Research Proposal - Fault-Tolerainzing Shallow Circuits.

Michael Ben-Or David Ponarovsky

July 29, 2025

Abstract

We study the overall depth overhead cost required for constructing fault-tolerant circuits. We focus on shallow depth circuit classes, in particular, $\mathbf{QAC}_0, \mathbf{QNC}_{0,f}$, $\mathbf{QNC}_1$, and '**QNC** without reset gates', and certain known problem candidates for demonstrating quantum advantage such as factoring [Sho97] and Instantaneous Quantum Polynomial-time [BMS17], [Pal+24]. We aim to answer whether there exists a fault tolerance with only constant overhead at the circuit's depth. A positive answer implies that computing logarithmic depth circuits when subjected to noise is not harder than computing in an ideal environment.

1 Introduction.

The Quantum Computation model is widely believed to be superior to classical models, offering asymptotic speedup in tasks such as factoring [Sho97], searching [Gro96], simulating, and more relative to the best-known classical solutions. Yet even though there is almost complete agreement about the superiority of the ideal quantum model, there is still a debate over whether it is possible to implement complex computation in the real world, where the qubits and gates are subject to faults. Similarly, the feasibility of realizing classical computation has also been an open question, In fact the question about the feasibility of computation under noise is almost as ancient as the computer science field itself, initialized by Von Neumann [Neu56] at the time that classical computation putted in debuts. Time been pass and the followed works had pointed that not even a polynomial computation in the presence of noise is still reasonable but one can implement a fault tolerance version at a most constant times cost at the circuits depth [Pip85]. Or in asymptotic sense, classical computation in the presence of noise is as exactly hard as computation in ideal environment.

Recently, the feasibility question has been raised again, this time regarding quantum computing, and while an intensive work has been done, and also succeed to prove that polynomial quantum computation can be made fault tolerance, [AB99],[Got14] and even with only constant overhead at the original circuit width [Gro19], the required depth over-head is still not well understood. We stress out that in all the familiar constructions, in construct to Pippenger [Pip85], original constant-depth gates are mapped to asymptotically grow[1] depth gates.

Moreover, even the depth overhead is particularly interesting as today's quantum machines are challenged to maintain quantum states for a long time [**CITE**]. The limitations of these machines have motivated research to define NISQ, which stands for Noisy Intermediate-Scale Quantum, referring to the current era of quantum computing characterized by quantum processors that have a limited number of qubits and are prone to errors due to noise. In addition to NISQ, another common characterization for limited quantum computation is computation without reset gates, which has been proved to be impossible when restricted to polynomial space [Aha+96]. Having a constant depth-overhead fault tolerance scheme would imply the feasibility of log depth computation in that model.

This work addresses the above. We ask whether a magnitude depth overhead is an unavoidable price that one has to pay, If a Constant Depth Fault Tolerance Construction (CDFT) exists, and if so, how to construct it. In particular, whether an ideal $\mathbf{QNC}_1$, the class of problems that can be decided by logarithmic depth quantum circuits, can be computed in noisy-$\mathbf{QNC}_1$ circuits.

[1] Note, that here, classical computation is also counted in the overall depth cost

Additionally, we extend the question beyond the standard classes and ask about fault-tolerant sampling. Specifically, we consider several sampling processes by shallow quantum circuits, which are believed to be infeasible for classical circuits, such as Instantaneous Quantum Polynomial-time [BMS17], [Pal+24], and ask about the depth efficiency of their fault-tolerant version.

The proposal is organized as follows. Section 2 presents the notations, formal definitions, and states the open problems that will be studied through the research. Then, Section 3 describes strategies to prove CDFT. In particular, it lists primitives that can be used to achieve it and discusses how far we are from obtaining them. Having said that, Section 4 presents the first cues against the possibility of CDFT and provides the entry points to prove the impossibility claim. Finally, Section 5 discusses the applications and implications of either the correctness of CDFT or the impossibility of CDFT, from both theoretical and practical views.

2 Notations.

We use the standard notations commonly used in the literature. When not otherwise mentioned, we consider quantum states over qubits, each lying in a two-dimensional Hilbert space $\mathcal{H}_2$, and denote by $\mathcal{H}_{2^n}$ the Hilbert space of an n-qubit system. Pure quantum states and their dual presentations are denoted by $|\psi\rangle, \langle\psi|$, and in the matrix representation, we use $|\psi\rangle\langle\psi|$ to denote its density matrix. We will use ρ to denote a mixed state, whose density matrix is a trace one PSD matrix. We use $\mathcal{N} : L(\mathcal{H}) \to L(\mathcal{H})$ to denote a p-local stochastic noise channel, namely a channel in which for any subset S of the (qu)bits, the probability that all the qubits in S absorb noise is less than $p^{|S|}$. We recall that for a constant-depth circuit, when the fanout/in of its subgates is bounded, one can map the running of the circuits subjected to p-local stochastic noise to a running when the states are subjected only to p'-local stochastic noise before entering the circuit, and then the rest of the computation is done in an ideal environment [Got14], where p' is a function of p and constants. If the gate is also a measure, for example as a decoder, then the mapping induces also q-local stochastic noise on the measurements.

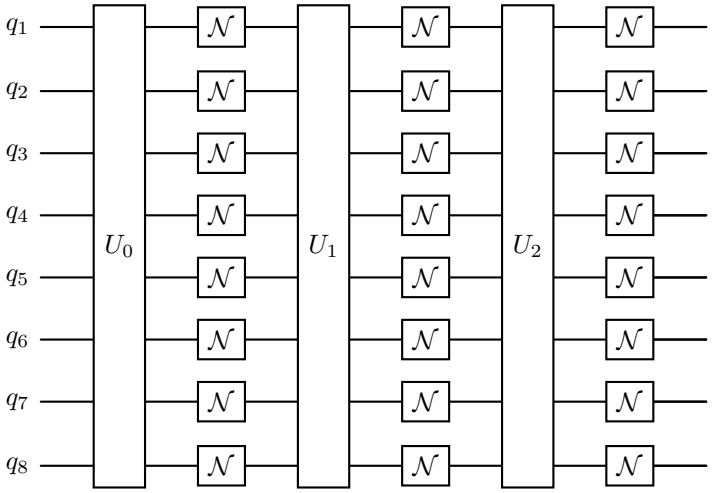

Figure 1: Circuit subjected to noise.

We think about computation subjected to noise as the running of a circuit, in which at any time, qubits might be 'flipped', or formally, with some constant probability, they are replaced with the fully mixed state. Since our computation might create correlations between the errors, we will assume nothing about the behavior of the errors except that big errors are unlikely. By doing that, the induction step doesn't have to guarantee the errors being uncorrelated.

We use Definition 2.1 to describe the running of a circuit subjected to noise. Section 2 illustrates a noisy circuit. In the figure, the channel N acts on each qubit separately, yet this is not the case, and we impose it in that way only to make a clear distinction between the original gates and the noise channels.

Definition 2.1. 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-local stochastic channel.

Generally speaking, we say that a decision problem is solvable by a uniform family of circuits $\mathcal{C}$ if there is a polynomial $poly : \mathbb{R} \to \mathbb{R}$, such that for any large enough $n \in \mathbb{N}$, there exist $a, b \in (0, 1)$ at a distance of at least $b - a > 1/\text{poly}(n)$ and a polynomial Turing machine M such that for any given instance x with encoding length $|x| = n$, the running of M on x outputs $C_x \in \mathcal{C}$ that, when running over the zero word 0^*, induces on the first (qu)bit at least b probability to be at 1 if x is in the language and at most a to be at 1 otherwise. If a decision problem is solvable by a p-noisy version of $C \in \mathcal{C}$, we say that the problem is solvable by noisy-$\mathcal{C}$. We abuse the notation, and for complexity class Q, we define noisy-Q to be all the decision problems solvable by the noisy version of the circuit family that solves the problems in Q. For example, noisy-**BQP** is the class of all the decision problems solvable by noisy polynomial quantum circuits.

The first class we are interested in is Nick's Class, **NC** [**CITE**], characterizing the boolean circuits at logarithmic depth. This class was proven by Pippenger to be equal to its noisy version, namely noisy-**NC** = **NC** [Pip85]. Formally defined as follows:

Definition 2.2 (**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.

Second, the analog class of **NC** is **QNC**, which characterizes logarithmic depth quantum circuits. In **QNC**, the circuits are also allowed to have any single qubit gate. While in the classical case the number of functions from $\{0, 1\}^2 \to \{0, 1\}$ is finite, in the quantum case we have an infinite number of single gates. That motivated us to define $\mathbf{QNC_G}$ - the circuits when the gate set is restricted to some finite, constant size group G. We emphasize that in **BQP** there is no point in restricting to such a family since any gate can be polynomially approximated at polylogarithmic depth, so in that case, the restriction does not change computational power and one can assume to be able to apply any single qubit gate. However, when considering shallow circuits at logarithmic depth, such assumptions don't hold anymore.

Definition 2.3 (**QNC**)**.** The class of decision problems solvable by polynomial size, 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 2.4 ($\mathbf{QNC_G}$)**.** For a fixing finate fan in/out gateset G, the class with deciding circuits at polynomial size, composed only for gates in G and at depth at most polylogaritmic. And in similar to $\mathbf{QNC}_i$, $\mathbf{QNC_{G,i}}$ is the restriction to circuits with depth at most $\log^i(n)$.

Another setting which we find interesting is the equipping of classes with an unbounded fanout CNOT gate, a gate which acts as $|x\rangle \prod_i |y_i\rangle \to |x\rangle \prod_i |x \oplus y_i\rangle$. There are two main reasons we find those class worth considering. First, the unbounded fanout CNOT can be decomposed by chaining only two-qubit CNOTs, since for any CSS code, a CNOT can be implemented in a fault-tolerant manner almost for free. Second, there are candidates at $\mathbf{QNC}_{0,f}$ for proving quantum advantage[BMS17], [Pal+24].

Definition 2.5 ($\mathbf{QNC}_{0,f}$)**.** Similarly to $\mathbf{QNC}_0$, the class of decision problems solvable by constant depth and bounded fan out/in quantum circuits equipped additionally with a 'quantum fanout' gate is available, which CNOTs a qubit into arbitrarily many target qubits in a single step.

Finally, the last setting we consider is the restriction of the classes when there is no access to fresh qubits, or equivalently, no reset gates are allowed. In this setting, any step of computation accumulates entropy, and an exponential trade-off relation between entropy and depth was proved.

Definition 2.6 ($\mathbf{QNC}_1$ without reset gates.)**.** The class of decision problems solvable by polynomial size, logarithmic-depth, and finate fan out/in quantum circuits with bounded probability of error, without reset gates.

Those definitions lead us to ask our first open problem:

Open-Problem 1 (The Main Open Problem.)**.**

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

Our second main problem investigates if it matters which universal gateset is used for the simulation, or whether the previous question is affirmative when our computation is restricted to a finite gateset G' and given that the source was also restricted to use local computation in a finite set, that is, we ask:

Open-Problem 2 (Constant Depth Overhead on G' Restricted Machine.)**.** Does there exist a finite universal set G' such that for any finite two-qubit gateset G it holds that:

$$\mathbf{QNC}_{\mathbf{G},1} = \text{noisy-}\mathbf{QNC}_{\mathbf{G}',1}?$$

In this context, we mention the work of [Kim25], which shows that using a catalyst state[2], no bounded fan-out computation can simulate any single qubit gate with a constant T depth. Namely, in our words, they prove that there exists a finite gate set G' such that:

$$\mathbf{QNC}_{f,1} = \mathbf{QNC}_{f,\mathbf{G}',1} \text{ using catalyst state.}$$

We hope that our work will also lead to an understanding of the importance, or the non-importance, of the basic components being used.

3 Strategies to get CDFT.

Here we summarize and present the main gadgets that were invented in past fault tolerance constructions [AB99], [Got14], and [Gro19]. These gadgets will allow us to simplify the model we work with, presenting an almost proof for CDFT, and focusing our question about complexity into a question about the existence of particular quantum error correction codes. The main gadgets are fault-tolerant State Preparation (SP) and Memory error correction codes (ME). The first presents how, while using the original fault tolerance construction based on concatenation [AB99], one can initialize any quantum state subjected to local stochastic noise at no additional cost to the fault tolerance construction scheme being used. Since encoding is a Clifford operation, and any m-bit Clifford can be implemented in $O(\log m)$ time, then when $m = \Theta(\log^{\alpha} n)$ the fault-tolerant version of the 'encoder' has $O(\log n)$ depth. So using SP, one can initialize m-length blocks encoded in any error correction code at noisy-$\mathbf{QNC}_1$.

The second gadget is Memory, a particular type of code which allows restraining the error rate by exhibiting a constant depth procedure that, when promising that the error rate is below a threshold, suppresses the error by at least a constant factor. Using memory, we will be able to promise with high probability that the error rate is lower than some fraction.

3.1 State Preparation.

The following definition extends the idea of solving decision problems with computation subjected to noise to preparing quantum states with fault tolerance when subjected to noise.

Definition 3.1 (State Preparation.)**.** Let $\mathcal{C}$ be a set of circuits. We say that $S : \mathcal{C} \to$ **p-noisy circuits** is an $[\alpha, (p \to q)]$-State-Preparation scheme for $\mathcal{C}$ if for any $C \in \mathcal{C}$, we have that $S(C) = \tilde{C}$ such that:

1. Depth $(\tilde{C}) \leq \alpha$ Depth (C).
2. Width $(\tilde{C}) \leq \alpha$ Width (C).
3. The state prepared by $\tilde{C}$, namely $\tilde{C}\,|0\rangle$ is the state prepared by C when subjected to q-local stochastic noise.

Based on the fault-tolerance construction in [AB99], one can obtain a $[\text{polylog}(n), (p \to q)]$-SP, where n is the number of the source's circuit qubits, which will next be used as a block length of a desired code. Here we present an informal description of it and refer to [Gro19] for more details.

Figure 2 illustrates the preparation scheme. Denote by E the encoder of the desired code to prepare, and by E_{con}^{-1} the decoder of the single-level concatenation code. First, we apply a fault-tolerant version of the encoder E, using the k-level concatenated code; that stage is

[2] In the catalytic computation model, one has access to a complicated resource state $|\phi\rangle$, yet he has to return/keep it at the end of the running.

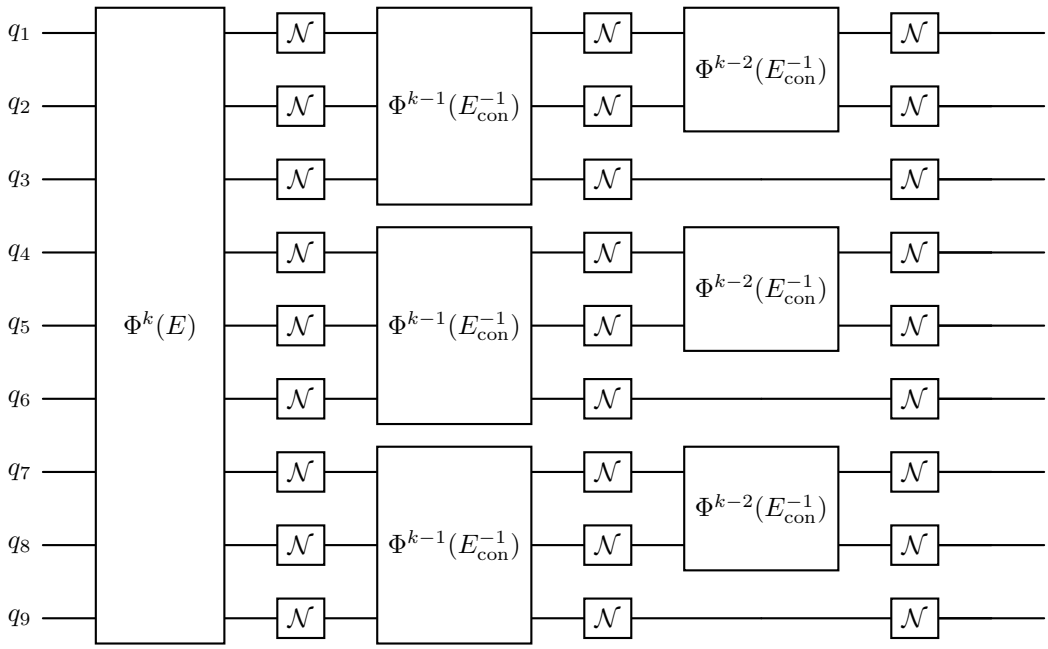

Figure 2: Preparing a quantum states via the concatenation fault tolerance.

represented as $\Phi^k(E)$. Then we decode the concatenated code from top to bottom; namely, in the jth stage, we apply $\Phi^{j-1}(E_{\text{con}}^{-1})$.

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

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

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

3.2 Memory.

Definition 3.2 (Ideal (β, γ)-Memory)**.** We say that a (quantum) error correction code C is an Ideal (β, γ)-Memory code if there is a constant depth procedure $\mathbf{D}$ such that for any I of size $|I| \geq (1-\beta)n$ and a mixed states σ and ρ such σ distributed over the C's codewords $\sigma \in C$ and $\mathbf{Tr}_I(\rho) = \mathbf{Tr}_I(\sigma)$, we have that there is subset of qubits J at size at least $(1-\gamma)n$:

$$\mathbf{Tr}_J \mathbf{D}(\rho) = \mathbf{Tr}_J(\sigma)$$

We would like to extend the memory gadgets to work with high probability, which motivates us to define the following:

Definition 3.3 ($(\mathcal{P}_1, \mathcal{P}_2)$- thermal couple.)**.** Let $\mathcal{P}_1, \mathcal{P}_2$ be sets of density matrices induced over the n-qubit Hilbert space, and let $\mathcal{N}$ be a p-stochastic local noise channel for some constant $p \in (0,1)$. We say that the couple $(\mathcal{P}_1, \mathcal{P}_2)$ is a thermal couple if for any $\rho \in \mathcal{P}_2$, we have $\mathcal{N}(\rho) \in \mathcal{P}_1$ with high probability.

Definition 3.4 ($(\mathcal{P}_1, \mathcal{P}_2)$-Memory)**.** Consider a $(\mathcal{P}_1, \mathcal{P}_2)$- thermal couple, We say that C is a $(\mathcal{P}_1, \mathcal{P}_2)$-Memory if there is a constant depth procedure $\mathbf{D}$, such that for any $\rho \in \mathcal{P}_1$ we have $\mathbf{D}(\rho) \in \mathcal{P}_2$, with high probability.

For example, consider a code C with a Δ-regular Tanner graph. Let $\mathcal{P}_1$ be all the noisy states derived from codewords in C such that the syndrome graph induced by them can be decomposed into disjoint $\Delta/2$-connected components $A_1, A_2, ..A_l$, each of size at most $|A_i| < \beta\sqrt{n}$, and the $\Delta/2$-distance between any two of them A_i, A_j, namely the number of edges needed to add to merge them into one single $\Delta/2$-connected component, is at least $\theta \min(|A_i|, |A_j|)$. We call such decomposition characterization $(\beta\sqrt{n}, \theta)$ error decomposition.

Now let $\mathcal{P}_2$ be all the deviations from C, such that the syndrome graph induced by them can be decomposed into $(\gamma\sqrt{n}, \theta)$ error decomposition. The couple $(\mathcal{P}_1, \mathcal{P}_2)$ is thermal couple, And combining the quantum expander code and the parallel small set-flip decoder [Gro19] they defines a $(\mathcal{P}_1, \mathcal{P}_2)$-memory.

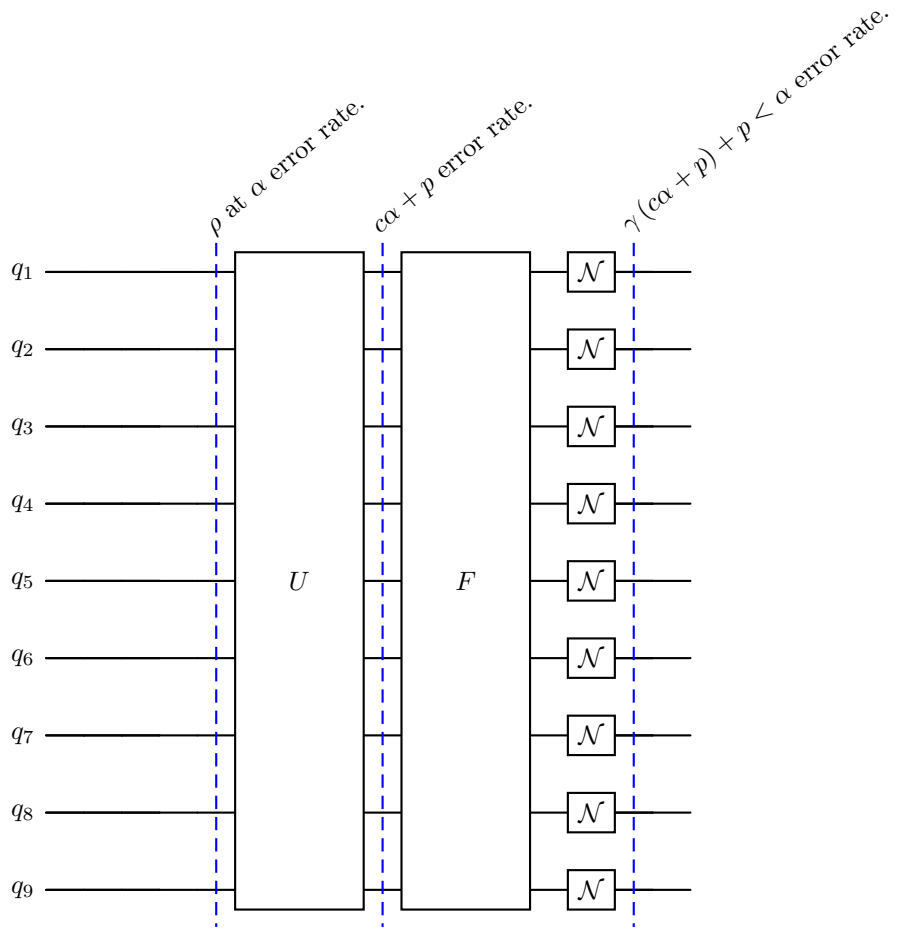

Figure 3: Usage of Ideal (β, γ)-Memory to obtain fault tolerance computation.

3.3 Gate Teleportation.

Gate teleportation is a method to 'encode' operations by quantum states. At a high level, given a precomputed state, it allows one to apply an operation (gate) using (probably) simpler gates. The precomputed states are called **Magic States**.

3.3.1 Leading Example: T-Teleportation.

Recall that the Clifford[3] + T is a universal quantum gate set. The Clifford group alone is considered, from the computer science point of view, a simple/weak computational class since it can be classically simulated[4]. Yet, we will see that given access to the magic $|T\rangle = T|+\rangle$, one can simulate the T gate using only Clifford gates and measurements.

In Figure 4, we have the T-teleportation gadget. The state progresses up to the measurement

[3] Generated by H, S and CX

[4] And conjectured to be strictly weaker than **P**

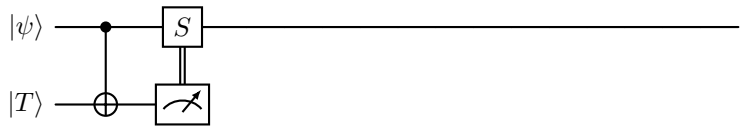

Figure 4: Simulating the T-gate, using the $|T\rangle$ magic state.

as follows:

$$\left(\sum_x \alpha_x |x\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\frac{\pi}{4}}|1\rangle\right) \overset{\mathbf{CX}}{\mapsto} \sum_{x,y} \frac{1}{\sqrt{2}} \alpha_x |x\rangle |x \oplus y\rangle e^{i\frac{\pi}{4}y}$$

$$\mapsto \begin{cases} \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}x} = T|\psi\rangle & \text{measured 0} \\ \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}\bar{x}} & \text{measured 1} \end{cases}$$

$$\overset{\mathbf{CS}}{\mapsto} \begin{cases} T|\psi\rangle \\ \sum_x \alpha_x |x\rangle e^{i\left(\frac{\pi}{4}\bar{x}+\frac{\pi}{2}x\right)} = \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}} e^{i\left(\frac{\pi}{4}\bar{x}+\frac{\pi}{4}x\right)} \end{cases}$$

$$= \begin{cases} T|\psi\rangle \\ e^{i\frac{\pi}{4}} \sum_x \alpha_x |x\rangle e^{i\frac{\pi}{4}} = e^{i\frac{\pi}{4}} T|\psi\rangle \end{cases}$$

Similarly, any two-qubit gate U can be encoded using a proper magic state, and the gate teleportation will be composed by entangling using CNOT, then measurement, and eventually, upon the measurement result P, applying a correction $UPU^\dagger$. We refer to [**CITE**] for further reading.

Open-Problem 3. Does there exist a Memory code for which one can implement gate teleportation to a universal gate set in a local manner?

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

We provide beneath without a formal proof a fault construction that gives an almost CDFT.

1. We start by initializing many encoded magic states and encoded zeros via the state preparation scheme. Since the block is of length $\log^\alpha(n)$, the depth required for that stage is $\log\log(n)$.
2. In each even step, we apply $\mathbf{D}$ to keep the error rate low. It fails with probability at most $\Theta\left(\frac{1}{n^k}\right)$, so by the union bound the probability that $\mathbf{D}$ had at least a single failure is bounded by $\Theta(\frac{1}{n^{k'}})$.
3. We compute the gates over the odd iterations. Each gate is replaced by two applications of gate teleportation, exploiting the magic states. Each application of Clifford, in the second and the first level of the Clifford hierarchy, is followed by $\log(\log(n))$ depth computation for deciding which operation should be applied next.

So in overall the depth overhead we get is $\log\log n$, when the battle neack is the time required to decide on the correction **[COMMENT]** change term given the measurement results of the gate teleportation gadget. That raise the question whether there exists Memory codes for which one can perform the correction searching in $O(1)$ depth. [Gu+24]

4 Cues against CDFT.

So far, we discussed what might give CDFT. In this section, we briefly review results concerning the hardness of implementing logical operators fault-tolerantly at constant depth. We first present a property of stabilizer codes called disjointness [BK21], which quantifies how the structure of the code is far from being just a union of disjoint subsystems. In [BK21], they proved a relation between the disjointness value and the complexities of the logical operators that can be computed either transversally or by shallow depth circuits.

Then, we present a connection between the ability to compute Toffoli transversely and computing homomorphically [NS17]. The connection was shown to hold for a relatively wide family of codes, yet it is not generally correct for all codes. In particular, it doesn't hold for the Shor code.

4.1 The disjointness of stabilizer codes.

Definition 4.1. Let P be a logical Pauli in a stabilizer code C. Denote by $\Gamma_c(P)$ the c-disjointness of P, which is defined to be the size of the maximal subset of P-representations such that each qubit touches at most c of them, divided by c.

The c-disjointness of C is defined to be the minimum of c-disjointness, where the minimization is taken over all the logical Paulis of C.

1. **Disjointness of classical repetition code.** $= 1$
   The X_1 generator is $X^{\otimes n}$, the Z_1 generator representations are $\{Z^i \otimes I^{\otimes n/i} : i \in [n]\}$ and for Y_1 are $\{Y^i \otimes X^{\otimes n/i} : i \in [n]\}$. Thus, $\Delta_c(X_1) = \frac{1}{c}$ for any c and $\Delta_c = \frac{1}{c} \Rightarrow \Delta = 1$.
2. **Disjointness of 2D Toric code.** $\geq \frac{\sqrt{n}}{2}$.
   First notice that any two representation of Y_1 intersect in at least two qubits. (four orbits, two horizontally and two vertically.), Thus $\Delta_1(Y_1) = 1$. In addition since one can take disjoint colomuns as X_1 presentations and disjoint rows Z_1 represenations, we have that $\Delta_1(X_1) = \Delta_1(Z_1)$ is at least $\sqrt{n}$, similarly we get the same for Y_2, X_2, Z_2 and therefore, $\Delta_1 = \min \Delta_1 = 1$. Yet, for Δ_2, we have form the same argues as presented previously that $\Delta_2(X_1) = \Delta_2(Z_1) \geq \frac{1}{2}\sqrt{n}$. Ans also $\Delta_2(Y_1) \geq \frac{1}{2}\sqrt{n}$.
3. **Disjointness of the good quantum LDPC code.** $\geq \frac{\frac{1}{2}\Delta^2}{\frac{1}{2}\Delta^2 - 1}$. [5]
   Denote by Q_{ab} the subset of edges associated multiplicating by a or a^{-1} from left and multiplicating by b or b^{-1} from right namely $Q_{ab} = \{(g, agb), (g, a^{-1}gb^{-1})\}$, and consider the following edges partiiton $Q = \{Q_{ab} : a, b \in A \times A\}$. By the cleaning lemma [BT09][YC10], and the **[COMMENT]** enter here, intimidate claim., for any logical pauli g there is a represenation g_{ab} such that g' acts trivally on the qubits in Q_{ab}. Therefore, for any g the set $A(g) = \{g_{ab} : a, b \in A \times A\}$ is $\frac{1}{2}\Delta^2 - 1$-disjointness[6]. Thus the disjointness of the code is at least:
   $$\max_c \Delta_c \geq \Delta_{\frac{1}{2}\Delta^2 - 1} \geq \frac{|Q|}{\frac{1}{2}\Delta^2 - 1} = \frac{\frac{1}{2}\Delta^2}{\frac{1}{2}\Delta^2 - 1}$$
   Open-Problem 4. Does there exist a memory code that asymptotically approaches $\to 1$ disjointness?

4.2 Fault Tolerance and Homomorphic Computation.

While the source for disjointness were computational,

Definition 4.2. A quantum code is an r-fold quantum code, if it's codewords can be written as product over r subsystems:

$$|i\rangle_L = \otimes_j^r |\psi_{i,j}\rangle$$

When we think of the states in each subsystem as codewords of subcodes, note that any code is at least a 1-fold code. If each of the subcodes has distance 1, then we call the code a maximally redundant code. An example of a maximally redundant code is the Shor code.

It was shown in [NS17] that any binary code which is not a maximally redundant code cannot offer transversal logical Toffoli; otherwise, it implies the existence of a relatively low-resource consuming homomorphic protocol which violates Nayak's bound [Nay99].

[Nay99]

Open-Problem 5. Does computing Toffoli at shallow depth, similar to the transversal case, imply homomorphic computation at a cost contradicting Nayak's bound? And in a more general context, when Information Theory imposes restrictions on the depth overhead of fault tolerance?

[5] Ours.

[6] Any qubit belongs to a single Q_{ab} and therefore is not on the support of g_{ab}.

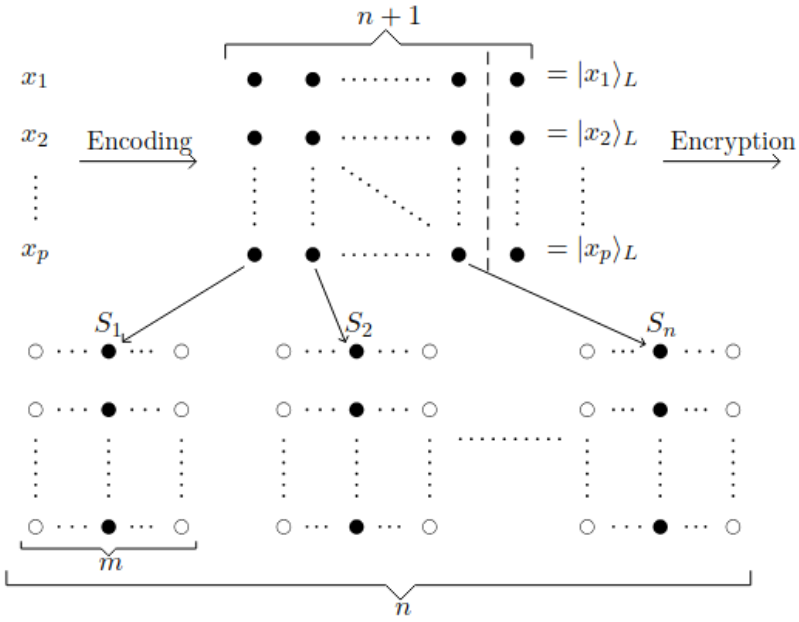

Figure 5: Skecth of the encryption scheme, taken form [NS17]

5 Summery and Applications.

Up to this point, we have tried to gets hints about whether it is likely to have a CDFT. Now we're prompted to ask: Suppose that we have an answer about the hardness of computing in the presence of noise compared to computing in an ideal environment, what can be learned beyond the context of fault tolerance? We divide our discussion into the YES scenario, in which we have CDFT, and the NO scenario, in which we don't.

5.1 The NO Scenario.

Since we know that classical computation in the presence of noise can be computed at constant overhead in depth and in particular Noise-$\mathbf{NC}_1 = \mathbf{NC}_1$, it's tempting to conclude that this scenario implies $\mathbf{NC}_1 \neq \mathbf{QNC}_1$. Yet, taking a second look points out that such a move is not so direct, and that is because of two main reasons. First, the impossibility of CDFT doesn't contradict by itself a scenario where $\mathbf{QNC}_1$ is degenerated, for example, if $\mathbf{QNC}_1 = \mathbf{QNC}_0$. Then one can close $\mathbf{QNC}_1$ to noise by mapping circuits to their constant depth equivalence first and then applying a fault tolerance scheme; the final circuit would be a fault-tolerant circuit at logarithmic depth. Second, when saying that we know how to compute classily in the presence of noise, we mean in the presence of classical noise.

Open-Problem 6. Whether and when, separation between noise classes implies separation between their ideal origins, In particular, on what conditions:

$$\mathbf{QNC}_1 \neq \text{Noisy-}\mathbf{QNC}_1 \Rightarrow \mathbf{QNC}_1 \neq \mathbf{NC}_1$$

5.2 The YES Scenario.

Having a CDFT is the first stage in realizing a quantum advantage when restricted to limited (quantum) computational power. Especially, it's required to enable computation in logarithmic depth in the setting where reset gates are not allowed. This is due to the fact that there is a trade-off between the memory of the system and the entropy accumulated, which grows exponentially with the depth [AB99]. We finish the proposal by presenting a question of engineering. We

would like to have an end-to-end realization of computation that might demonstrate quantum advantage in the limited setting without reset gates.

Open-Problem 7. Quantum Advantage Without Reset Gates. Does there exist problems believed to be hard classically but easy quantumly, which can be computed fault-tolerantly, without the use of reset gates? In particular, Is it possible to factor big integers or sampling from IQP without reset gates? What is the computational power of an ideally polynomial machine with an access to noisy-$\mathbf{QNC}_1$ machines without reset gates?

References

[Neu56] J. von Neumann. "Probabilistic Logics and the Synthesis of Reliable Organisms From Unreliable Components". In: *Automata Studies*. Ed. by C. E. Shannon and J. McCarthy. Princeton: Princeton University Press, 1956, pp. 43–98. ISBN: 9781400882618. DOI: doi:10.1515/9781400882618-003. URL: https://doi.org/10.1515/9781400882618-003.

[Pip85] Nicholas Pippenger. "On networks of noisy gates". In: *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)*. 1985, pp. 30–38. DOI: 10.1109/SFCS.1985.41.

[Aha+96] D. Aharonov et al. *Limitations of Noisy Reversible Computation*. 1996. arXiv: quant-ph/9611028 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/9611028.

[Gro96] Lov K. Grover. *A fast quantum mechanical algorithm for database search*. 1996. arXiv: quant-ph/9605043 [quant-ph].

[Sho97] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. DOI: 10.1137/s0097539795293172. URL: https://doi.org/10.1137%2Fs0097539795293172.

[AB99] Dorit Aharonov and Michael Ben-Or. *Fault-Tolerant Quantum Computation With Constant Error Rate*. 1999. arXiv: quant-ph/9906129 [quant-ph].

[Nay99] Ashwin Nayak. *Optimal lower bounds for quantum automata and random access codes*. 1999. arXiv: quant-ph/9904093 [quant-ph]. URL: https://arxiv.org/abs/quant-ph/9904093.

[BT09] Sergey Bravyi and Barbara Terhal. "A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes". In: *New Journal of Physics* 11.4 (Apr. 2009), p. 043029. DOI: 10.1088/1367-2630/11/4/043029. URL: https://dx.doi.org/10.1088/1367-2630/11/4/043029.

[YC10] Beni Yoshida and Isaac L. Chuang. "Framework for classifying logical operators in stabilizer codes". In: *Phys. Rev. A* 81 (5 May 2010), p. 052302. DOI: 10.1103/PhysRevA.81.052302. URL: https://link.aps.org/doi/10.1103/PhysRevA.81.052302.

[Got14] Daniel Gottesman. *Fault-Tolerant Quantum Computation with Constant Overhead*. 2014. arXiv: 1310.2984 [quant-ph].

[BMS17] Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. "Achieving quantum supremacy with sparse and noisy commuting quantum computations". In: *Quantum* 1 (Apr. 2017), p. 8. ISSN: 2521-327X. DOI: 10.22331/q-2017-04-25-8. URL: https://doi.org/10.22331/q-2017-04-25-8.

[NS17] Michael Newman and Yaoyun Shi. *Limitations on Transversal Computation through Quantum Homomorphic Encryption*. 2017. arXiv: 1704.07798 [quant-ph]. URL: https://arxiv.org/abs/1704.07798.

[Gro19] Antoine Grospellier. "Constant time decoding of quantum expander codes and application to fault-tolerant quantum computation". Theses. Sorbonne Université, Nov. 2019. URL: https://theses.hal.science/tel-03364419.

[BK21] John Bostanci and Aleksander Kubica. *Finding the disjointness of stabilizer codes is NP-complete*. 2021. arXiv: 2108.04738 [quant-ph]. URL: https://arxiv.org/abs/2108.04738.

[Gu+24] Shouzhen Gu et al. "Single-Shot Decoding of Good Quantum LDPC Codes". In: *Communications in Mathematical Physics* 405.3 (Mar. 2024). ISSN: 1432-0916. DOI: 10.1007/s00220-024-04951-6. URL: http://dx.doi.org/10.1007/s00220-024-04951-6.

[Pal+24] Louis Paletta et al. "Robust sparse IQP sampling in constant depth". In: *Quantum* 8 (May 2024), p. 1337. ISSN: 2521-327X. DOI: 10.22331/q-2024-05-06-1337. URL: https://doi.org/10.22331/q-2024-05-06-1337.

[Kim25] Isaac H. Kim. *Catalytic z-rotations in constant T-depth*. 2025. arXiv: 2506.15147 [quant-ph]. URL: https://arxiv.org/abs/2506.15147.