psi\rangle$  and such that when  $D'$  is subjected to a local noise model with parameter  $p$ , there exists a  $\mathcal{N}$  a local stochastic noise on the qubits of  $|\psi\rangle$  with parameters  $p' = c \cdot p$  such that:

$$\Pr[\text{output of } D' \text{ is not } \mathcal{N}(|\psi\rangle)] \leq \delta$$

In addition  $D'$  has  $m'$  qubits and  $T'$  time steps where:

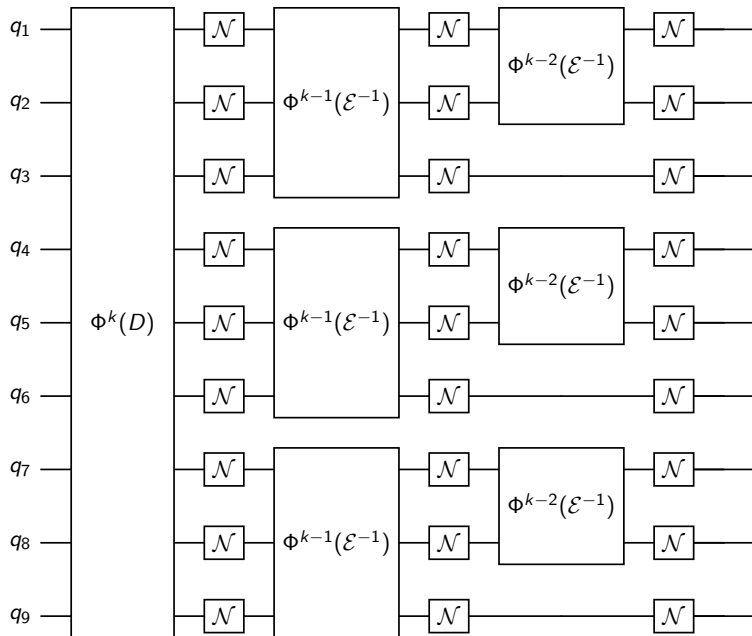
$$m' = m \text{ polylog } (|D|/\delta)$$

$$T' = T \text{ polylog } (|D|/\delta)$$

---

<sup>7</sup>Theorem 6.4 in Grossepi  ier 2019

# Proof Sketch.



## Proof Sketch.

The probability that the  $i$ th bit will absorb an error at the end is bounded by:

$$(cp)^{2^{k-1}} + (cp)^{2^{k-2}} + \dots (cp)^{2^{k-3}} + \dots + cp \leq c_2 p$$

So we prepared the state  $|\psi\rangle$ , subjected to local noise (depolarizing noise) at rate  $c_2 p$ .

## Corollary

We can assume that we have an access to polynomially number of magic states encoded in whatever code we like. Moreover, denote by  $n$  the complexity parameter (input length). if the encoding gate (of the desired code) is  $D$  and it's depth is  $T$ , such that

$$T \text{polylog}(|D|) = O(\log n)$$

then the preparation of the magic is in noisy-QNC<sub>1</sub>.

# Hypergraph Product Code.

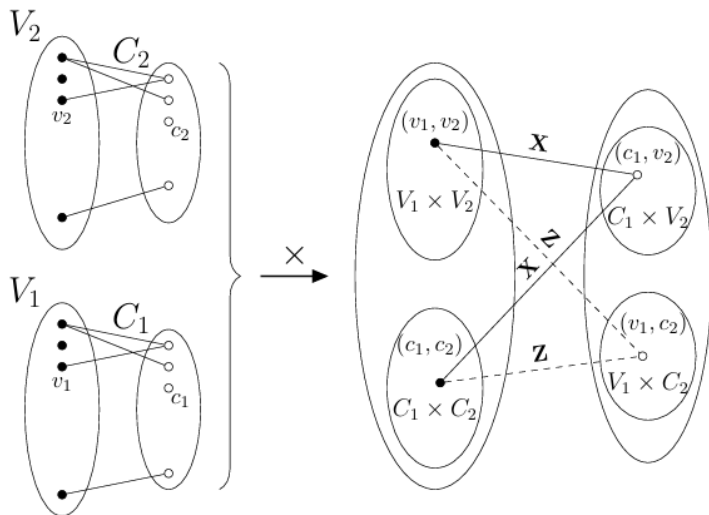


Figure: Hypergraph Product code Tanner graph / stabilizers.

## Hypergraph Product Code.

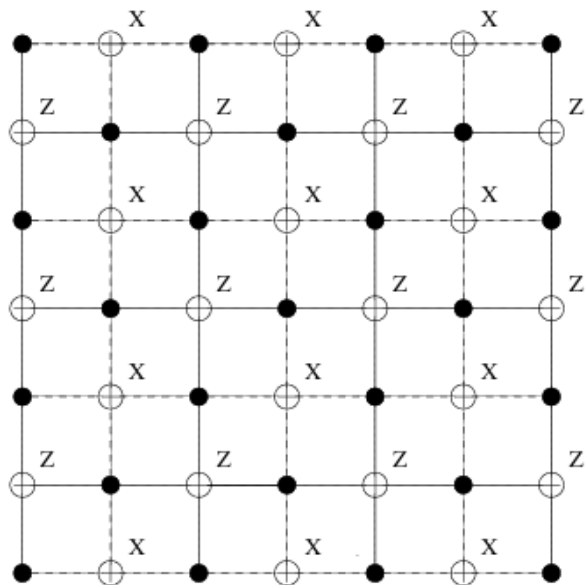


Figure: The Toric code can be thought of as the hypergraph product



# Error reduction in the Quantum Expander Code.

## Quantum Expander Code.

Consider  $C_1, C_2$  (classical) expanders codes<sup>8</sup>. Consider the Hypergraph code defined by them.

## Proof Idea

- ▶ First, proving that for adversarial errors with weight at most  $\alpha\sqrt{n}$ , the error can be reduced by a constant factor. The proof uses the expansion in classical codes.
- ▶ Second, showing that with probability  $1 - \Theta(e^{-\sqrt{n}})$ , the error can be decomposed into disjoint errors, each with a size of at most  $\alpha\sqrt{n}$ .

---

<sup>8</sup>such  $C_1^\perp, C_2^\perp$  also have a good distance.

# Fault Tolerance at Constant Space Overhead.

## Start.

We prepare  $\sqrt{n}$  blocks at length  $\Theta(\sqrt{n})$  each, we do it sequentially, so the preparation requires  $\Theta(\sqrt{n} \text{polylog } n)$  ancilla.

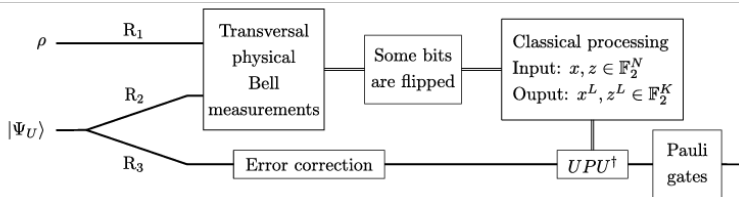
## Error reduction.

Constantly apply rounds of error reduction.

## Simulate a gate.

- ▶ If the gate is a logical Pauli, we apply it in a transversal manner.
- ▶ We prepare the magic state suite for the gate and simulate the gate using the magic procedure - Entangle the states (through transversal CNOT), measure and decode the measurement. Then applying a correction which might be either transversal logical Pauli (if the gate were Clifford) or logical Clifford (if the gate were T). For the second we will have to repeat on the procedure.

# Fault Tolerance at Constant Space Overhead.



An almost  $\mathbf{QNC}_1 = \text{noisy-}\mathbf{QNC}_1$

Encode each qubit by expander code at length  $\Theta(\log^{10}(n))$ .  
Prepare  $2|D|$  magic states from each type in the beginning.

Where did we cheat?

Decide what correction to apply  $UPU^\dagger$  given the measurement is not a trivial task. In particular, it isn't clear if it can be done in constant depth.

# Open Problems.

- ▶ Is there a non-trivial lower bound for deciding  $UPU^\dagger$ ?
- ▶ Implementing logical gates natively without magic states at a constant depth.

# Sheets.

1. The Tanner graph of the classical code  $C_X$  used to correct  $X$ -type errors is the subgraph of  $G_Q$  induced by the  $V \times V \cup C \times C$  qubits and the set of  $Z$ -type generators.