Modified belief propagation decoders for QLDPC codes

arXiv:1903.07404, PhysRevA.100.012330

Alex Rigby, JC Olivier, and Peter Jarvis

UNIVERSITY of TASMANIA

Outline

- Belief propagation (BP) decoding for classical LDPC codes
- BP for QLDPC codes
- Existing modifications to BP
- New modified decoders
- Some results

Classical decoding

- Linear code $\mathcal{C} \subset \mathrm{GF}(q)^n$ with parity-check matrix H
- Transmit codeword $\boldsymbol{x} \in \mathcal{C}$ across channel
- Receive $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e} \in \mathrm{GF}(q)^n$
- Infer most-likely error consistent with syndrome $\boldsymbol{z} = H\boldsymbol{y} = H\boldsymbol{e}$

$$\hat{\boldsymbol{e}} = \underset{\boldsymbol{e} \in \mathrm{GF}(q)^n}{\mathrm{argmax}}\, P(\boldsymbol{e}|\boldsymbol{z}) = \underset{\boldsymbol{e} \in \mathrm{GF}(q)^n}{\mathrm{argmax}}\, P(\boldsymbol{e})\delta(H\boldsymbol{e} = \boldsymbol{z})$$

- Probability $P(\hat{\boldsymbol{e}} \neq \boldsymbol{e})$ of a decoding error is the frame error rate (FER)
- NP-complete

Belief propagation

- Instead make a symbol-wise estimate $\hat{\boldsymbol{e}} = (\hat{e}_1, \ldots, \hat{e}_n)$ where

$$\hat{e}_j = \underset{e_j \in \mathrm{GF}(q)}{\mathrm{argmax}} P(e_j|\boldsymbol{z})$$

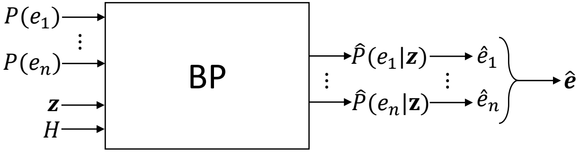
- Can obtain $P(e_j|\boldsymbol{z})$ through marginalization:

$$P(e_j = a|\boldsymbol{z}) = \sum_{\boldsymbol{e}:e_j=a} P(\boldsymbol{e}|\boldsymbol{z}) \propto \sum_{\boldsymbol{e}:e_j=a} P(\boldsymbol{e})\delta(H\boldsymbol{e} = \boldsymbol{z})$$

- Assume error components are independent:

$$P(e_j = a|\boldsymbol{z}) \propto \sum_{\boldsymbol{e}:e_j=a} \delta(H\boldsymbol{e} = \boldsymbol{z}) \prod_{l=1}^{n} P(e_l)$$

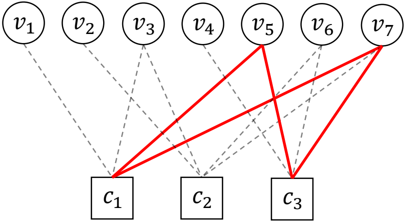
- Can approximate these marginals using belief propagation



Belief propagation - inside the black box

- Iterative message passing on graph $G = (V, C, E)$ defined by H
- Error components $\longleftrightarrow$ error nodes $V = \{v_1, \ldots, v_n\}$
- Rows of $H \longleftrightarrow$ check nodes $C = \{c_1, \ldots, c_m\}$
- Edge $\{c_i, v_j\} \in E$ if $H_{ij} \neq 0$
- E.g., $[7, 4, 3]$ Hamming code

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \longleftrightarrow$$



- Estimate $\hat{P}(e_j|\boldsymbol{z})$ made in each iteration
- Converges to exact value if G is a tree, but no cycles $\Rightarrow$ bad distance
- Keeps going until $\hat{\boldsymbol{z}} = H\hat{\boldsymbol{e}} = \boldsymbol{z}$ or max iterations reached
- Can perform well if graph is sparse and has few short cycles

Stabilizer code decoding

- Stabilizer code $\mathcal{Q}$ with stabilizer $\mathcal{S} = \langle M_1, \ldots, M_m \rangle \subset \mathcal{P}_n$
- Transmit codeword $|\phi\rangle \in \mathcal{Q}$ across Pauli channel
- Receive $E|\phi\rangle$ where error $E \in \mathcal{P}_n$
- Measure syndrome $\boldsymbol{z}$ where $z_i = \delta(\{E, M_i\} = 0)$
- Optimal decoder infers

$$\hat{A} = \operatorname*{argmax}_{A \in \mathcal{P}_n/\mathcal{S}} P(A|\boldsymbol{z})$$

- #P-complete[1]
- Resort to inferring $\hat{E} = \hat{E}_1 \otimes \cdots \otimes \hat{E}_n$ where

$$\hat{E}_i = \operatorname*{argmax}_{E_i \in \mathcal{P}_1} P(E_i|\boldsymbol{z})$$

- Can approximate these marginals using BP by making a link to classical codes over $\mathrm{GF}(4)$

[1] Iyer, Poulin, IEEE Trans. Inf. Theory 2015 (arXiv:1310.3235)

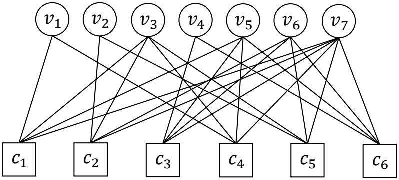
GF(4) BP

- Map $\mathcal{P}_1 \leftrightarrow \mathrm{GF}(4)$ with

$$I \leftrightarrow 0,\ X \leftrightarrow 1,\ Y \leftrightarrow \bar{\omega},\ Z \leftrightarrow \omega$$

- Map generators $M_1, \ldots, M_m$ of stabilizer $\mathcal{S}$ to rows of $m \times n$ $\mathrm{GF}(4)$ matrix H
- E.g., Steane code

$$\begin{matrix} X & I & X & I & X & I & X \\ I & X & X & I & I & X & X \\ I & I & I & X & X & X & X \\ Z & I & Z & I & Z & I & Z \\ I & Z & Z & I & I & Z & Z \\ I & I & I & Z & Z & Z & Z \end{matrix} \leftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \omega & 0 & \omega & 0 & \omega & 0 & \omega \\ 0 & \omega & \omega & 0 & 0 & \omega & \omega \\ 0 & 0 & 0 & \omega & \omega & \omega & \omega \end{pmatrix} \leftrightarrow$$



- Map error $E \in \mathcal{P}_n$ to element of $\boldsymbol{e} = \mathrm{GF}(4)^n$
- Syndrome is

$$\boldsymbol{z} = \mathrm{tr}(H\bar{\boldsymbol{e}})$$

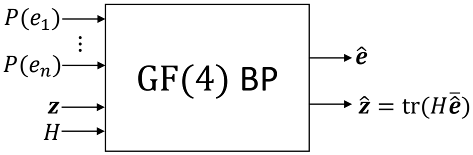
where $\mathrm{tr}(x) = x + \bar{x}$ [$\mathrm{tr}(0) = \mathrm{tr}(1) = 0$ and $\mathrm{tr}(\omega) = \mathrm{tr}(\bar{\omega}) = 1$]

GF(4) BP

- GF(4) BP using $\boldsymbol{z}$ and H to find $\hat{\boldsymbol{e}} = (\hat{e}_1, \ldots, \hat{e}_n) \leftrightarrow \hat{E} = \hat{E}_1 \ldots \hat{E}_n$
- Initial probabilities are

$$
\begin{aligned}
p(e_j = 0) &= P(E_i = I) = 1 - p \\
p(e_j = 1) &= P(E_i = X) = p_X \\
p(e_j = \bar{\omega}) &= P(E_i = Y) = p_Y \\
p(e_j = \omega) &= P(E_i = Z) = p_Z
\end{aligned}
$$

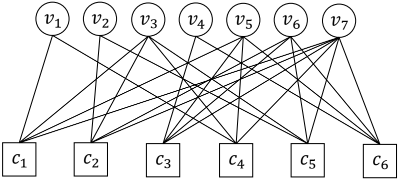
- Not quite standard classical BP as $\boldsymbol{z} = \mathrm{tr}(H\bar{\boldsymbol{e}})$ rather than $\boldsymbol{z} = H\boldsymbol{e}$



Problems

- Degeneracy can cause issues with finding symbol-wise most likely error[2]
- E.g., $\mathcal{S} = \langle XX, ZZ \rangle$, $\boldsymbol{z} = (0,1) \Rightarrow E \in \{XI, IX, YZ, ZY\}$
- If $P(E_1) = P(E_2)$ then $P(E_1|\boldsymbol{z}) = P(E_2|\boldsymbol{z}) \Rightarrow \hat{E}_1 = \hat{E}_2$
- Stabilizer generators commuting $\Rightarrow$ unavoidable 4-cycles

$$\begin{matrix} X & I & X & I & X & I & X \\ I & X & X & I & I & X & X \\ I & I & I & X & X & X & X \\ Z & I & Z & I & Z & I & Z \\ I & Z & Z & I & I & Z & Z \\ I & I & I & Z & Z & Z & Z \end{matrix} \leftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \omega & 0 & \omega & 0 & \omega & 0 & \omega \\ 0 & \omega & \omega & 0 & 0 & \omega & \omega \\ 0 & 0 & 0 & \omega & \omega & \omega & \omega \end{pmatrix} \leftrightarrow$$



[2] Poulin, Chung, QIC 2008 (arXiv:0801.1241)

GF(2) BP

- For CSS codes, can use GF(2) BP instead
- $\mathcal{P}_n \leftrightarrow \mathrm{GF}(2)^{2n}$ with $X_1^{u_1} Z_1^{v_1} \dots X_n^{u_n} Z_n^{v_n} = X^{\boldsymbol{u}} Z^{\boldsymbol{v}} \leftrightarrow (\boldsymbol{u}|\boldsymbol{v})$
- Generators of $\mathcal{S}$ map to rows of $m \times 2n$ matrix $H = (H_X|H_Z)$
- If CSS, then can represent with X-only and Z-only generators

$$H = \left(\begin{array}{c|c} \tilde{H}_X & 0 \\ 0 & \tilde{H}_Z \end{array} \right)$$

- E.g., Steane code again:

$$\begin{matrix} X & I & X & I & X & I & X \\ I & X & X & I & I & X & X \\ I & I & I & X & X & X & X \\ Z & I & Z & I & Z & I & Z \\ I & Z & Z & I & I & Z & Z \\ I & I & I & Z & Z & Z & Z \end{matrix} \leftrightarrow \left(\begin{array}{ccccccc|ccccccc} 1&0&1&0&1&0&1&0&0&0&0&0&0&0 \\ 0&1&1&0&0&1&1&0&0&0&0&0&0&0 \\ 0&0&0&1&1&1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&1&1&1 \end{array} \right)$$

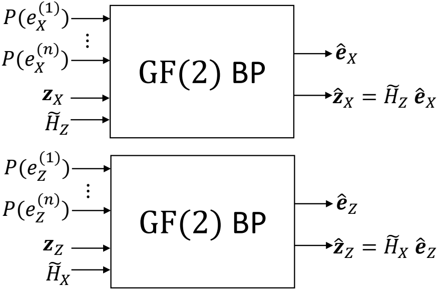
- $\mathcal{S}$ abelian $\leftrightarrow \tilde{H}_Z \tilde{H}_X^T = 0$
- Dual containing (DC) if representation with $\tilde{H} = \tilde{H}_X = \tilde{H}_Z$

GF(2) BP

- Errors $E \propto X^{\boldsymbol{e}_X} Z^{\boldsymbol{e}_Z} \leftrightarrow \boldsymbol{e} = (\boldsymbol{e}_X^T | \boldsymbol{e}_Z^T)^T$
- Syndrome

$$\boldsymbol{z} = \begin{pmatrix} \tilde{H}_X \boldsymbol{e}_Z \\ \tilde{H}_Z \boldsymbol{e}_X \end{pmatrix} = \begin{pmatrix} \boldsymbol{z}_Z \\ \boldsymbol{z}_X \end{pmatrix}$$

- Assume X and Z error components occur independently
- Infer each separately using GF(2) BP
- Use $\tilde{H}_Z$ and $\boldsymbol{z}_X$ to get $\hat{\boldsymbol{e}}_X$; prior probs $P(e_X^{(j)} = 1) = p_X + p_Y \; (= 2p/3)$
- Use $\tilde{H}_X$ and $\boldsymbol{z}_Z$ to get $\hat{\boldsymbol{e}}_Z$; prior probs $P(e_Z^{(j)} = 1) = p_Y + p_Z \; (= 2p/3)$



Pros and cons

- Lower complexity than $\mathrm{GF}(4)$ decoding
- Fewer 4-cycles; must still be 4-cycles if DC though as $\tilde{H}\tilde{H}^T = 0$
- Ignores correlations between error components

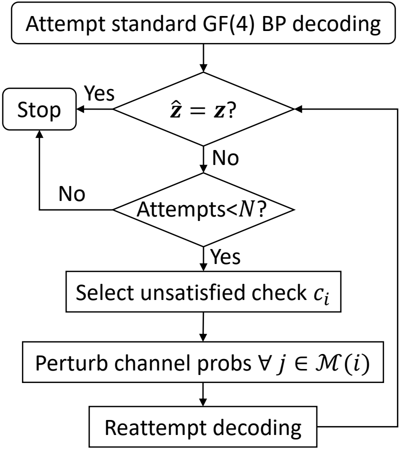
$$P(e_Z^{(j)} = 1 | e_X^{(j)} = 1) = \frac{p_Y}{p_X + p_Y} \ \left(= \frac{1}{2}\right)$$

$$P(e_Z^{(j)} = 1 | e_X^{(j)} = 0) = \frac{p_Z}{1 - (p_X + p_Y)} \ \left(= \frac{p}{3 - 2p}\right)$$

$$P(e_X^{(j)} = 1 | e_Z^{(j)} = 1) = \frac{p_Y}{p_Y + p_Z} \ \left(= \frac{1}{2}\right)$$

$$P(e_X^{(j)} = 1 | e_Z^{(j)} = 0) = \frac{p_X}{1 - (p_Y + p_Z)} \ \left(= \frac{p}{3 - 2p}\right)$$

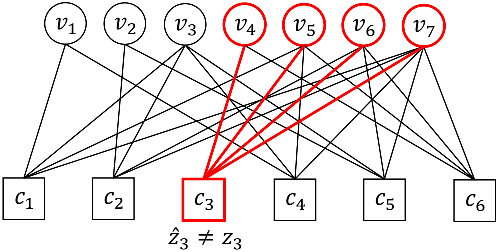
Existing decoders - random perturbation[3]



- Perturbation is

$$p_I \to p_I$$
$$p_X \to (1+\delta_X)p_X$$
$$p_Y \to (1+\delta_Y)p_Y$$
$$p_Z \to (1+\delta_Z)p_Z$$

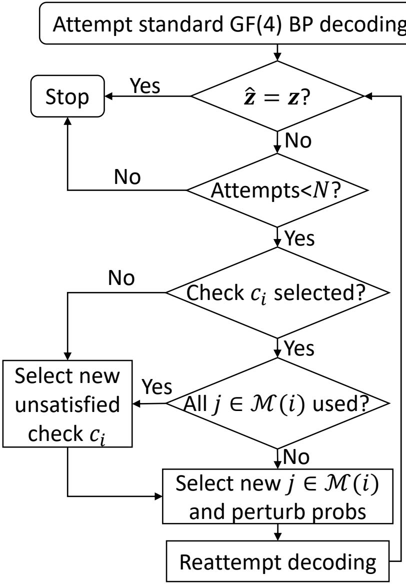
- δ_X, δ_Y, and δ_Z uniformly distributed over $[0, \delta]$



---

[3]Poulin, Chung, QIC 2008 (arXiv:0801.1241)

Existing decoders - enhanced feedback (EFB)[4]

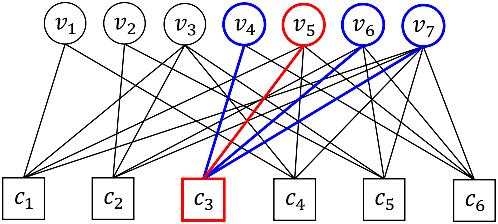


- If $z_i = 1$ but $\hat{z}_i = 0$

$$p_\sigma \to \begin{cases} \frac{p}{2} & \text{if } \sigma = I, \text{ or } M_i^{(j)} \\ \frac{1-p}{2} & \text{otherwise} \end{cases}$$

- If $z_i = 0$ but $\hat{z}_i = 1$

$$p_\sigma \to \begin{cases} \frac{1-p}{2} & \text{if } \sigma = I, \text{ or } M_i^{(j)} \\ \frac{p}{2} & \text{otherwise} \end{cases}$$



$\hat{z}_3 \neq z_3$

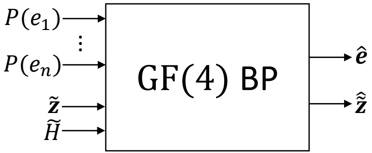
[4] Wang et al., IEEE Trans. Inf. Theory 2012 (arXiv:0912.4546)

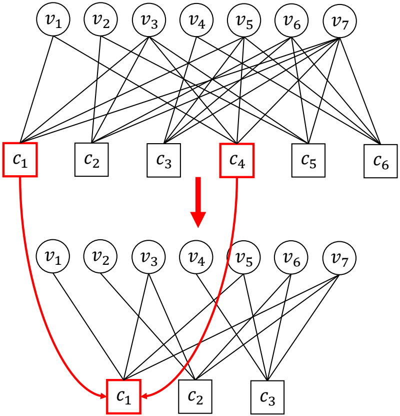
Existing decoders - supernode[5]

- Modification to GF(4) BP for DC CSS codes

$$\boldsymbol{z} = \mathrm{tr}(H\bar{\boldsymbol{e}}) = \mathrm{tr}\left[\begin{pmatrix} \tilde{H} \\ \omega\tilde{H} \end{pmatrix}\bar{\boldsymbol{e}}\right] = \begin{pmatrix} \mathrm{tr}(\tilde{H}\bar{\boldsymbol{e}}) \\ \mathrm{tr}(\omega\tilde{H}\bar{\boldsymbol{e}}) \end{pmatrix} = \begin{pmatrix} \boldsymbol{z}_Z \\ \boldsymbol{z}_X \end{pmatrix}$$

- As $\mathrm{tr}(\omega x) + \omega\mathrm{tr}(x) = \bar{x}$, can define $\tilde{\boldsymbol{z}} = \tilde{H}\boldsymbol{e} = \boldsymbol{z}_X + \omega\boldsymbol{z}_Z$
- Use classical GF(4) BP to infer $\boldsymbol{e}$ from $\tilde{\boldsymbol{z}}$
- Can view as grouping checks c_i and $c_{i+m/2}$ into a "supernode"
- Reduces complexity and number of 4-cycles





[5]Babar et al., IEEE Access 2015

New decoders - adjusted

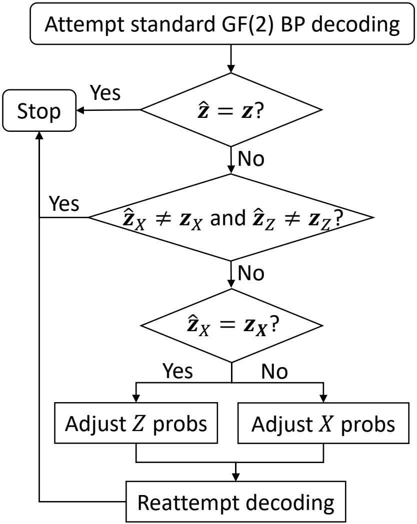
- $\mathrm{GF}(2)$ based for CSS codes
- Reintroduce $X - Z$ correlations
- If $\hat{\boldsymbol{z}}_X = \boldsymbol{z}_X$ but $\hat{\boldsymbol{z}}_Z \neq \boldsymbol{z}_Z$,

$$P(e_Z^{(j)}) \rightarrow P(e_Z^{(j)} | \hat{e}_X^{(j)})$$

- If $\hat{\boldsymbol{z}}_Z = \boldsymbol{z}_Z$ but $\hat{\boldsymbol{z}}_X \neq \boldsymbol{z}_X$,

$$P(e_X^{(j)}) \rightarrow P(e_X^{(j)} | \hat{e}_Z^{(j)})$$

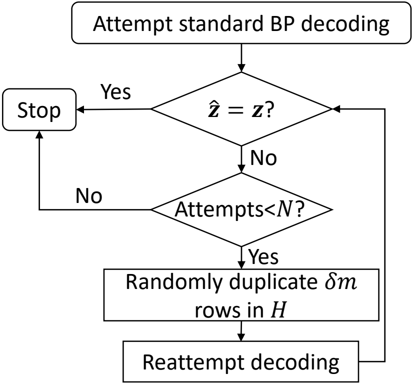
- Extends previously proposed perfect matching decoder[6]

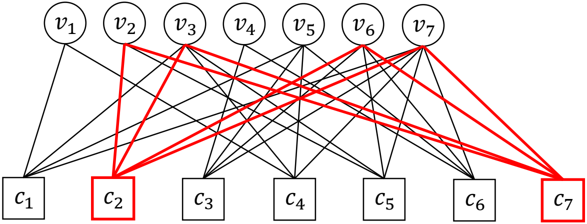


[6] Delfosse, Tillich, IEEE ISIT 2014, (arXiv:1401.6975)

New decoders - augmented

- Previously proposed for classical codes[7]
- Can be based on $\mathrm{GF}(2)$, $\mathrm{GF}(4)$, or supernode decoder
- Fraction of rows duplicated is augmentation density δ
- Duplicates check nodes and their connections in factor graph
- Actually introduces more 4-cycles

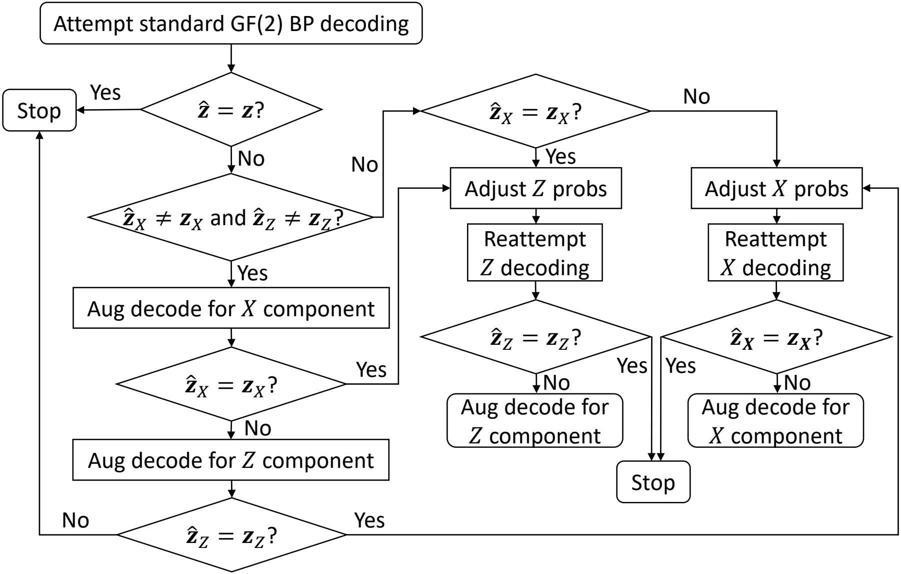




[7]Rigby et al., EURASIP JWCN 2018

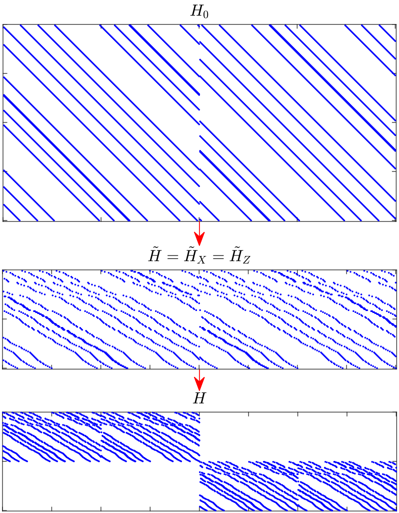
New decoders - combined

- Combine adjusted and augmented decoders for CSS codes



Results - bicycle

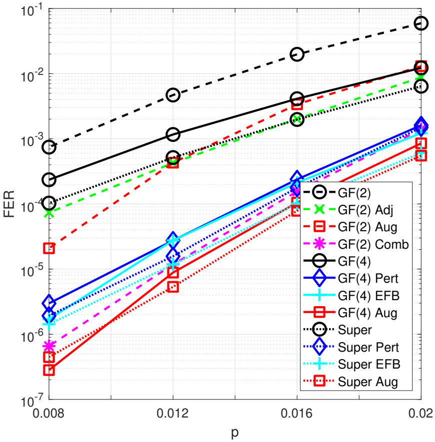
- $[[400, 200]]$ DC CSS code[8]
- Construct $n \times n$ circulant A
- $H_0 = [\ A \quad A^T\ ]$
- $H_0 H_0^T = AA^T + A^T A = 0$
- Remove $(n-m)/2$ rows to get $\tilde{H}$
- Distance likely $<$ row weight w
- $w = 20$ used
- $\tilde{H}$ yields $2,737$ 4-cycles



[8] MacKay, Mitchison, McFadden, IEEE Trans. Inf. Theory 2004 (arXiv:quant-ph/0304161)

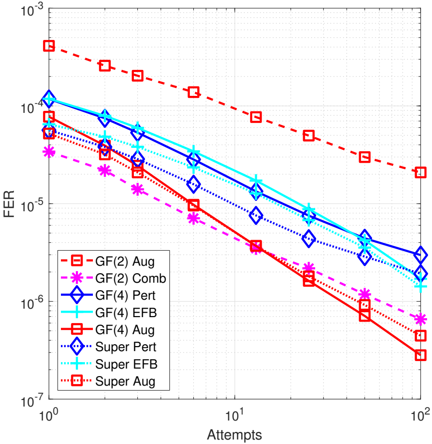
Results - bicycle

- $N = 100$ attempts
- Supernode $>$ $\mathrm{GF}(4)$ $>$ $\mathrm{GF}(2)$
- Adjusted matches supernode
- Augmented $\mathrm{GF}(2)$ OK, but not great
- Random perturbation and EFB similar
- Augmented $\mathrm{GF}(4)$, augmented supernode both perform better
- Combined decoder performs well too



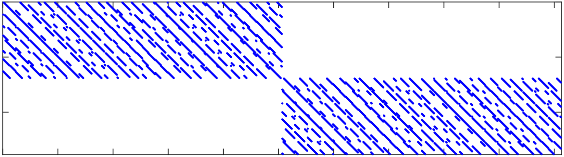
Results - bicycle

- $p = 0.008$
- Roughly linear reduction in FER with N on log-log
- Only require ~ 25 attempts with augmented/combined to match rand pert and EFB with 100



Results - Quasi-cyclic

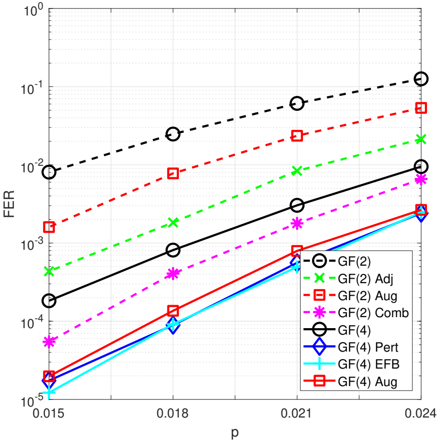
- $[[506, 240]]$ non-DC CSS code[9]
- Construct base matrices $J \times L$ matrix $\mathcal{H}_X$ and $K \times L$ matrix $\mathcal{H}_Z$
- Elements belong to $\{0, 1, \ldots, P-1\}$
- Get $\tilde{H}_X$ ($\tilde{H}_Z$) from $\mathcal{H}_X$ ($\mathcal{H}_Z$) by replacing each element with shifted $P \times P$ identity
- Possible to select $\mathcal{H}_X$ and $\mathcal{H}_Z$ such that $\tilde{H}_Z \tilde{H}_X^T = 0$
- Can also ensure that $\tilde{H}_X$ and $\tilde{H}_Z$ are free of 4-cycles
- Used $P = 23$, $J = K = 6$, and $L = 22$



[9] Hagiwara, Imai, IEEE ISIT 2007 (arXiv:quant-ph/0701020)

Results - Quasi-cyclic

- Cannot use supernode based decoders
- Performance of augmented $\mathrm{GF}(2)$ decoder is underwhelming
- Suggests augmentation alleviates effect of 4-cycles
- Augmented, random perturbation, and EFB all perform similarly



Summary

- Adjusted decoder successfully reintroduces correlation
- Augmented and combined decoder perform well
- Outperform random perturbation and EFB for DC CSS
- Similar performance on non-DC CSS
- Fighting 4-cycles with more 4-cycles