Karlsruhe Institute of Technology

Decoding of Quantum LDPC Codes with Modified Belief Propagation Decoder

Final Presentation

Alexander Schnerring

Motivation

- Quantum computers are believed to be capable of outperforming classical computers for certain problems
- Example: *Shor's algorithm* finds prime factors of an integer in sub-exponential time

  $\rightarrow$ This has far-reaching consequences for public-key cryptography schemes

- Problem: Quantum information is particularly susceptible to noise

  $\rightarrow$ **Quantum Error Correction:** Add redundant information to quantum information it against noise

Overview

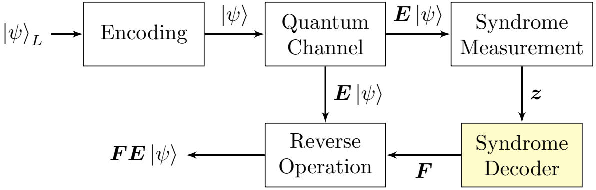
- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Overview

- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Quantum Error Correction

- Quantum codeword $|\psi\rangle$ cannot be measured directly
  $\rightarrow$ Decoding is based on **syndrome measurement**



- Syndrome only depends on the error $\boldsymbol{E}$
  $\rightarrow$ It suffices to consider errors rather than codewords

Quantum Errors

- *Digitization theorem:* It suffices to consider **four error types** that can occur in a quantum channel:

  I: no error $\quad$ X: bit flip $\quad$ Z: phase flip $\quad$ Y: bit flip and phase flip

- A quantum codeword of length N is corrupted by errors of the form $\boldsymbol{E} \in \{I, X, Y, Z\}^N$
- Error types are isomorph to $\mathrm{GF}(4)$:

$+$	I	X	Z	Y
I	I	X	Z	Y
X	X	I	Y	Z
Z	Z	Y	I	X
Y	Y	Z	X	I

- *Index-based notation:*
  - We omit identity entries and write indices of non-identity entries in the subscript
  - Example for $N = 5$: $\boldsymbol{E} = \begin{pmatrix} I & X & I & Z & I \end{pmatrix} \leftrightarrow \boldsymbol{E} = X_1 Z_3$

Stabilizer Formalism

Karlsruhe Institute of Technology

- Define a quantum code in terms of its *stabilizers* $\boldsymbol{S}_m \in \{I, X, Y, Z\}^N$ ("quantum parity checks")
- **Stabilizer matrix S**: $M \times N$ matrix, composed of M stabilizers $\boldsymbol{S}_m$
  $\rightarrow$ Quantum analogue to the classical parity check matrix
- Example: $\boldsymbol{S} = \begin{pmatrix} X & Y & I \\ Z & Z & Y \end{pmatrix}$
- We can think of $\boldsymbol{S}$ as a mapping from the error space to the syndrome space:

$$\boldsymbol{S} : \{I, X, Y, Z\}^N \mapsto \{0, 1\}^M, \ \boldsymbol{E} \mapsto \boldsymbol{z}$$

- Syndrome $\boldsymbol{z} = \langle \boldsymbol{S}, \boldsymbol{E} \rangle$: Binary vector of length M, indicating which quantum parity checks are satisfied

Further reading: Daniel Gottesman.
Stabilizer codes and quantum error correction.
Dissertation (Ph.D.), California Institute of Technology, 1997.

Normalizer $N(\mathcal{S})$

- S partitions error space $\{I, X, Y, Z\}^N$ into 2^M **cosets**
- Errors in in the same coset share the same syndrome
- **Normalizer $N(\mathcal{S})$**: Coset corresponding to the trivial syndrome
- Errors connected by an element in $N(\mathcal{S})$ result in an identical syndrome

Overview

Karlsruhe Institute of Technology

- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Constructing Quantum Codes

- Not any $\boldsymbol{S}$ defines a valid quantum code
- $\boldsymbol{S}$ has to satisfy the **symplectic criterion**: Each pair of rows $\boldsymbol{S}_m$, $\boldsymbol{S}_n$ has to satisfy $\langle \boldsymbol{S}_m, \boldsymbol{S}_n \rangle = 0$
- CSS codes: Write stabilizer matrix as $\boldsymbol{S} = \begin{pmatrix} X \cdot \boldsymbol{H}_X \\ Z \cdot \boldsymbol{H}_Z \end{pmatrix}$, where $\boldsymbol{H}_X$ and $\boldsymbol{H}_Z$ are classical binary PCMs
- Then $\boldsymbol{H}_X$ and $\boldsymbol{H}_Z$ have to satisfy:

$$\boldsymbol{H}_X \boldsymbol{H}_Z^T = \boldsymbol{0} \mod 2$$

Further reading: A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane.
Quantum error correction via codes over GF(4).
In *Proceedings of IEEE International Symposium on Information Theory*, 1997.

Hypergraph Product Code Construction

Karlsruhe Institute of Technology

- Converts two classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with PCMs $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ to a quantum code

- $\boldsymbol{S} = \begin{pmatrix} \boldsymbol{X} \cdot \boldsymbol{H}_X \\ \boldsymbol{Z} \cdot \boldsymbol{H}_Z \end{pmatrix}$, where
  - $\boldsymbol{H}_X = [\boldsymbol{H}_1 \otimes \boldsymbol{I}_{N_2} \mid \boldsymbol{I}_{M_1} \otimes \boldsymbol{H}_2^T]$
  - $\boldsymbol{H}_Z = [\boldsymbol{I}_{N_1} \otimes \boldsymbol{H}_2 \mid \boldsymbol{H}_1^T \otimes \boldsymbol{I}_{M_2}]$

- $\dim \boldsymbol{H}_1 = M_1 \times N_1$
- $\dim \boldsymbol{H}_2 = M_2 \times N_2$

Further reading: Jean-Pierre Tillich and Gilles Zémor.
Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength.
IEEE Transactions on Information Theory, Vol. 60 (2), 2014.

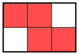
Hypergraph Product Code Construction

- Converts two classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with PCMs $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ to a quantum code

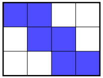
- $\boldsymbol{S} = \begin{pmatrix} \boldsymbol{X} \cdot \boldsymbol{H}_X \\ \boldsymbol{Z} \cdot \boldsymbol{H}_Z \end{pmatrix}$, where
  - $\boldsymbol{H}_X = [\boldsymbol{H}_1 \otimes \boldsymbol{I}_{N_2} \mid \boldsymbol{I}_{M_1} \otimes \boldsymbol{H}_2^T]$
  - $\boldsymbol{H}_Z = [\boldsymbol{I}_{N_1} \otimes \boldsymbol{H}_2 \mid \boldsymbol{H}_1^T \otimes \boldsymbol{I}_{M_2}]$

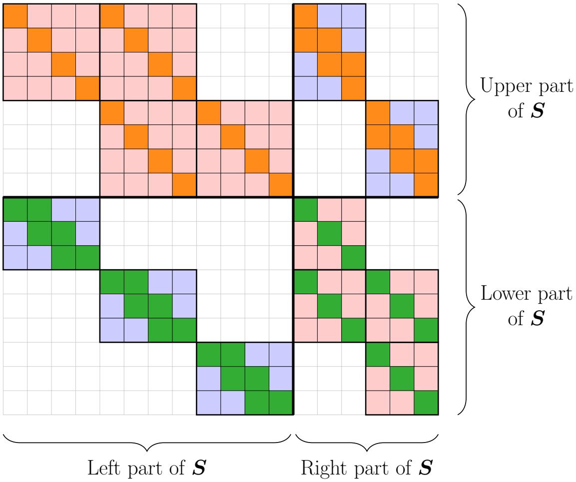
- $\dim \boldsymbol{H}_1 = M_1 \times N_1$
- $\dim \boldsymbol{H}_2 = M_2 \times N_2$

$\boldsymbol{H}_1$



$\boldsymbol{H}_2$



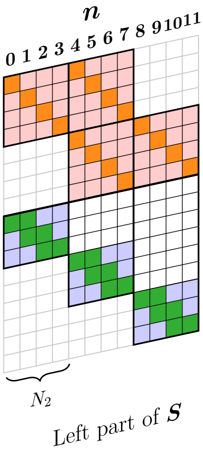


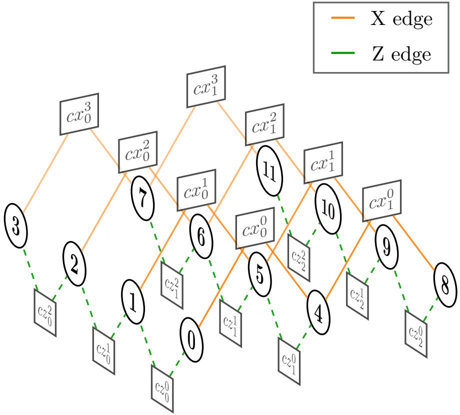
Further reading: Jean-Pierre Tillich and Gilles Zémor.
Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength.
IEEE Transactions on Information Theory, Vol. 60 (2), 2014.

Hypergraph Product Code Construction

- We propose the representation of an index n as outer o and inner index i
- Outer index: $o = \left\lfloor \frac{n}{N_2} \right\rfloor$
- Inner index: $i = n \mod N_2$
- We refer to an error W_n with outer index o and inner index i as W_o^i
- Subgraph induced by nodes with identical i is isomorph to $\mathcal{T}(\boldsymbol{H}_1)$
- Subgraph induced by nodes with identical o is isomorph to $\mathcal{T}(\boldsymbol{H}_2)$

$\rightarrow$ Properties of HP code are connected to classical codes

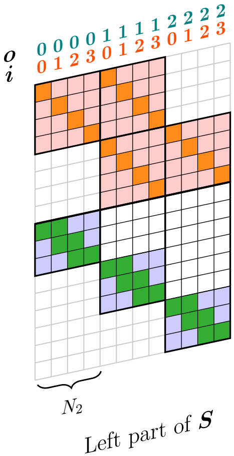


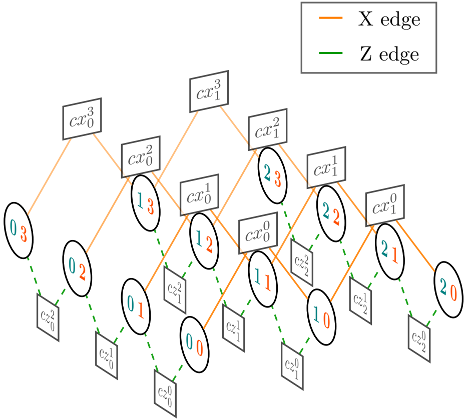


Hypergraph Product Code Construction

- We propose the representation of an index n as outer o and inner index i
- Outer index: $o = \left\lfloor \dfrac{n}{N_2} \right\rfloor$
- Inner index: $i = n \mod N_2$
- We refer to an error W_n with outer index o and inner index i as W_o^i
- Subgraph induced by nodes with identical i is isomorph to $\mathcal{T}(\boldsymbol{H}_1)$
- Subgraph induced by nodes with identical o is isomorph to $\mathcal{T}(\boldsymbol{H}_2)$

$\rightarrow$ Properties of HP code are connected to classical codes





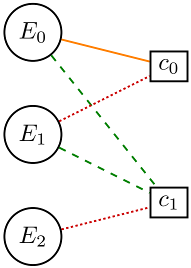
Overview

- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Quaternary Belief Propagation

- Belief Propagation: Find $\boldsymbol{F}$ based on $\boldsymbol{z}$ by exchanging messages over the Tanner graph $\mathcal{T}(\boldsymbol{S})$
- Four-dimensional probability distributions $p_n^W = P(E_n = W)$ are passed over the edges

- Implementation:
  - Kuo and Lai propose to exchange scalar messages
  - Key idea: Only exchange information whether entries on qubits commute with corresponding edge type
  - Efficient implementation in log-domain further reduces complexity



$$\boldsymbol{S} = \begin{pmatrix} \boldsymbol{X} & \boldsymbol{Y} & \boldsymbol{I} \\ \boldsymbol{Z} & \boldsymbol{Z} & \boldsymbol{Y} \end{pmatrix}$$

Further reading: Kao Yueh Kuo and Ching-Yi Lai.
Refined belief-propagation decoding of quantum codes with scalar messages.
2020 IEEE Globecom Workshops, GC Wkshps 2020.

Overview

- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Split Beliefs

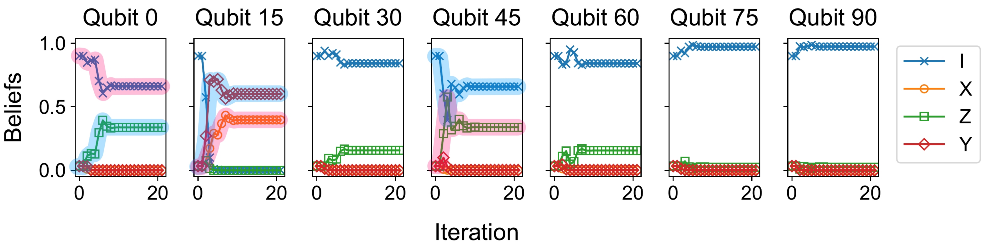
- Suppose two errors $\boldsymbol{E}_1$ and $\boldsymbol{E}_2$ of equal weight have the same syndrome (i.e. they are related by an element in $N(\mathcal{S})$)
- Decoder attempts to converge to both errors **simultaneously**, resulting in an **invalid superposition**

- **Example:**
  - The $[[129, 28, 3]]$ HP code is constructed from $\mathcal{C}_1$ ($[7, 4, 3]$ BCH code) and $\mathcal{C}_2$ ($[15, 7, 5]$ BCH code)
  - Pairs of weight-2 errors ($\boldsymbol{E}_1 = Z^i_{o_0} Y^i_{o_1}, \boldsymbol{E}_2 = X^i_{o_1} Z^i_{o_2}$) share the same syndrome

$\rightarrow$ We propose a **post-processing step** exploiting the structure of HP codes

Split Beliefs in the [[129, 28, 3]] HP Code

- Decoder attempts to converge to $\boldsymbol{E}_1 = Z_0 Y_{15}$ and $\boldsymbol{E}_2 = X_{15} Z_{45}$ **simultaneously**:



- The performance could be increased if the decoder decided for **one solution**, leading to decoding success for one of the errors (instead of none)

  $\rightarrow$ Idea: Apply **post-processing step** to decide for one error

Post-Processing Step

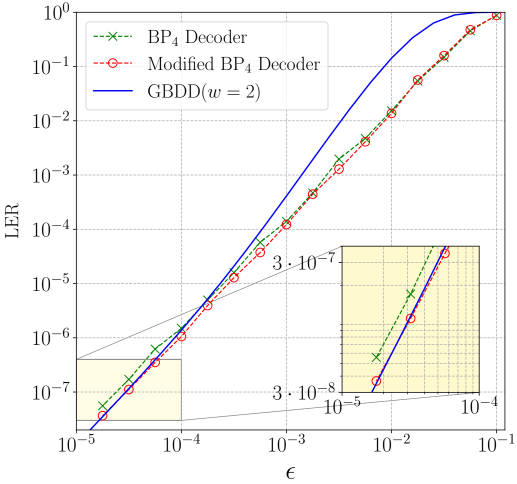
- Since both errors are of equal weight, we arbitrarily choose $\boldsymbol{E}_1 = Z_{o_0}^i Y_{o_1}^i$
- Split syndrome $\boldsymbol{z}$ into two parts, $\boldsymbol{z}_X$ and $\boldsymbol{z}_Z$, i.e. $\boldsymbol{S} = \begin{pmatrix} \boldsymbol{X} \cdot \boldsymbol{H}_X \\ \boldsymbol{Z} \cdot \boldsymbol{H}_Z \end{pmatrix} \begin{matrix} \rightarrow \boldsymbol{z}_X \\ \rightarrow \boldsymbol{z}_Z \end{matrix}$
- Post-processing:
  1. Only Y entry induces non-trivial syndrome in $\boldsymbol{z}_Z$
     $\rightarrow$ Use $\boldsymbol{z}_Z$ to determine o_1 and i of Y entry
  2. The syndrome is linear, i.e. $\boldsymbol{z}_X(Z_{o_0}^i Y_{o_1}^i) = \boldsymbol{z}_X(Z_{o_0}^i) + \boldsymbol{z}_X(Y_{o_1}^i) \mod 2$
     $\rightarrow$ Compute "residual" syndrome $\boldsymbol{z}_X(Z_{o_0}^i)$
  3. Use $\boldsymbol{z}_X(Z_{o_0}^i)$ to determine o_0 of Z entry

Note that $\boldsymbol{z}(\boldsymbol{E})$ denotes the syndrome of error $\boldsymbol{E}$.

Simulation Results

- Generalized bounded distance decoder (GBDD):
  - GBDD(w) corrects all correctable errors of weight smaller or equal than w
  - Approximates optimal performance in the low error rate region
- Unmodified decoder performs close to GBDD(w=2)
- A small gap remains in the low error rate region

  $\rightarrow$ This can (mostly) be attributed to split beliefs
- Modified decoder closes this gap



Overview

- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Message Overestimation

- Message reliability is overestimated due to statistical dependence (e.g. caused by short cycles)
- Decoder might fail to converge due to oscillating beliefs or might converge to a wrong solution

  $\rightarrow$ We propose to apply **variable message normalization**

- **Example:**
  - The *symmetric* $[[900, 36, 10]]$ HP code is constructed by choosing a regular $[24, 6]$ LDPC code $\mathcal{C}_{\mathrm{C}} = \mathcal{C}_1 = \mathcal{C}_2$ in the HP code construction
  - For this code, many decoding failures are caused by message overestimation

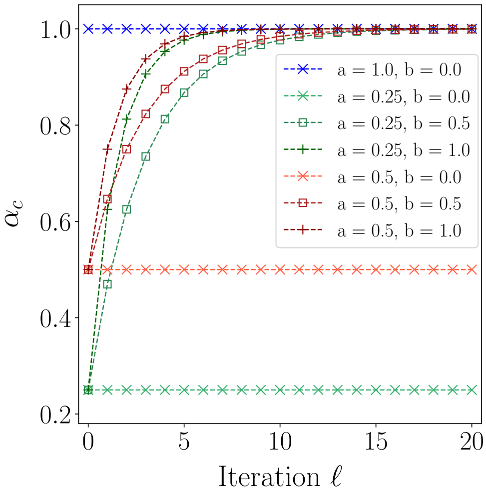
Variable Message Normalization

- Existing work: Message normalization alleviates problem of message overestimation
  $\rightarrow$ Multiply check-to-variable messages with scalar α_c

- We propose to increase α_c with every iteration:

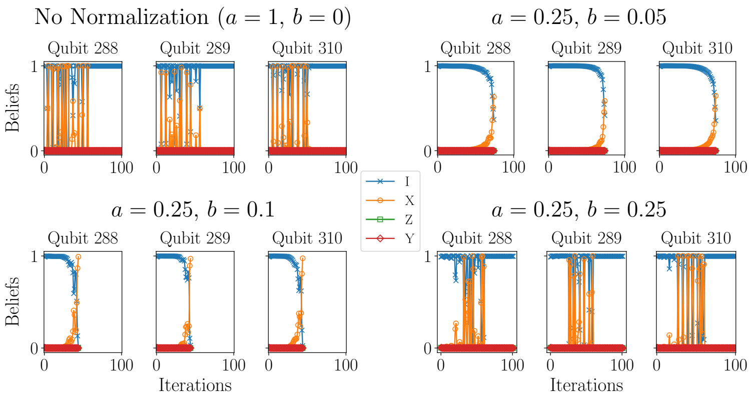
$$\alpha_c(a,\, b,\, \ell) = 1 - (1-a) \cdot 2^{-b \cdot \ell}$$

- a: controls initial value of α_c
- b: controls speed at which α_c converges to 1
- ℓ: Iteration



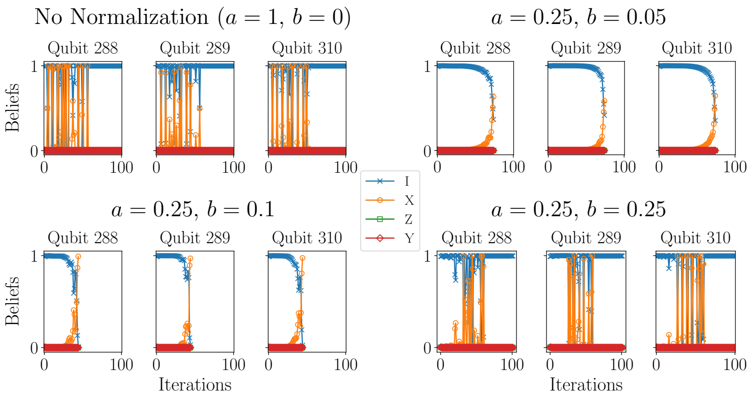
Overestimation-Underestimation-Trade-Off

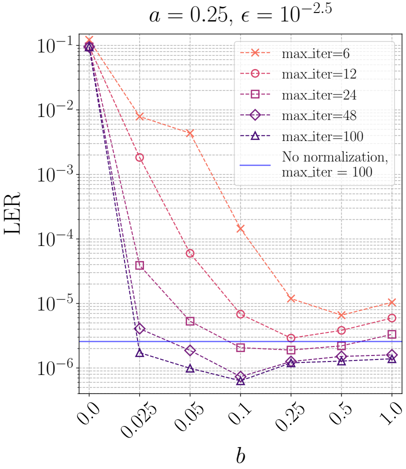
- Parameter b has to be chosen carefully
- Decoding the error $X_{288}X_{289}X_{310}$ with different b:



Overestimation-Underestimation-Trade-Off

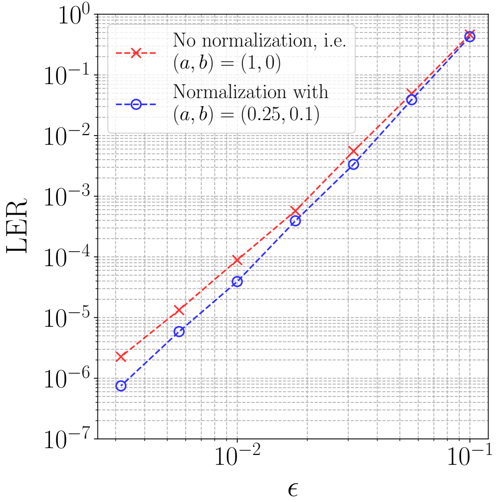
- Parameter b has to be chosen carefully
- Decoding the error $X_{288}X_{289}X_{310}$ with different b:





Simulation Results

- We compare decoding performance of the quaternary BP on the $[[900, 36, 10]]$ HP with
  - no normalization
  - variable normalization
- Variable message normalization enhances decoding performance (especially in the low error rate domain)



Overview

- Basics on Quantum Error Correction
- Hypergraph Product Codes
- Modifications to Quaternary Belief Propagation
  - Post-Processing
  - Variable Message Normalization
- Conclusion

Summary

- Quantum stabilizer codes are the quantum analogue to classical linear codes
- HP code construction enables us to construct quantum codes from any two classical codes

- Belief propagation of HP codes comes with several decoding issues:
  - Split beliefs due to properties of the classical codes
  - Message overestimation

- We address these issues by modifying the BP decoder:
  - **Post-processing step** exploiting code structure
  - **Variable message normalization**

Outlook

- Generalize post-processing step to tackle split beliefs on a broader class of codes
- Find an optimal strategy to adapt normalization factor α_c during decoding
- and more...

Why is Syndrome Measurement Possible?

- Consider the code defined by $\boldsymbol{S} = \left(\begin{smallmatrix} Z & Z & I \\ I & Z & Z \end{smallmatrix}\right)$, i.e.

$$|\psi\rangle_{\mathrm{L}} = \alpha\,|0\rangle + \beta\,|1\rangle \xmapsto{\text{Encoding}} |\psi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$$

- Suppose a bit flip on the second qubit occurs, i.e. $\boldsymbol{E} = \begin{pmatrix} I & X & I \end{pmatrix}$
- The resulting state will be

$$\boldsymbol{E}\,|\psi\rangle = \alpha\,|010\rangle + \beta\,|101\rangle$$

- Measurement of $\boldsymbol{S}_0 = \begin{pmatrix} Z & Z & I \end{pmatrix}$ reveals whether first two qubits are different
- Measurement of $\boldsymbol{S}_1 = \begin{pmatrix} I & Z & Z \end{pmatrix}$ reveals whether last two qubits are different

$\rightarrow$ We can measure the error without measuring the information!

Syndrome Computation

- The syndrome in the **binary case** is obtained as

$$z_m = \sum_n f(H_{mn}, e_n) \mod 2, \qquad \text{where} \qquad \begin{array}{c|cc} f(\cdot,\cdot) & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

- A check $\boldsymbol{H}_m$ is satisfied if $\boldsymbol{H}_m$ and $\boldsymbol{e}$ are both non-zero in an even number of positions

- The syndrome in the **quaternary case** is obtained as

$$z_m = \sum_n f(S_{mn}, E_n) \mod 2, \qquad \text{where} \qquad \begin{array}{c|cccc} f(\cdot,\cdot) & I & X & Z & Y \\ \hline I & 0 & 0 & 0 & 0 \\ X & 0 & 0 & 1 & 1 \\ Z & 0 & 1 & 0 & 1 \\ Y & 0 & 1 & 1 & 0 \end{array}$$

- A check $\boldsymbol{S}_m$ is satisfied if $\boldsymbol{S}_m$ and $\boldsymbol{E}$ are both non-zero and different in an even number of positions

Message Update Rules of BP_4

- Initial beliefs on qubit n:

$$\boldsymbol{\Lambda}_n = (\Lambda_n^X,\, \Lambda_n^Y,\, \Lambda_n^Z) \in \mathbb{R}^3$$

- Variable-to-check-messages:

$$\lambda_{S_{mn}}(\Gamma_{n\to m}^W) = \lambda_{S_{mn}}\left(\Lambda_n^W + \sum_{m\in\mathcal{M}(n)\setminus n} \mathbb{1}\{\langle S_{m'n}, W\rangle = 1\}\, \Delta_{m'\to n}\right),$$

where

$$\lambda_\eta(\boldsymbol{L}) = \ln \frac{1 + \sum_{V\in\{X,Y,Z\}:\,\langle \eta,\, V\rangle = 0} e^{-L^V}}{\sum_{V\in\{X,Y,Z\}:\,\langle \eta,\, V\rangle = 1} e^{-L^V}}$$

- Check-to-variable messages:

$$\Delta_{m\to n} = (-1)^{z_m} \mathop{\boxplus}_{n'\in\mathcal{N}(m)\setminus n} \lambda_{S_{mn'}}(\boldsymbol{\Gamma}_{n'\to m})$$

Hypergraph Product Code Construction

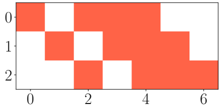
- Converts two classical codes $\mathcal{C}_1$ and $\mathcal{C}_2$ with PCMs $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ to a quantum **CSS code**

$$\boldsymbol{H}_X = [\boldsymbol{H}_1 \otimes \boldsymbol{I}_{N_2} \mid \boldsymbol{I}_{M_1} \otimes \boldsymbol{H}_2^T] \qquad \boldsymbol{H}_Z = [\boldsymbol{I}_{N_1} \otimes \boldsymbol{H}_2 \mid \boldsymbol{H}_1^T \otimes \boldsymbol{I}_{M_2}]$$

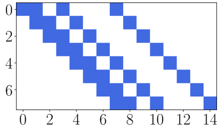
- Stabilizer matrix: $\boldsymbol{S} = \begin{pmatrix} \boldsymbol{X} \cdot \boldsymbol{H}_X \\ \boldsymbol{Z} \cdot \boldsymbol{H}_Z \end{pmatrix}$

- Using $[7,4,3]$ and $[15,7,5]$ BCH codes results in the $[[129,28]]$ HP code:

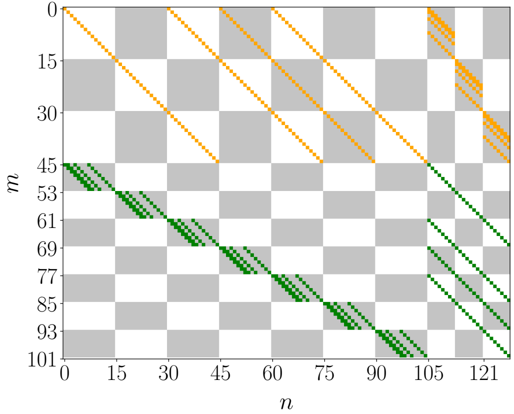
$\boldsymbol{H}_1$:



$\boldsymbol{H}_2$:

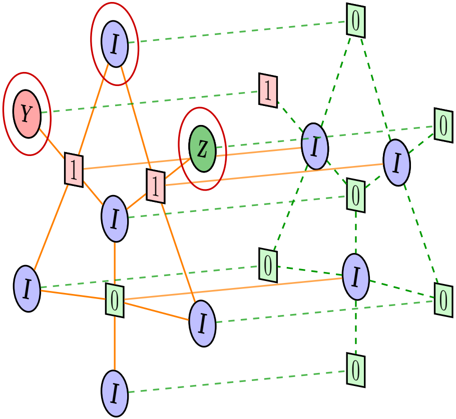


$\boldsymbol{S}$:

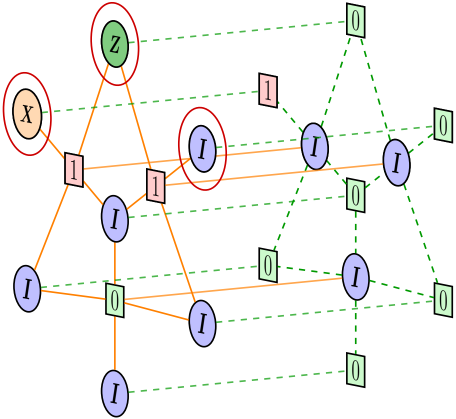


Split Beliefs in the [[129, 28]] HP Code

- Tanner graph $\mathcal{T}(\boldsymbol{H}_1)$ present in subgraph of $\mathcal{T}(\boldsymbol{S})$ induced by variable nodes with identical inner index



$$\boldsymbol{E}_1 = \boldsymbol{Z}_0^i \boldsymbol{Y}_1^i$$



$$\boldsymbol{E}_2 = \boldsymbol{X}_1^i \boldsymbol{Z}_3^i$$