A TEMPLATE FOR ARXIV STYLE *

Author1, Author2
Affiliation
Univ
City
`{Author1, Author2}email@email`

Author3
Affiliation
Univ
City
`email@email`

ABSTRACT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

***K*eywords** First keyword · Second keyword · More

1 Introduction

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris. Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

2 Background

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. See Section 2.

2.1 Small Set Flip

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue

* *Citation*: **Authors. Title. Pages.... DOI:000000/11111.**

quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

$$\xi_{ij}(t) = P(x_t = i, x_{t+1} = j | y, v, w; \theta) = \frac{\alpha_i(t) a_{ij}^{w_t} \beta_j(t+1) b_j^{v_{t+1}}(y_{t+1})}{\sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i(t) a_{ij}^{w_t} \beta_j(t+1) b_j^{v_{t+1}}(y_{t+1})} \tag{1}$$

2.1.1 Headings: third level

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Paragraph Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

3 Algorithm: K-Top Probabilistic Flip Method (K-Top PFM)

Algorithm 1: `sort-top-K(T)`

Data: A vector $T \in \mathbb{Z}_2^N$
Result: A set S of the top K indices in T

$S \leftarrow$ `indices of a descending radix sort of` T`'s rows`;
return A set of the top K indices in S;

Algorithm 2: `probabilistic-set-flip(`E`)`

Data: A syndrome $\sigma_0 \in \mathbb{F}_2^M$
Result: Deduced error $\widehat{E}$ if the algorithm converges and $\perp$ otherwise

$\widehat{E} \leftarrow 0^N$;
$\sigma \leftarrow \sigma_0$;
while $\exists F \in \mathscr{F} : |\sigma| - |\sigma \oplus \sigma_X(\boldsymbol{k})| > 0$ **do**
    $T \leftarrow H_Z H_X^T \sigma$;
    `generators` $\leftarrow$ `sort-top-K`(T);
    `to-check` $\leftarrow \bigcup_{i \in \texttt{generators}} \mathcal{P}(\mathcal{C}_{Z\,i})$;
    $\boldsymbol{k} \leftarrow \arg\max_{\boldsymbol{k} \in \texttt{to-check}} \frac{|\sigma| - |\sigma \oplus \sigma_X(\boldsymbol{k})|}{|\boldsymbol{k}|}$;
    $\widehat{E} \leftarrow \widehat{E} \oplus \boldsymbol{k}$;
    $\sigma \leftarrow \sigma \oplus \sigma_X(\boldsymbol{k})$;
end
return $\widehat{E}$ if $|\sigma| = 0$, $\perp$ otherwise.

3.1 A Moral Reason/ Intuition

The algorithm is essentially the same as Small Set Bit Flip [TODO: CITE] with a minor difference, only a constant number of generators are checked. The idea here is that given a syndrome σ and a parity check matrix, H_X, the ith row of $H_X^T \sigma$ equals the number of error-ed checks that a qubit touches. Then, the kth row of $H_Z H_X^T \sigma$ is roughly correlated to the number of error-ed checks that the qubits in the kth generator touch. This rough correlation comes from the fact that we are working with expander codes. So then, if you get the generators touching the most error-ed stabilizers, it would stand to reason that flipping some subset of qubits from a “highly error-ed generator" would result in decreasing the syndrome.

4 PFM Analysis

The following section assumes that we are working with syndrome $\boldsymbol{\sigma_X}$, a generator matrix H_Z, and parity check matrix H_X. The analysis is the same for a syndrome, $\boldsymbol{\sigma_Z}$, generator matrix H_X, and parity check matrix H_Z.

Notation

Given a vector $\boldsymbol{v}$, define v_i to be the value of the ith row of $\boldsymbol{v}$.

Definitions

Let $\Delta_{\text{stablizer}}$ equal to the degree of a stabilizer vertex. Note that due to the hypergraph's construction, all stabilizers have the same constant degree. Let Δ_{bit} equal to the degree of a qubit vertex. As with the stabilizers, all qubits have the same constant degree. Also, for generator k, let $\aleph$ be the set of stabilizers neighboring the generator. Note that $|\aleph| \leq \Delta_{\text{stablizer}}\Delta_{\text{bit}}$.

Given a syndrome, $\boldsymbol{\sigma_X}$, define a “bit-score vector", $\boldsymbol{b} = H_X^T\boldsymbol{\sigma_X}$ where $\boldsymbol{b} \in \mathbb{Z}^N$. Then, define a “generator-score vector" as $\boldsymbol{g} = H_z\boldsymbol{b}$ where $\boldsymbol{g} \in \mathbb{Z}^M$. Moreover, assume that for error $e \in \mathbb{F}_2^N$, $\mathbf{Pr}[e_i = 1] = p$ for all $i \in [N]$ (i.e. the error is modeled as independent). Let $q = 1 - p$. Let $s_1, s_2, ..., s_M$ denote the set of stabilizer vertices. Let $N_i = \sum_{j\in\Gamma(s_i)} \boldsymbol{e}_j$ where $N_i \in \mathbb{Z}$. N_i can be thought of as the number of qubits with an error in the neighborhood of stabilizer i.

Also, let random variable $S_i \in F_2$ correspond to $\boldsymbol{\sigma_X}_i$. Then we know that

$$\mathbf{Pr}[S_i = 1] = \mathbf{Pr}[N_i \texttt{ is odd}] = \tfrac{1}{2} - \tfrac{1}{2}(1-2p)^{\Delta_{\text{stablizer}}}.$$

Next, define indicator random variable, L_j to be 1 if $\boldsymbol{\sigma_X}_i = 0$ and $N_i > 0$. Basically, L_j indicates whether a stabilizer check succeeds, but an error is in its neighborhood. I.e. stabilizer j is “lying."

So then,

$$\begin{aligned}\mathbf{Pr}[L_j = 1] &= \mathbf{Pr}[\boldsymbol{\sigma_X}_i = 0 \mid S_i > 0] \\ &= \mathbf{Pr}[S_i \texttt{ is even}] - \mathbf{Pr}[S_i = 0] \\ &= \tfrac{1}{2} + \tfrac{1}{2}(1-2p)^{\Delta_{\text{stablizer}}} - (1-p)^{\Delta_{\text{stablizer}}}.\end{aligned}$$

Then define random variable, E_k to be

$$E_k = \sum_{\texttt{Stabilizer } j \in \aleph_k} L_j.$$

E_k is basically the number of time a generator k, lies for all stabilizers neighboring the generator.

We can then say that

$$E_k \sim \texttt{Binom}(\aleph_k, \tfrac{1}{2} + \tfrac{1}{2}(1-2p)^{\Delta_{\text{stablizer}}} - (1-p)^{\Delta_{\text{stablizer}}}).$$

Then, let random variable $B_i \in \mathbb{Z}$ correspond to $\boldsymbol{b}_i$ and random variable $G_i' \in \mathbb{Z}$ correspond to $\boldsymbol{g}_i$.

So,

$$S_i \sim \texttt{Bernoulli}\Big(\tfrac{1}{2} - \tfrac{1}{2}(1-2p)^{\Delta_{\text{stablizer}}}\Big).$$

Then,

$$B_i = \sum_{\texttt{Stabilizer } j \in \Gamma(\texttt{Bit } i)} S_j$$

So,

$$B_i \sim \texttt{Binom}(\Delta_{\text{bit}}, \tfrac{1}{2} - \tfrac{1}{2}(1-2p)^{\Delta_{\text{stablizer}}}).$$

And then,

$$G'_k = \sum_{\texttt{Bit } i \in \Gamma(\texttt{generator } k)} \sum_{\texttt{Stabilizer } j \in \Gamma(\texttt{Bit } i)} S_j$$

So then,

$$G'_k \sim \texttt{Binom}(\Delta_{\text{bit}}\Delta_{\text{stablizer}}, \tfrac{1}{2} - \tfrac{1}{2}(1-2p)^{\Delta_{\text{stablizer}}}).$$

The pfm algorithm (Algorithm 2) on line 5 gets the K generators, indexed by $g_1, g_2, ..., g_K$, with the top values of $\boldsymbol{g}_i$ for $i \in [M]$. WLOG, assume $\boldsymbol{g}_{g_1} \geq \boldsymbol{g}_{g_2} \geq ... \geq \boldsymbol{g}_{g_K}$. Then, we can think of $\mathbf{E}[G'_{g_i}]$ as the expected value of the ith top sample from M samples of the distribution defining G'_i.

Let random variable G_k then equal

$$G_k = \sum_{\texttt{Stabilizer } j \in \aleph_k} S_j.$$

Note that $|\aleph| \geq (1-\delta)\Delta_{\text{stablizer}}\Delta_{\text{bit}}$ because we are working with expander codes. So then,

$$\begin{aligned}\mathbf{E}[G_k] &= \sum_{\texttt{Stabilizer } j \in \aleph_k} \mathbf{E}[S_j] \\ &\geq (1-\delta)\Delta_{\text{stablizer}}\Delta_{\text{bit}} \mathop{\mathbf{E}}_{j\in[M]}[S_j] \\ &\geq (1-\delta)\,\mathbf{E}[G'_k].\end{aligned}$$

Lemma 4.1. *For a generator, given E_k and G, we can find some correction vector $\boldsymbol{k} \in \mathbb{F}_2^N$ such that $|\sigma| - |\sigma \oplus \sigma_X(\boldsymbol{k})| \geq G_k - E_k$ and $|k| \leq \frac{1-\delta}{\Delta_{bit}}(G_k + E_k)$ for $G > E_k$.*

Proof. TODO: part 1 is that there are 3 types of stabilizers in neighbourhood. Those from G', those from E, and those in neither. If those in neither, there is no neighbourhood in their error, so you can leave those bits alone. Then, by flipping bits connected to G' you decrease syndrome by G', but you add in at most E'

part 2: each flipping bit effects at least (1-delta) Δ_{bit}stables ☐

So then for any $\boldsymbol{e}$ where $|\boldsymbol{e}| < \min(\gamma_A n_A, \gamma_B n_B)$ by TODO: cite hypergraph prod paper, we know that we can always successfully correct errors if we can find a $\boldsymbol{k}$ such that $\boldsymbol{k}$ is a subset of a generator and

$$\frac{|\sigma| - |\sigma \oplus \sigma_X(\boldsymbol{k})|}{|\boldsymbol{k}|} \geq \frac{1}{3}.$$

Lemma 4.2. *We claim the following holds for an $i \in [K]$ and for $p_S = \mathbf{Pr}[S_j = 1]$ for any stabilizer j*

$$\begin{aligned}&\mathbf{Pr}\left[\frac{\Delta_{bit}(Gg_i - E_{g_i})}{(1-\delta)(Gg_i + E_{g_k})} < \frac{1}{3}\right] \\ &\leq \sum_{e=0}^{\Delta_{bit}-1} \text{orderprob}\left(\Delta_{bit}\Delta_{stablizer} - \Delta_{stablizer}e, p_S, i, \frac{(3\Delta_{bit} + 1 - \delta)e}{3\Delta_{bit} - 1 + \delta}\right) \cdot \mathbf{Pr}[E_{g_i} = e] + \sum_{e=\Delta_{bit}}^{\Delta_{bit}\Delta_{stablizer}} \mathbf{Pr}[E_{g_i} = e]\end{aligned}$$

where

$$\text{orderprob}(n, p, i, v) = \mathbf{Pr}[W_i \leq v]$$

and W_i is the ith largest order statistic from M samples of $\texttt{Binomial}(n, p)$.

See appendix TODO: cite for details

So then,

$$\mathbf{Pr}[\texttt{loop cannot find a correcting error}] \leq \prod_{i\in[K]} \mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(Gg_i - E_{g_i})}{(1-\delta)(Gg_i + E_{g_k})} < \frac{1}{3}\right]$$

lemma 4.1,

5 PFM Numerical Simulations

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. See Section 2.

6 PFM Future Outlook

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. See Section 2.

7 Conclusion

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. See Section 2.

8 Acknowledgments

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula. See Section 2.

9 Examples of citations, figures, tables, references

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui. [1, 2] and see [3].

The documentation for `natbib` may be found at

`http://mirrors.ctan.org/macros/latex/contrib/natbib/natnotes.pdf`

Of note is the command `\citet`, which produces citations appropriate for use in inline text. For example,

```
\citet{hasselmo} investigated\dots
```

produces

> Hasselmo, et al. (1995) investigated…

`https://www.ctan.org/pkg/booktabs`

9.1 Figures

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam

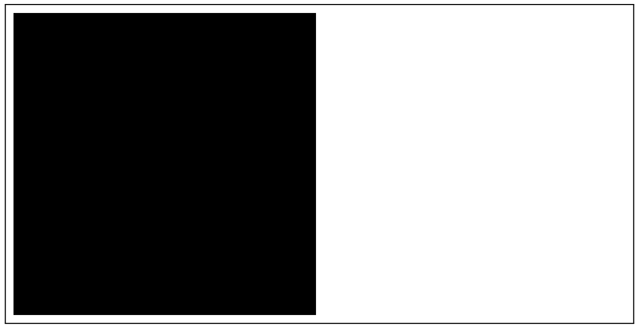

Figure 1: Sample figure caption.

Table 1: Sample table title

Part		
Name	Description	Size (μm)
Dendrite	Input terminal	$\sim$100
Axon	Output terminal	$\sim$10
Soma	Cell body	up to 10^6

elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi. See Figure 1. Here is how you add footnotes. [2] Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

9.2 Tables

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo. See awesome Table 1.

9.3 Lists

- Lorem ipsum dolor sit amet
- consectetur adipiscing elit.
- Aliquam dignissim blandit est, in dictum tortor gravida eget. In ac rutrum magna.

10 Conclusion

Your conclusion here

Acknowledgments

This was was supported in part by......

[2] Sample of the first footnote.

References

[1] George Kour and Raid Saabne. Real-time segmentation of on-line handwritten arabic script. In *Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on*, pages 417–422. IEEE, 2014. 9

[2] George Kour and Raid Saabne. Fast classification of handwritten on-line arabic characters. In *Soft Computing and Pattern Recognition (SoCPaR), 2014 6th International Conference of*, pages 312–318. IEEE, 2014. 9

[3] Guy Hadash, Einat Kermany, Boaz Carmeli, Ofer Lavi, George Kour, and Alon Jacovi. Estimate and replace: A novel approach to integrating deep neural networks with existing applications. *arXiv preprint arXiv:1804.09028*, 2018. 9

A Proof of Lemma 4.1

First, to just restate the lemma. We claim the following holds for an $i \in [K]$ and for $p_S = \mathbf{Pr}[S_j = 1]$ for any stabilizer j

$$\begin{aligned}
&\mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(Gg_i - E_{g_i})}{(1-\delta)(Gg_i + E_{g_k})} < \frac{1}{3}\right] \\
&\leq \sum_{e=0}^{\Delta_{\text{bit}}-1} \text{orderprob}\left(\Delta_{\text{bit}}\Delta_{\text{stablizer}} - \Delta_{\text{stablizer}}e, p_S, i, \frac{(3\Delta_{\text{bit}}+1-\delta)e}{3\Delta_{\text{bit}}-1+\delta}\right) \cdot \mathbf{Pr}[E_{g_i} = e] + \sum_{e=\Delta_{\text{bit}}}^{\Delta_{\text{bit}}\Delta_{\text{stablizer}}} \mathbf{Pr}[E_{g_i} = e]
\end{aligned}$$

where

$$\text{orderprob}(n, p, i, v) = \mathbf{Pr}[v < (1-\delta)W_i]$$

and W_i is the ith largest order statistic from M samples of $\texttt{Binomial}(n, p)$.

First, because $0 \leq E_{g_i} \leq \Gamma(\texttt{generator i}) \leq \Delta_{\text{bit}}\Delta_{\text{stablizer}}$,

$$\begin{aligned}
\mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(Gg_i - E_{g_i})}{(1-\delta)(Gg_i + E_{g_k})} < \frac{1}{3}\right] &= \sum_{e=0}^{\Delta_{\text{bit}}\Delta_{\text{stablizer}}} \mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(G_{g_i} - e)}{(1-\delta)(G_{g_i} + e)} < \frac{1}{3}\right] \mathbf{Pr}[E_{g_i} = e] \\
&\leq \sum_{e=0}^{\Delta_{\text{bit}}-1} \mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(G_{g_i} - e)}{(1-\delta)(G_{g_i} + e)} < \frac{1}{3}\right] \mathbf{Pr}[E_{g_i} = e] + \sum_{e=\Delta_{\text{bit}}}^{\Delta_{\text{bit}}\Delta_{\text{stablizer}}} 1 \cdot \mathbf{Pr}[E_{g_i} = e] \\
&= \sum_{e=0}^{\Delta_{\text{bit}}-1} \mathbf{Pr}\left[G_{g_i} < \frac{(3\Delta_{\text{bit}}+1-\delta)e}{3\Delta_{\text{bit}}-1+\delta}\right] \mathbf{Pr}[E_{g_i} = e] + \sum_{e=\Delta_{\text{bit}}}^{\Delta_{\text{bit}}\Delta_{\text{stablizer}}} 1 \cdot \mathbf{Pr}[E_{g_i} = e].
\end{aligned}$$

So then, for a given e, we just need to find an upper bound for

$$\mathbf{Pr}\left[G_{g_i} < \frac{(3\Delta_{\text{bit}}+1-\delta)e}{3\Delta_{\text{bit}}-1+\delta}\right].$$

We can then use Chebyshev inequality to get an upper bound of

$$\min\left(\frac{\mathbf{Var}[G_{g_i} \mid E_{g_i} = e]}{\left[\mathbf{E}[G_{g_i} \mid E_{g_i} = e] - \frac{1}{3}\right]^2}, 1\right)$$

if $\mathbf{E}[G_{g_i}] > \frac{1}{3}$ and an upper bound of 1 otherwise.

Then, we need to related G_{g_i} to G'_{g_i} as our algorithm only know G'_{g_i}.

Lemma A.1. $\mathbf{E}[G_{g_i} \mid E_{g_i} = e] \geq \mathbf{E}[G'_{g_i} \mid E_{g_i} = e] \cdot \left(1 - \frac{\Delta_{stablizer}-1}{N}\right)$

Proof. Fix $E_{g_i} = e$. Then, let $\alpha = G'_{g_i}$ and $\aleph = \{\, j \in [M] : S = 1 \,\}$. Note that $G_{g_i} = |\aleph|$ by definition of G_{g_i}. We then know that $\alpha \geq |\aleph|$ because α counts each stabilizer in $s \in \Gamma(\texttt{generator i})$ where $S_s = 1$ at least once. For $s \in \aleph$, let

$$O_s = |\,\{\, k : k \in \texttt{generator } i \wedge s \in \Gamma(\texttt{bit k}) \,\}\,| - 1.$$

In other words, O_s is the number of times a stabilizer in the neighborhood of a generator is "over-counted" in α. Then, $|\aleph| = \alpha - \sum_{s \in \aleph} O_s$ because we are subtracting the total number of "over-counted" stabilizers. Then, note that

$$\begin{aligned}
\mathbf{E}[O_s] &= \sum_{b \in \Gamma(s)} \mathbf{Pr}[b \in \texttt{generator i}] - 1 \\
&= 1 + \sum_{b \in \Gamma(s) \setminus t} \mathbf{Pr}[b \in \texttt{generator i}] - 1 \qquad \text{(at least 1 } t \in \Gamma(s) \text{ must be in } \texttt{generator i}\text{)} \\
&= (\Delta_{\text{stablizer}} - 1)\frac{1}{N}
\end{aligned}$$

for some $s \in \aleph$ and $t \in \Gamma(s)$. So then,

$$\begin{aligned}\mathbf{E}[|\aleph|] &= \mathbf{E}[\alpha] - \sum_{s\in\aleph} \mathbf{E}[O_s] \\ &\geq \mathbf{E}[\alpha] - \mathbf{E}[|\aleph|] \mathop{\mathbf{E}}_{s\in\aleph}[O_s] \\ &\geq \mathbf{E}[\alpha] - \mathbf{E}[\alpha] \mathop{\mathbf{E}}_{s\in\aleph}[O_s] \\ &\geq \mathbf{E}[\alpha]\left(1 - \frac{\Delta_{\text{stablizer}} - 1}{N}\right).\end{aligned}$$

□

So then, lets define

$$G^e \sim \texttt{Binomial}(\Delta_{\text{stablizer}}\Delta_{\text{bit}} - \Delta_{\text{stablizer}}e, p_S)$$

and, for $i \in [K]$, $G^e_{k_i}$ to be the top ith order statistic from M samples.

Lemma A.2. $\mathbf{E}[G'_{g_i} \mid E_{g_i} = e] \geq \mathbf{E}[G^e_{k_i}]$

Proof. If $E_{g_i} = e$, we also know that for some $s_1, s_2, ..., s_e \in \aleph$, $S_{s_j} = 0$ for $j \in [e]$. So then, given e, G'_{g_i} is the ith largest sample of M from $\texttt{Binomial}(\Delta_{\text{stablizer}}\Delta_{\text{bit}} - c\Delta_{\text{stablizer}}e, p_S)$ for some $0 < c \leq 1$. This is true because each stabilizer, s_j, that must be 0 neighbors at most $\Delta_{\text{stablizer}}$ bits in generator i and neighbors at least one bit in generator i. □

Lemma A.3. $\mathbf{Var}[G'_{g_i}] \geq \mathbf{Var}[G_{g_i} \mid E_{g_i} = e]$

Proof. First, we need to show that $\mathbf{Var}[G'_{g_i} \mid E_{g_i}] \geq \mathbf{Var}[G_{g_i} \mid E_{g_i} = e]$. This can be seen easily because

$$\mathbf{Var}[G_{g_i} \mid E_{g_i}] = \mathbf{E}[(G_{g_i} \mid E_{g_i})^2] - \mathbf{E}[G_{g_i} \mid E_{g_i}]^2$$

□

Finally, we get that

$$\mathbf{Pr}\left[G_{g_i} < \frac{(3\Delta_{\text{bit}} + 1 - \delta)e}{3\Delta_{\text{bit}} - 1 + \delta}\right] \leq \min\left(\frac{\mathbf{Var}[G'_{g_i}]}{\left[\mathbf{E}[G^e_{k_i}] - \frac{1}{3}\right]^2}, 1\right)$$

and that

$$\mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(Gg_i - E_{g_i})}{(1-\delta)(Gg_i + E_{g_k})} < \frac{1}{3}\right] = \sum_{e=0}^{\Delta_{\text{bit}}-1} \min\left(\frac{\mathbf{Var}[G'_{g_i}]}{\left[\mathbf{E}[G^e_{k_i}] - \frac{1}{3}\right]^2}, 1\right)\mathbf{Pr}[E_{g_i} = e] + \sum_{e=\Delta_{\text{bit}}}^{\Delta_{\text{bit}}\Delta_{\text{stablizer}}} 1 \cdot \mathbf{Pr}[E_{g_i} = e].$$

Then, also observe that, for a fixed $E_{g_k} j$,

$$\mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(G''g_i - E_{g_i})}{(1-\delta)(G''g_i + E_{g_k})} < \frac{1}{3}\right] \geq \mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(Gg_i - E_{g_i})}{(1-\delta)(Gg_i + E_{g_k})} < \frac{1}{3}\right]$$

if $\mathbf{E}[G''_{g_i}] < TODO: thethingwewant$ $\mathbf{E}[G''_{g_i}] \leq \mathbf{E}[G_{g_i}]$, $\frac{\mathbf{Var}[G''_{g_i}]}{\mathbf{Var}[G'_{g_i}]} \geq \frac{\mathbf{E}[G'_{g_i}]}{\mathbf{E}[G''_{g_i}]}$, TODO: AND ARE CALCULATED VIA CHEBYSHEVS INEQUALITY. TODO: the above comes from some magic having to do with Chebyshev's bounds and square root and the way we calculate thing huh.

We then know that $\mathbf{E}[G_{g_i}] \geq (1-\delta)\,\mathbf{E}[G'_{g_i}]$ and that TODO: var. And we also know that G'_{g_i} is the ith largest of M samples from $\texttt{Binomial}(\Delta_{\text{stablizer}}\Delta_{\text{bit}}, p_S)$. If $E_{g_i} = e$, we also know that for some $s_1, s_2, ..., s_e \in \aleph$, $S_{s_j} = 0$ for $j \in [e]$.

So then, given e, G_{g_i} is the ith largest sample of M from $\texttt{Binomial}(\Delta_{\text{stablizer}}\Delta_{\text{bit}} - c\Delta_{\text{stablizer}}e, p_S)$ for some $0 < c \leq 1$. This is true because each stabilizer, s_j, that must be 0 neighbors at most $\Delta_{\text{stablizer}}$ bits in generator g_i and neighbors at least one bit in g_i.

So then, we can see that

$$\mathbf{E}[(1-\delta)G_{g_i} \mid E_{g_i} = e] \geq \mathbf{E}\big[(1-\delta)G''_{k_i}\big]$$

where

$$G'' \sim \texttt{Binomial}(\Delta_{\text{stablizer}}\Delta_{\text{bit}} - \Delta_{\text{stablizer}}e, p_S)$$

and $k_1, k_2, ..., k_K$ are the order statistics with $G''_{k_1} \geq G''_{k_2} \geq ... \geq G''_{k_K}$. Finally, because

$$\mathbf{Pr}\left[\frac{\Delta_{\text{bit}}(G''g_i - E_{g_i})}{(1-\delta)(G''g_i + E_{g_k})} < \frac{1}{3} \mid E_{g_i} = e\right] = \text{orderprob}\left(\Delta_{\text{bit}}\Delta_{\text{stablizer}} - \Delta_{\text{stablizer}}e, p_S, i, \frac{(3\Delta_{\text{bit}} + 1 - \delta)e}{3\Delta_{\text{bit}} - 1 + \delta}\right)$$

the lemma holds.