

Does $\mathbf{QNC}_1 = \text{noisy-}\mathbf{QNC}_1$?

David Ponarovsky

June 24, 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).
- ▶ Next week, directions and hints that might show separation. (\neq).

TAKEAWAYS:

- ▶ More about codes.
- ▶ First view to fault tolerance.

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.

Definition

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 deciding 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.

Encode each bit with the repetition code $0 \mapsto 0^m$, $1 \mapsto 1^m$. Now observe that any logical operation, without decoding, can be made in $O(1)$ depth.

For example, $\text{OR}(\bar{x}, \bar{y})$ can be computed by applying in parallel $\text{OR}(x_i, y_i)$ for each i .

The 'Decoding' trick.

Instead of completely decoding, we would apply only a single step of partial decoding. We assume that in each code block the bits are partitioned into random disjoint triples, and we will apply a local correction to each of the triples by majority.

Claim

There are constants $\alpha, \eta \in (0, 1)$ such that for any bit string x at a distance $\leq \alpha n$ from the code (Repetition Code), one cycle of local correction on x yields x' such that:

$$d(x', C) \leq \eta n$$

The 'Decoding' trick.

Suppose that a bit absorb a bit flip with probability p . So in expectation we expect that entire block at length n will absorb pn flips.

$$\eta(\beta + p)n \leq \beta n$$
$$\beta \geq \frac{p}{1 - \eta}$$

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^+ .

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.

The Decoding Algorithm.

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

Result:

$$\arg \min \{y \in C : |y + x|\}$$

if $d(y, C) <$

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

2 $x'_v \leftarrow$

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

3 **end**

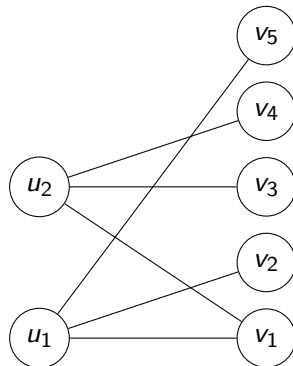
4 **for** $v \in V^-$ **do**

5 $x'_v \leftarrow$

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

6 **end**

7 **return** x



We will call to the first stage, when only the right vertices suggest correction the right round, and to the second stage a left round. For the whole procedure, we will call a single correction round.

Lemma

If the error is at wight less than βn then a single round of the majority reduce the error by at least constant fraction.

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 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 that this amount is strictly lower by a constant factor than $|e|$.

First, let's use the expansion property for getting an upper bound on $T^{(1)}$ size:

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

Since any left vertex adjoins to at most Δ faulty bits we have that $\Delta|S^{(0)}| \leq |e|$. Combing with the inequality above we get:

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

Hence for $|e|/n \leq \beta = \frac{1}{2}\Delta - \sqrt{2\lambda}$ it holds that $\Delta|T^{(1)}| \leq \frac{1}{2}|e|$.
Namely the error is reduced by half.

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>.

Hypergraph Product Code.



Figure: Caption for the image

Hypergraph Product Code.



Figure: Caption for the image

Error reduction in the Quantum Expander Code.

Quantum Expander Code.

Consider C_1, C_2 (classical) expanders codes¹. Consider the Hypergraph code defined by them.

First

Error Reducing Stage. One shows that for any error with weight at most $\alpha\sqrt{n}$, the error can be reduced. The proof uses the expansion in the classical codes.

Second

Then, one shows that with probability $1 - \Theta(e^{-\sqrt{n}})$, the error can be decomposed into disjoint errors, each with size at most $\alpha\sqrt{n}$.

¹such C_1^\perp, C_2^\perp also have a good distance.

Hypergraph Product Code.

Start

Initialize Magic states in parallel for both the Clifford and the T states. Do it using the original threshold construction.



Figure: Caption for the image

Disjointness.