Localitiy of Small-Set-Flip Decoder.

David Ponarovsky

July 2, 2025

Introduction

Last Time:

- An almost $\mathbf{QNC}_1 =$ noisy-$\mathbf{QNC}_1$.
- Original fault tolerance gives us way to prepare 'memmory'.

Today:

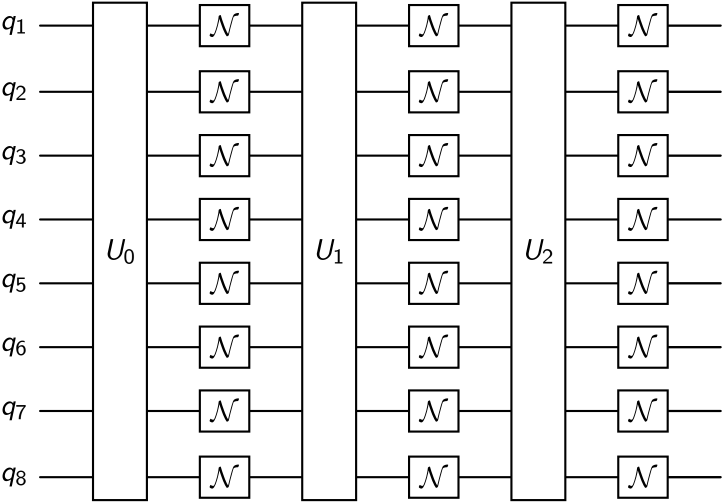
- More about Noise, p-local noise $\leftrightarrow^1$ (p', q')-initial error per correction cycle.
- Formal statement, of the decoding theroem.
- A bit on the locality of the algorithem.

TAKEAWAYS:

- More about codes.
- First view to fault tolerance.
- Nice open problems.

[1] When using the LDPC codes

Nosiy Circuit.



(p', q)-Simplified Model.

Definition

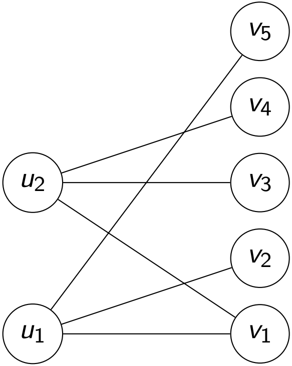
Local Stochastic Noise. Denote by E the subset of faulty qubits. We say that an error model behave according to the local stochastic noise, if:

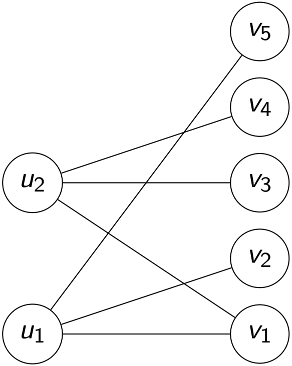
$$\mathbf{Pr}[|E| = t] \leq O(p^t)$$

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

Definition

Let $p', q \in (0, 1)$ and let C be an error correction code, The decoding problem at the (p', q)-**Simplified Model**, is defined to find (a correction to) error E, promised it subjected to local stochastic nosie p, given syndorom measurment subjected to local stochastic noise q.


v_5
v_4
u_2
v_3
v_2
u_1
v_1


v_5
v_4
u_2
v_3
v_2
u_1
v_1

The Decoding Algorithm.

First noitce that the repetition code could be defined as Tanner code, for any Δ-regular graph G and local code C_0 which is the repetition over Δ 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: $x \in \mathbb{F}_2^n$

for $v \in V^+$ **do**

  $x'_v \leftarrow \arg\min \{y \in C_0 : |y + x|_v|\}$

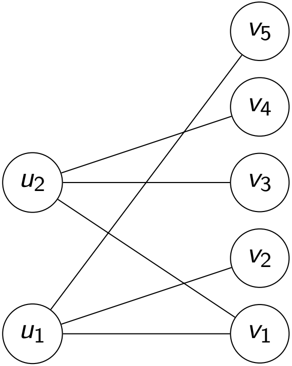
end

for $v \in V^-$ **do**

  $x'_v \leftarrow \arg\min \{y \in C_0 : |y + x|_v|\}$

end

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:

$$\frac{1}{2}\Delta|T^{(1)}| \leq \Delta\frac{|T^{(1)}||S^{(0)}|}{n} + \lambda\sqrt{|T^{(1)}||S^{(0)}|}$$

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

$$\Delta^2|T^{(1)}| \leq \left(\frac{1}{2} - \frac{|S^{(0)}|}{n}\right)^{-2}\lambda^2|S^{(0)}|$$

Since any left vertex adjoins to at least single faulty bit we have that $|S^{(0)}| \leq |e|$. Combing 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 $\Delta|T^{(1)}| \leq \frac{1}{2}|e|$. [2]

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

The Franch'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 Franch's Construction.

Franch gadgets.

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

Theorem [3]

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:

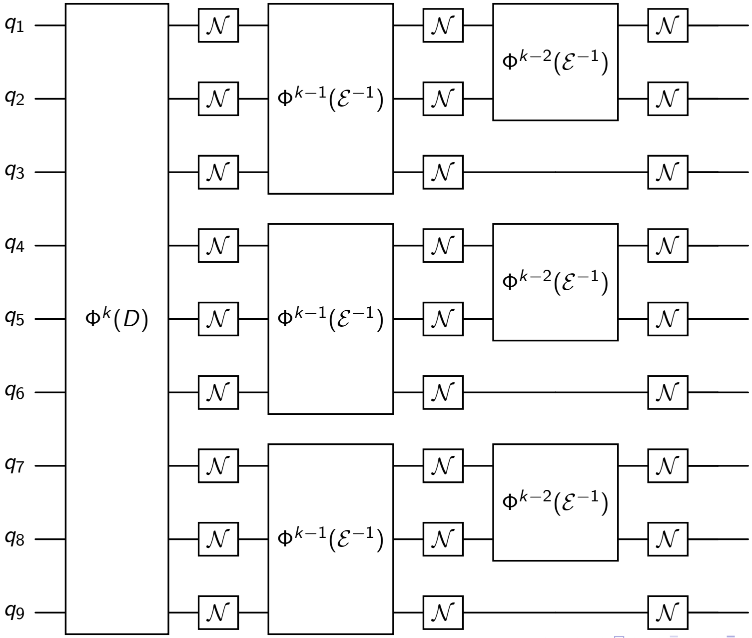
$$\mathbf{Pr}[\text{ output of } D' \text{ is not } \mathcal{N}(|\psi\rangle)] \leq \delta$$

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

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

[3] Theorem 6.4 in Grospellier 2019

Proof Sketch.



Proof Sketch.

The probability that the ith bit will absorb an error at the end is bounded by:

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

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 accsess to polynomialy number of magic states encoded in whatever code we like. Moreover, denote by n the complexitiy parameter (input length). if the encoding gate (of the desired code) is D and it's depth is T, such that

$$T\textbf{polylog}\left(|D|\right) = O(\log n)$$

then the preparation of the magic is in noisy-$\mathbf{QNC}_1$.

Hypergraph Product Code.

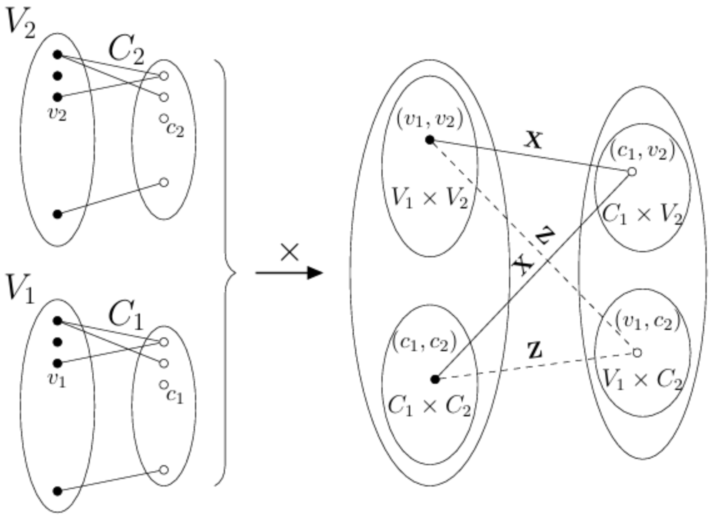


Figure: Hypergraph Product code Tanner graph / stabilizers.

Hypergraph Product Code.

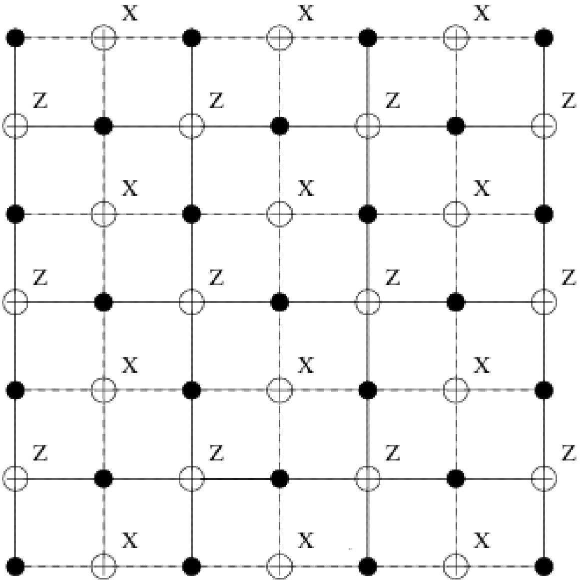


Figure: The Toric code can be thought of as the hypergraph product

Error reduction in the Quantum Expander Code.

Quantum Expander Code.

Consider C_1, C_2 (classical) expanders codes[4]. 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 $\alpha\sqrt{n}$.

[4] such $C_1^{\perp}, C_2^{\perp}$ also have a good distance.

Fault Tolerance at Constant Space Overhead.

Start.

We preapere $\sqrt{n}$ blocks at length $\Theta(\sqrt{n})$ each, we do it sesenqutaly, so the preaperation requires $\Theta(\sqrt{n}\textbf{polylog}\,n)$ anciles.

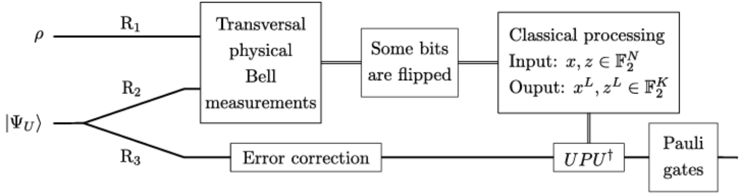
Error reduction.

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 reapet on the procedure.

Fault Tolerance at Constant Space Overhead.



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

Encode each qubit by exapnder code at length $\Theta(\log^{10}(n))$.
Prepere $2|D|$ magic states form 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.