Memory.

September 29, 2025

1 Relaxation to The Fault Tolerance Model.

We are interested in the following extension to the fault-tolerant circuit model. We are equipped with an additional type; in each turn, a strong entity, which we trust, sets a hint I_t on the type. We would like to minimize $|I| := \min_t |I_t|$. In particular, a fault-tolerant construction in the standard model exhibits a fault-tolerant construction in the relaxed model with $|I| = 0$.

Another example is using the hints given by the strong entity for either deciding what correction should be applied or what 'gate-teleportation correction' should be applied. It is easy to check that previous constructions give relaxed fault tolerance such that:

1. They output encoded states with non-trivial distance.
2. They exhibit only a constant overhead in depth.
3. At each turn, $|I_t|/$ logical qubits depends on the code length.

That brings us to the following question:

Open-Problem 1. Is there a relaxed fault tolerance scheme that benefits from the first and second bullets above, yet requires a hint at a length that is constant per logical qubit? Namely:

$$\frac{|I|}{\text{logical qubits}} = O(1)?$$

2 Notations and Definitions.

Consider a code with a left k-colorized Tanner graph $\mathcal{T}$, such that any two left bits of the same color share no check. For a subset of bits S, we denote by S_{c_1} its restriction to color c_1. We use the integer Δ to denote the right degree of $\mathcal{T}$. Our computation is subject to p-depolarized noise. We denote by m the block length of the code. The decoder works as follows:

1. On the hint-type Pick a random color.

   [COMMENT] In the relaxed version: the 'right/best' color is given by the strong entity.

2. For any (q)bit at that color, check if flipping it decreases the syndrome. If so, then flip it.

Claim 2.1. Let $\mathcal{T}$ be a Tanner graph such that $\Delta > 2k$. There is $p_0 \in (0,1)$ and $q \in (0,1)$ such that for any $p < p_0$ and a density ρ, which is subjected to q-local stochastic noise, there is a color c_1 such that after a cycle of absorbing p-depolarized noise and correcting according to the decoding rule when color $= c_1$, the resulting state ρ' will remain subjected to q-local stochastic noise.

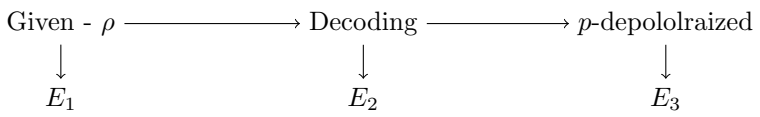

Figure 1: Illustration of the cycle.

2.1 Proof.

First, let's bound the probability that the error after the decoding round (E_2) is supported on S. (We use here the fact that views of the bits through their stabilizer don't overlap since we took only bits of the same color for the decoding.)

$$\mathbf{Pr}\left[\mathbf{Sup}\left(E_2\right)=S\right] \leq \mathbf{Pr}\left[\text{any bit } v \in S_{c_1} \text{ sees majority of satisfied checks }\right] \leq q^{\frac{1}{2}\Delta|S|_{c_1}}$$

Now, to roughly analyze the error after observing a round of p-depolarized noise, we consider a model in which new errors due to the depolarized channel don't correct previous errors. Thus, we get:

$$\mathbf{Pr}\left[\mathbf{Sup}\left(E_3\right)=S\right] \leq \sum_{S' \subset S} q^{\frac{1}{2}\Delta|S'|_{c_1}} p^{|S/S'|}$$

On the other hand,

$$\sum_{c_i} |S|_{c_i} = k \cdot \mathbf{E}\left[|S|_{c_i}\right] = |S|$$

$$\Rightarrow \max_{c_i} |S|_{c_i} \geq \frac{1}{k}|S|$$

So if c_1 is the color that maximizes $|S|_{c_1}$, then:

$$\begin{aligned}\mathbf{Pr}\left[\mathbf{Sup}\left(E_3\right)=S\right] &\leq \sum_{S' \subset S} q^{\frac{1}{2}\Delta|S'|/k} p^{|S/S'|} \\ &\leq \left(q^{\frac{1}{2k}\Delta}+p\right)^{|S|} \leq q^{|S|}\end{aligned}$$

3 Suitable Codes.

We first show that the partition code has a representation (a check matrix) for which the induced $\mathcal{T}$ satisfies the relation $\Delta > 4k$, and then show that the hypergraph product code defined by multiplying the Tanner graphs of that representation gives $\Delta > 2k$.

Claim 3.1. Let C be a code with a Tanner graph $\mathcal{T}$. Denote by $\mathcal{T}^\top$ the Tanner graph of the transpose code and by $Q\left(\mathcal{T} \times \mathcal{T}^\top\right)$ the Tanner graph obtained by the hypergraph product. Then:

1. $\Delta\left(Q\left(\mathcal{T} \times \mathcal{T}^\top\right)\right) = \max\{\Delta(\mathcal{T}), \Delta(\mathcal{T}^\top)\}$
2. $k\left(Q\left(\mathcal{T} \times \mathcal{T}^\top\right)\right) \leq k(\mathcal{T}) + k(\mathcal{T}^\top)$

Proof. Easy. □

Claim 3.2. The repetition code has a representation for which $\Delta > 4k$.

Proof. Denote by H_0 the checks obtained by treating the repetition code as a Tanner code over the cyclic graph. Observe that $k_0 = 2$ and $\Delta_0 = 2$.

Now, let V^+, V^- be a partition of the bits according to their color. Any check of the form $v^+ + v^-$ where $v^\pm \in V^\pm$ agrees with the coloring. So, by adding a perfect matching, we increase Δ by 1 and keep the colorization. We have $\sim n/2!$ such matchings, so we can add 100Δ and get the correction of the claim.

Furthermore, the length of the transposed code increases by the number of checks we add, and its distance can't decrease. So, we get that the parameters of the transposed code are $[n+100\Delta n, 1, \geq n]$. □

Hence, we have a simple code that can serve as memory in the relaxed setting. Yet, it doesn't provide a solution to the problem since the dimension of the code is non-trivial[1]:

$$K_Q = K_1 K_2 + K_1^\top K_2^\top \geq O(1) + \Theta(n)$$

Thus, we will still need to perform a non-trivial computation for the gate-teleportation gadget.

[COMMENT] In fact, since $\dim \mathcal{T}^\top \geq |C| - |V|$ and $|V|\Delta = |C|\Delta_2 \leq |C|k \leq |C|\frac{1}{2}\Delta$ we get that $\dim \mathcal{T}^\top \geq \Theta(n)$. For the hypergraph product. .

$$\frac{1}{2}\Delta \leq (1-\varepsilon)\Delta \leq \frac{\Delta}{k} \leq \frac{\Delta}{\Delta_2} \leq \frac{|\Gamma(A)|}{|A|}$$

Question. Consider the n-dimensional toric code, where qubits are placed on k-cells of the n-dimensional hypercubic lattice. For an i-cell, denote by Δ_i^+ the number of $(i+1)$-cells adjacent to it, and by Δ_i^- the number of $(i-1)$-cells adjacent to it. For which values of k do both of the following strict inequalities hold?

$$\Delta_k^+ > \Delta_{k+1}^-, \qquad \Delta_k^- > \Delta_{k-1}^+.$$

Answer. In an n-dimensional hypercubic lattice one has

$$\Delta_i^+ = 2\,(n-i), \qquad \Delta_i^- = 2\,i.$$

Therefore, the two inequalities become

$$2(n-k) > 2(k+1) \quad \Longleftrightarrow \quad k < \tfrac{n-1}{2},$$
$$2k > 2\big(n-(k-1)\big) \quad \Longleftrightarrow \quad k > \tfrac{n+1}{2}.$$

These conditions are mutually exclusive, since they require simultaneously

$$k < \frac{n-1}{2} \quad \text{and} \quad k > \frac{n+1}{2}.$$

Thus, there is no value of k (for any dimension n) for which both inequalities hold at once.

Yet, if one is willing to satisfy only the first inequality. Then:

$$1 < \frac{\Delta_k^-}{\Delta_{k-1}^+} = \frac{2k}{2(n-(k-1))} \to k > \frac{2}{3}n$$

Should be verified:

1. In addition the dimension of the code should be $\binom{n}{k}$. (Also known as the Betti numbers).
2. Numebr of k-cells shared by a j - cell and a i -cell. $\binom{j-i}{k-i}$.
3. The partiy of $\binom{2l}{l}$.
4. should understand: Math stachexhange.

[1] Can be decreased to $\Theta(\sqrt{n})$ if we choose $C_1 = C$ and C_2 to be the transposed code instead of choosing $C_1 = C_2 = C$.

4 Amplification.

Claim 4.1. Consider the tanner graph of the classic code C_X which can be used to construct a quantum LDPC code. For any constant $c \in (0,1)$ there exist $\gamma < c$ and a subset of qubits B at size $B = \gamma n < cn$ such that $|\Gamma(B)| < \frac{1}{2}\Delta B$.

Proof. Easy. □

Now consider the following construction, we pick $c = \frac{1}{\Delta^2}$, and B at size lower than γn, denote by A the complement of B. Now pick Θ hash functions $\Theta = \{h : \Gamma(A) \to \Gamma(B)/\Gamma(A)\}$. One one hand:

$$\begin{aligned}\frac{|\Gamma(A)|}{|\Gamma(B)/\Gamma(A)|} &\geq \frac{|\Gamma(A)|}{|\Gamma(B)|} \geq \frac{|\Gamma(A)|}{\frac{1}{2}\Delta|(B)|} \\ &\geq \frac{(1-\gamma)\,n}{\frac{1}{2}\gamma n} \geq 2\Delta(1-\frac{1}{\Delta}) \geq \Delta\end{aligned}$$

In addition, $|\Gamma(B)/\Gamma(A)| \cdot \Delta_2 \geq |B| \Rightarrow |\Gamma(B)/\Gamma(A)| \geq |B|/\Delta_2$ and hence:

$$\frac{|\Gamma(A)|}{|\Gamma(B)/\Gamma(A)|} \leq \frac{|\Gamma(A)|\Delta_2}{|B|} \leq \frac{|A|}{|B|}\Delta\Delta_2$$

Notice that if for any B at the range $(1/\Delta^3, 1/\Delta^2)n$ we have that $|\Gamma(B)| \geq \frac{1}{2}\Delta|B|$ then it means that there is no codeword in C_X at weight $(1/\Delta^3, 1/\Delta^2)n$, thus we if use the (n,k)-Toric we can also finds B at size $\geq 1/\Delta^3 n$.

We add the following checks $X_i \cdot X_{\theta(i)}$. The degree of the bits changes as follow:

1. If $v \in A$ then: $\Delta(v) = \Delta + |\Theta|\Delta$
2. Else, namely $v \in B$, denote by Δ_l, Δ_r the degree of v when restricted to $\Gamma(A)/\Gamma(B)$ and $\Gamma(B)/\Gamma(A)$,and define $\xi = \Delta_l|\Theta| + \Delta_r|\Theta| \cdot \left(\frac{|\Gamma(A)|}{|\Gamma(B)/\Gamma(A)|}\right)^{-1}$ then: $\Delta + \xi \geq \Delta(v) \geq \Delta + \frac{1}{2}\xi$.

5 Classical Case, Repetition Code.

In each decoding iteration, we pick random triples and set the values of their bits to the majority. Now, assume that the probability of a subset S being an error is less than $q^{|S|}$, and denote by X_i the random variable that counts the number of triples for which i of their bits belong to S. On one hand:

$$|S| = \sum_i iX_i = X_1 + 2X_2 + 3X_3$$

On the other, after a decoding cycle the probability of an error is:

$$\mathbf{Pr}\left[E_2 = S\right] = q^{2X_1+2X_2+2X_3} = q^{|S|+X_1-X_3}$$

Now for $|S| \leq n/3$ we have that $\mathbf{E}\left[X_1 - X_3\right] \geq |S|/4$. **[COMMENT]** Require proof.

So, we find that after a cycle of correction and p-depolarized noise accumulation, we have:

$$\mathbf{Pr}\left[E_3 = S\right] \leq \left(q^{\frac{5}{4}} + p\right)^{|S|} \leq q^{|S|}$$

And if the distance of any small check is d, then we would find that the exponent of q is:

$$|S| + \sum_{i=1}^{d}(d-i)\,X_i - \sum_{i=d+1}^{\Delta}(i-d)\,X_i$$

For expander checking[2], we have that having an error over $|S|$ qubits after a correction round implies that the error spread over $(1+\varepsilon)|S|$[3]. Thus, we get that with high probability:

$$\leq \left(q^{1+\varepsilon}/\left(1-o(f)\right)+p\right)^{|S|}$$

6 Another Decoder.

Consider the follow decoder: Any bit picks two random checks adjoin to it. If they both unsatisfied it flips itself. The idea, is that we might control the amount of independence.

Let X_u^v be the indicator, indicating that the bits v and u choose checks that share a bit, we call it a collision, To compute he expected number of collisions, we define the graph given by 4-steps walk over the Tanner graph. Then:

$$\sum \mathbf{E}\left[X_u^v\right] = \frac{1}{\Delta^2}\cdot 1_S^\top A_G 1_S \leq \frac{1}{\Delta^2}\frac{\left(\Delta\Delta_2\right)^2|S|^2}{n} + \frac{1}{\Delta^2}\lambda\left(\Delta\Delta_2\right)^2|S|$$

Where S is the subsets of the faulty bits. So if the 4-steps graph is Ramanujan, namely $\lambda \approx \Delta\Delta_2$:

$$\approx \frac{\Delta_2^2|S|}{n} + \frac{\Delta_2}{\Delta}|S| \to \frac{\Delta_2}{\Delta}|S|$$

It's even easier to bound the expectation of the pairs u and v which share the same check. So given a checks choice, we have that the probability of error to kept:

$$\sim q^{\left(2-\frac{\Delta_2}{\Delta}\right)|S|}$$

Conditioned on the case that the number of collision is not far from the expectation.

7 Concentration in Local Stochastic Noise.

Denote by μ the expected flips, and by $\alpha, \beta < 1$ marginal parameters such the volume of picking $(\mu-\beta, \mu+\beta)$ is larger than picking $(\geq \mu+\alpha)$.

$$\begin{aligned}\mathbf{Pr}\left[\frac{|S|}{n} \geq \mu+\alpha\right] &\leq \sum_{m\geq\mu+\alpha} C q^{n(\mu+\alpha)} \leq q^{n(\alpha-\beta)} \sum_{m\geq\mu+\alpha} \star \\ &\leq q^{n(\alpha-\beta)}\mathbf{Pr}\left[|\frac{|S|}{n}-\mu| \leq \beta\right]\end{aligned}$$

Other way, first use the Markov inequality to bound the space that $\geq n\alpha$ so we get $\geq \frac{1}{2}\cdot\frac{1}{\alpha}\cdot 2^n$, and then use the local stochastic property:

$$\leq C\frac{\frac{1}{2}}{\alpha}\cdot 2^n \cdot q^{\alpha n} = \frac{\alpha}{2}C\left(2q^\alpha\right)^n$$

For big enough α we see that the probability decay exponentially. (An also way to prove that $q^q \geq \frac{1}{2}$).

[2]Two rounds of fixed checks are taken such that the parity check matrix is an expander according to some expansion measure.

[3]Conditioned on the assumption that in the previous moment for the decoding there were fewer than γn faulty bits.

8 Bounding $E(S,S)$, fixed $|S|$, by Branuli Process.

First, consider $\mathcal{D}$ that pick any vertex in probability $|S|/n + \varepsilon$. With hight probability all the assignments mark more than $|S|$ vertices. Denote by $\tilde{S}$ the drawn vertices, with high probability $E(S,S) \leq E(\tilde{S},\tilde{S})$, just by monotonically. On the other hand:

$$\mathbf{E}\left[E(S,S)\right] \leq (1-o(\star))\,\mathbf{E}\left[E(\tilde{S},\tilde{S})\right] \leq (1-o(\star))\sum_{i\sim j} A_{ij}\mathbf{E}\left[x_i x_j\right] \approx \left(\frac{|S|}{n}+\varepsilon\right)^2 \cdot \Delta|S|$$

In particular if $|S|/n \leq \delta$ then:

$$\mathbf{E}\left[E(S,S)\right] \approx\leq (\delta+\varepsilon)^2\Delta|S|$$

Math-exchange concentration. https://www.cs.columbia.edu/ djhsu/coms4773-s24/lectures/mcdiarmid.pdfMcdiarn