

A Tale of Five Decoders.

David Ponarovsky

October 15, 2025

Introduction

Today:

- ▶ Noisy Circuits.
- ▶ Definitions and Motivation.
- ▶ Pippenger Construction. (Classical, Fault Tolerance with constant overhead at depth).
- ▶ 'Franch-line' works, modern fault tolerance methods and gadgets. ('log n' overhead at depth).
- ▶ An almost $\mathbf{QNC}_1 = \text{noisy-QNC}_1$.
- ▶ Next week, directions and hints that might show separation. (\neq).

TAKEAWAYS:

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

Nosiy Circuit.

Figure: Decoder Majoritiy

Nosiy Circuit.

Figure: Decoder Colors

Nosiy Circuit.

Figure: Decoder Picking Random

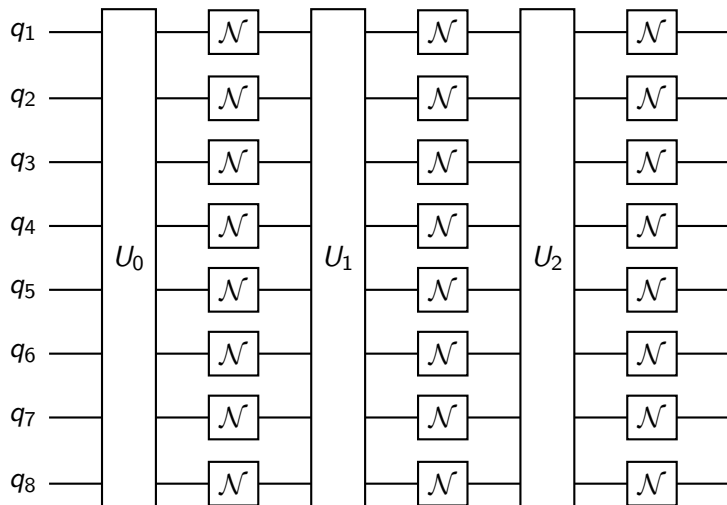
Nosiy Circuit.

Figure: Decoder SWIFT

Nosiy Circuit.

Figure: Decoder Max Color

Nosiy Circuit.



Nosiy Circuit.

Definition

p - Depolarizing Channel. The qubit depolarizing channel with parameter $p \in [0, 1]$ is the quantum channel \mathcal{D}_p defined by:

$$\mathcal{D}_p(\rho) = (1 - p)\rho + p \cdot \frac{I}{2}$$

where ρ is a single-qubit density matrix and I is the identity matrix.

Definition

p -Noisy Circuit. Given a circuit C (regardless of the model), its p -noisy version \tilde{C} is the circuit obtained by alternately taking layers from C and then passing each (qu)bit through a p -Depolarizing channel.

Threshold Theorem.

Theorem (Threshold Theorem. Informal.)

There is a universal $p_{th} \in (0, 1)$ such that for any $p < p_{th}$, any circuit in BQP can be simulated by a p -noisy BQP circuit. The simulating circuit has a depth that is at most $\text{polylog } n$ times the original depth.

Definitions

Definition (**NC** - Nick's Class)

NC_{*i*} is the class of decision problems solvable by a uniform family of Boolean circuits, with polynomial size, depth $O(\log^i(n))$, and fan-in 2.

Definition (**QNC**)

The class of decision problems solvable by polylogarithmic-depth, and finite fan out/in quantum circuits with bounded probability of error. Similarly to **NC**_{*i*}, **QNC**_{*i*} is the class where the circuits have $\log^i(n)$ depth.

Definition (**QNC**_G)

For a fixed finite fan in/out gateset G , the class with deciding circuits composed only for gates in G and at depth at most polylogarithmic. And in similar to **QNC**_{*i*}, **QNC**_{G,*i*} is the restriction to circuits with depth at most $\log^i(n)$.

Pippenger's Construction.

Theorem (Threshold Theorem - Pippenger. Informal.)

There is fault tolerance construction with a constant depth overhead.

Idea.

- ▶ Encode each bit with the repetition code $0 \mapsto 0^m, 1 \mapsto 1^m$.
- ▶ The OR and the AND operations can be made in $O(1)$ depth (without decoding).

$$\begin{aligned}\bar{\mathbf{OR}}(\bar{x}, \bar{y}) &= \mathbf{OR}(x_0 x_0, x_0 \dots, y_0 y_0 y_0 \dots) \\ &= \mathbf{OR}(x_0, y_0) \mathbf{OR}(x_0, y_0) \mathbf{OR}(x_0, y_0) \dots\end{aligned}$$

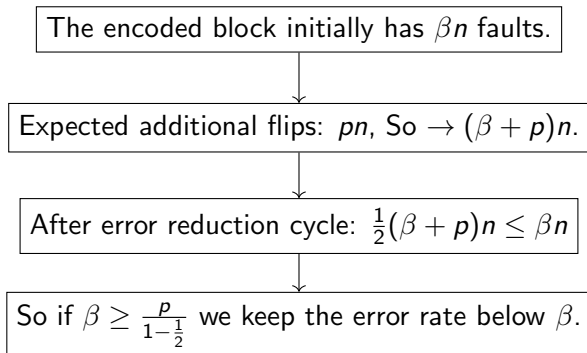
- ▶ Parital decoding. Keeping the error 'low', by a 'decoding' round. (Next slide).

The 'Decoding' trick.

Lemma

There exists $\beta \in (0, 1)$ such that if the error is at weight less than βn , then a single correction round reduces the error by at least a $\frac{1}{2}$ fraction.

Then



The Decoding Algorithm.

First notice 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:

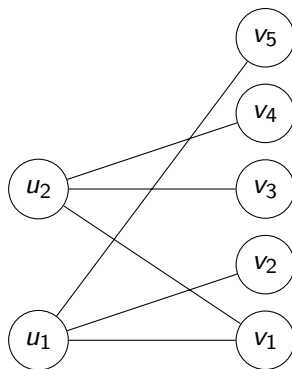
1. In every even iteration, all the vertices in V^+ 'correct' their local view based on the majority.
2. In every odd iteration, all the vertices in V^- 'correct' their local view based on the majority.

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

The Decoding Algorithm.

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

```
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 $\Delta|T^{(1)}| \leq \frac{1}{2}|e|$.¹

¹Reminder 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 ²

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:

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

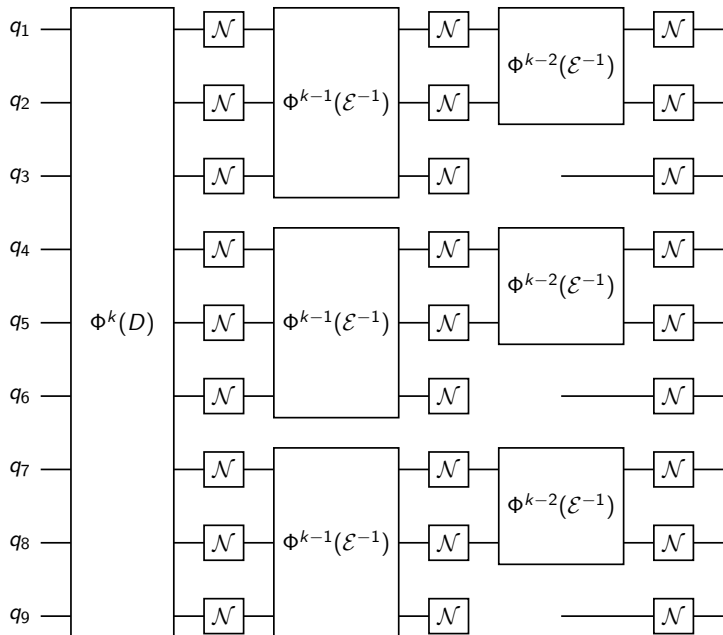
In addition D' has m' qubits and T' time steps where:

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

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

²Theorem 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-QNC₁.

Hypergraph Product Code.

Hypergraph_prod.png

Hypergraph Product Code.

toric_prod.png

Error reduction in the Quantum Expander Code.

Quantum Expander Code.

Consider C_1, C_2 (classical) expanders codes³. 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 $\alpha\sqrt{n}$.

³such 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.

`magic_prod.png`

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.