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

David Ponarovsky

June 24, 2025

Introduction

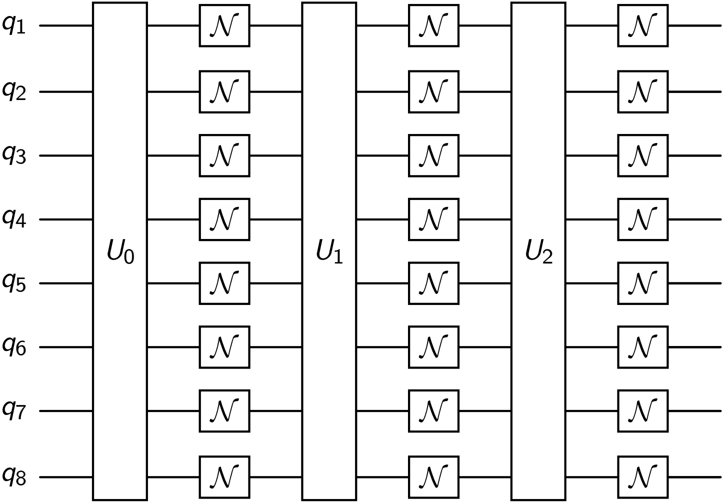
Today:

- 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 poly $\log n$ times the original depth.

Circuit	#Qubits	#Gates	$\mathbb{P}[\text{wrong output}]$
D	m	$\lvert\mathrm{D}\rvert$	$\leq p_{\mathrm{loc}}\,\lvert\mathrm{D}\rvert$
$\Phi_0(\mathrm{D})$	$7m$	$\leq c_0\,\lvert\mathrm{D}\rvert$	$\leq c_1\,p_{\mathrm{loc}}^2\,\lvert\mathrm{D}\rvert$
$\Phi_0^k(\mathrm{D})$	$7^k m$	$\leq c_0^k\,\lvert\mathrm{D}\rvert$	$\leq \dfrac{(c_1\,p_{\mathrm{loc}})^{2^k}}{c_1}\,\lvert\mathrm{D}\rvert$

Figure: Caption for the image

Threshold Theorem.

Definition

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

$\mathbf{NC}_i$ 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 finate fan out/in quantum circuits with bounded probability of error. Similarly to $\mathbf{NC}_i$, $\mathbf{QNC}_i$ is the class where the decisdes the circuits have $\log^i(n)$ depth.

Definition ($\mathbf{QNC_G}$)

For a fixing finate fan in/out gateset G, the class with deciding circuits composed only for gates in G and at depath at most polylogaritmic. And in similar to $\mathbf{QNC}_i$, $\mathbf{QNC_{G,i}}$ is the restirction to circuits with depath at most $\log^i(n)$.

Pippenger's Construction.

Theorem (Threshold Theorem - Pippenger. Informal.)

There is fault tolerance construction with a constant depth overhead.

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, $\mathrm{OR}(\bar{x}, \bar{y})$ can be computed by applying in parallel $\mathrm{OR}(x_i, y_i)$ 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:

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

The 'Decoding' trick.

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

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

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**

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

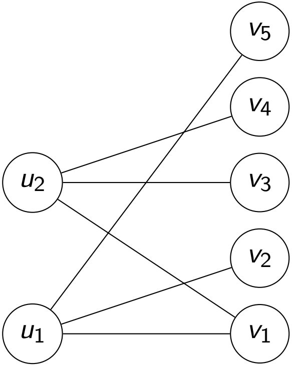
end

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

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

end

return x



The Decoding Algorithm.

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.*

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 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:

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

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

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

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:

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

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

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.

French gadgets.

- Encoded states and magic preparation (via original fault tolerance).
- Hypergraph product code.

Theorem [1]

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:

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

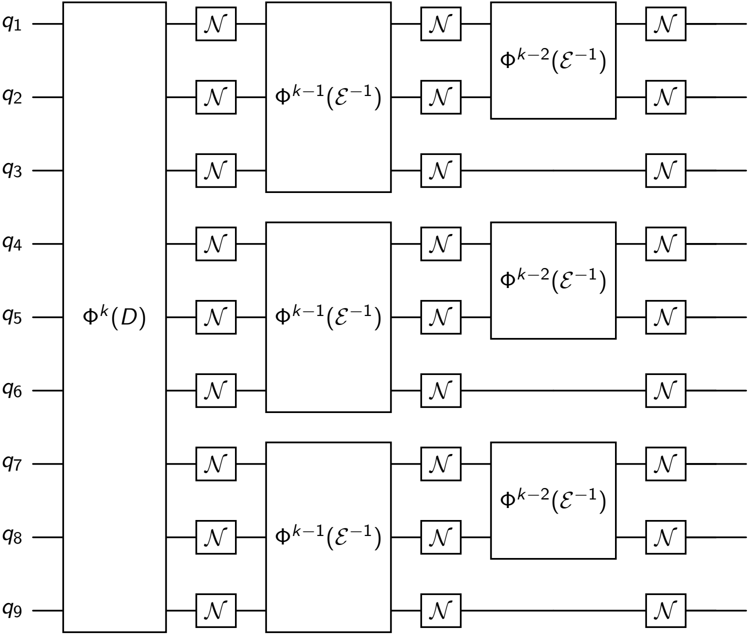
In addition D' has m' qubits and T' time steps where:

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

[1] Theorem 6.4 in Grospellier 2019

Proof Sketch.

Denote by $\Phi^k(D)$ the circuit obtained by the original fault-tolerance construction when concatinating k-times. Thus, the output of $\Phi_k(D)$ is $|\psi\rangle$ encoded in the concatenated code, thus we need to decode the output of $\Phi^k(D)$ in fault tolerant manner. We fix $\mathcal{E}^{-1}$ somde decoding circit for the Steane code and we denote by $\Lambda(D)$ the citrcuit $\Phi^1(D)$ followed by m_0 copies of $\mathcal{E}^{-1}$, one per block of the Steane code. In pariticular, the output of $\Lambda(D)$ is an m_0-qubit state. Similarly, the circuit $\Lambda^k(D)$ is the circuit $\Phi^k(D)$ followed by k layers of decoding, the ith decoding layer uses $\Phi^{k-i}\left(\mathcal{E}^{-1}\right)$.



q_1
q_2
q_3
q_4
q_5
q_6
q_7
q_8
q_9
$\Phi^k(D)$
$\mathcal{N}$
$\Phi^{k-1}(\mathcal{E}^{-1})$
$\Phi^{k-1}(\mathcal{E}^{-1})$
$\Phi^{k-1}(\mathcal{E}^{-1})$
$\Phi^{k-2}(\mathcal{E}^{-1})$
$\Phi^{k-2}(\mathcal{E}^{-1})$
$\Phi^{k-2}(\mathcal{E}^{-1})$

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

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

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

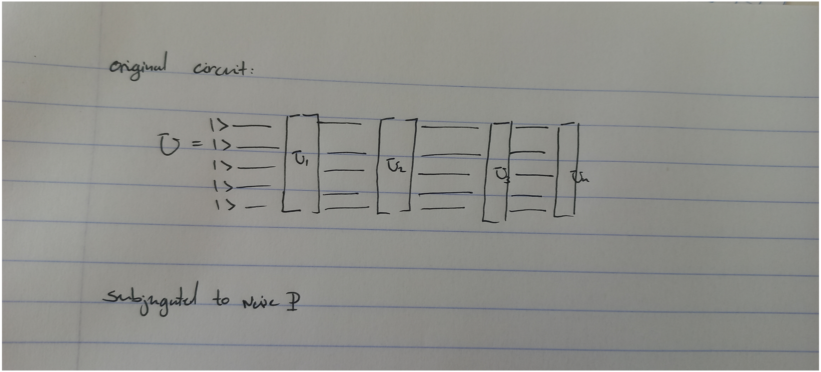
Corollary

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

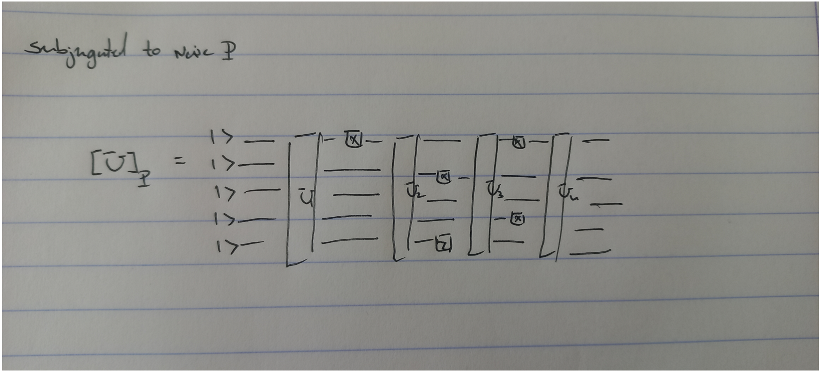
$$T\,\mathbf{polylog}\,(|D|) = O(\log n)$$

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

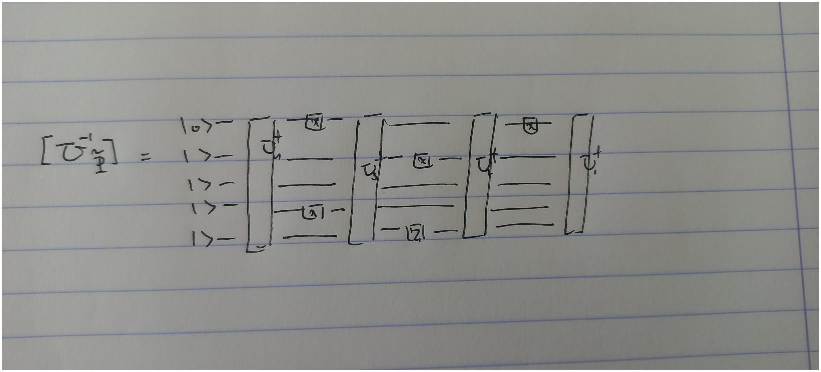
Title of the Frame



Title of the Frame



Title of the Frame



With high probability, $\Phi(D)\,|0\rangle$ sends us to ρ, which is not far from $C_{th}(|\psi\rangle)$. Then, applying the reverse side of the threshold construction sends us to $|\psi\rangle$.

$$|0\rangle \to C_{th}(C(|\psi\rangle)) \to C(|\psi\rangle)$$

Hypergraph Product Code.

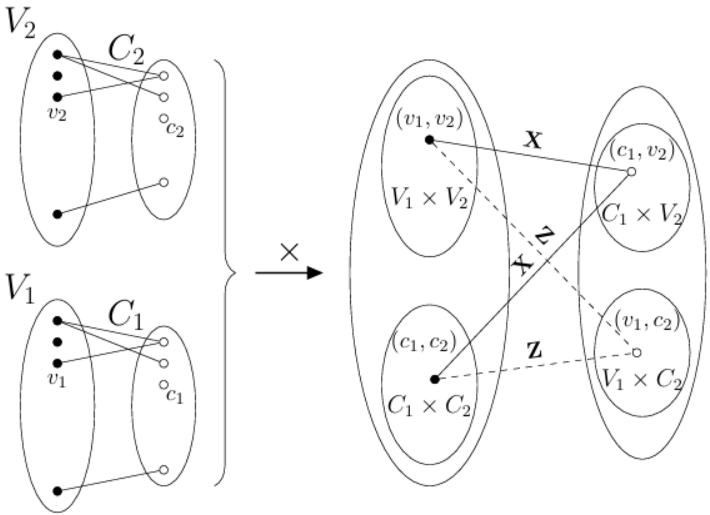


Figure: Caption for the image

Hypergraph Product Code.

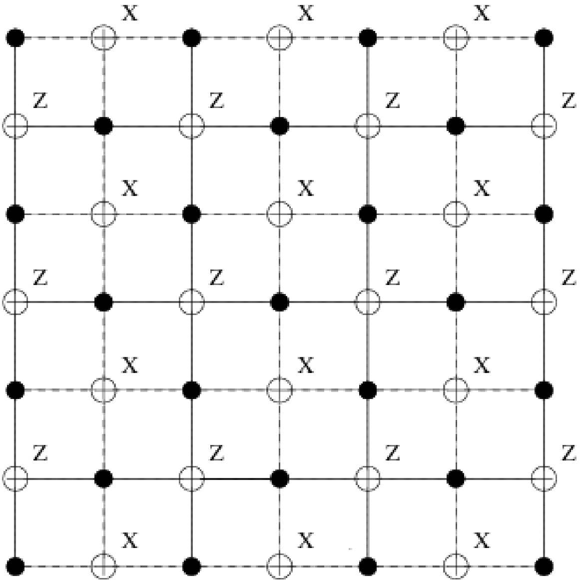


Figure: Caption for the image

Error reduction in the Quantum Expander Code.

Quantum Expander Code.

Consider C_1, C_2 (classical) expanders codes[2]. 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 $\alpha\sqrt{n}$.

[2] such $C_1^\perp, C_2^\perp$ 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.

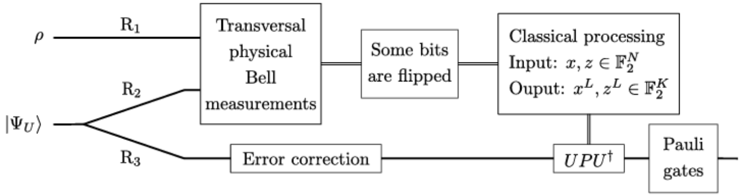


Figure: Caption for the image

Disjointness.