Decoding of Topological Quantum Codes

Ching-Yi Lai

Institute of Communications Engineering
National Yang Ming Chiao Tung University
(NYCU)
Taiwan

doi.org/10.1109/JSAIT.2020.3011758
arXiv:2104.00304
arXiv:2104.13659

Joint work with Dr Kao-Yueh Kuo (NYCU)

Outline

Real Task: The Factoring Problem

- Integer factoring
  - Input: a large composite number of L bits
  - Output: a nontrivial integer factor
- no known (classical) algorithm can do factoring in polynomial time $O(L^k)$ for some constant k.
- The largest number that is the product of two large primes of similar size and yet factored is RSA-768.
  - a 768-bit number with 232 decimal digits, on December 12, 2009
  - It takes almost 2000 years of computing on a single-core 2.2 GHz AMD Opteron.
  - $\sim 10^{20}$ operations
- Peter Shor's quantum factoring algorithm: $O(L^3)$ in time with $O(L)$ qubits.

Real Task: The Factoring Problem

- Integer factoring
  - Input: a large composite number of L bits
  - Output: a nontrivial integer factor
- no known (classical) algorithm can do factoring in polynomial time $O(L^k)$ for some constant k.
- The largest number that is the product of two large primes of similar size and yet factored is RSA-768.
  - a 768-bit number with 232 decimal digits, on December 12, 2009
  - It takes almost 2000 years of computing on a single-core 2.2 GHz AMD Opteron.
  - $\sim 10^{20}$ operations
- Peter Shor's quantum factoring algorithm: $O(L^3)$ in time with $O(L)$ qubits.

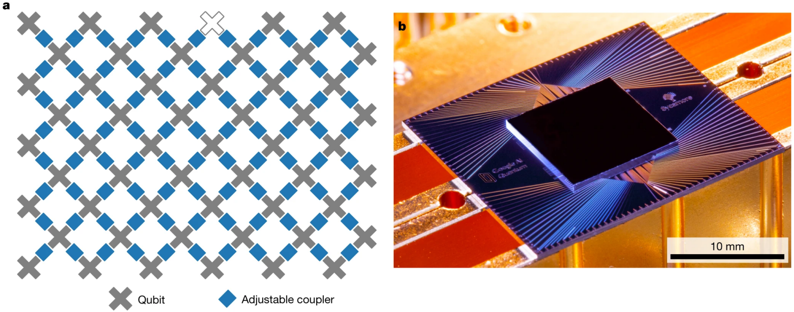
Need a quantum computer with $\sim$ 1000 qubits that affords 10^{10} operations!

Real Task: The Factoring Problem

- Integer factoring
  - Input: a large composite number of L bits
  - Output: a nontrivial integer factor
- no known (classical) algorithm can do factoring in polynomial time $O(L^k)$ for some constant k.
- The largest number that is the product of two large primes of similar size and yet factored is RSA-768.
  - a 768-bit number with 232 decimal digits, on December 12, 2009
  - It takes almost 2000 years of computing on a single-core 2.2 GHz AMD Opteron.
  - $\sim 10^{20}$ operations
- Peter Shor's quantum factoring algorithm: $O(L^3)$ in time with $O(L)$ qubits.

Need a quantum computer with $\sim$ 1000 qubits that affords 10^{10} operations!

Each quantum operation should be accurate up to $O(10^{-10})$ error rate!



Pauli and measurement errors

Average error	Isolated	Simultaneous
Single-qubit (e_1)	0.15%	0.16%
Two-qubit (e_2)	0.36%	0.62%
Two-qubit, cycle (e_{2c})	0.65%	0.93%
Readout (e_r)	3.1%	3.8%

Arute, F., Arya, K., Babbush, R. et al. “Quantum supremacy using a programmable superconducting processor," **Nature** 574, 505–510 (2019)

Need quantum error correction!

Discretization of the Errors

- The Pauli matrices

$$\{I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ\}$$

form a basis for the space of linear operators on a single-qubit $\mathcal{L}(\mathbb{C}^2)$.

Bit flip	$X\|0\rangle = \|1\rangle, \; X\|1\rangle = \|0\rangle$
Phase flip	$Z\|0\rangle = \|0\rangle, \; Z\|1\rangle = -\|1\rangle$

Discretization of the Errors

- The Pauli matrices

$$\{I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ\}$$

form a basis for the space of linear operators on a single-qubit $\mathcal{L}(\mathbb{C}^2)$.

Bit flip	$X\lvert 0\rangle = \lvert 1\rangle,\ X\lvert 1\rangle = \lvert 0\rangle$
Phase flip	$Z\lvert 0\rangle = \lvert 0\rangle,\ Z\lvert 1\rangle = -\lvert 1\rangle$

- (independent) Depolarizing channel with parameter ϵ:
  - no error (I) with probability $1 - \epsilon$
  - X with probability $\epsilon/3$
  - Y with probability $\epsilon/3$
  - Z with probability $\epsilon/3$

Commutation Relation

- n-fold Pauli operators $\{M_1 \otimes M_2 \otimes \cdots \otimes M_n : M_i \in \{I, X, Y, Z\}\}$.
  - $X \otimes X \otimes Y \otimes Z \otimes I \otimes Z$.
- Every n-fold Pauli operator has eigenvalue ± 1.
- Two Pauli operators either commute or anticommute with each other.
- For two Pauli operators f, g,

$$\langle f, g \rangle = \begin{cases} 0, & fg = gf; \\ 1, & \text{otherwise.} \end{cases}$$

Quantum Stabilizer Codes

- $\mathcal{S} = \langle \mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_m \rangle$: an Abelian subgroup of $\{I, X, Y, Z\}^n$ and $-I \notin \mathcal{S}$.

$$\langle \mathbf{S}_i, \mathbf{S}_j \rangle = 0.$$

- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ defined by stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $\mathbf{E} \in \{I, X, Y, Z\}^n$ of $\mathrm{wt}(\mathbf{E}) \leq d - 1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : \mathbf{S}|\psi\rangle = |\psi\rangle, \forall \mathbf{S} \in \mathcal{S}\}.$$

- For $\mathbf{S} \in \mathcal{S}$, $\mathbf{ES}$ and $\mathbf{E}$ have the same effect on the code space:

$$\mathbf{ES}|\psi\rangle = \mathbf{E}|\psi\rangle.$$

They are degenerate errors!

Quantum Stabilizer Codes

- $\mathcal{S} = \langle \mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_m \rangle$: an Abelian subgroup of $\{I, X, Y, Z\}^n$ and $-I \notin \mathcal{S}$.

$$\langle \mathbf{S}_i, \mathbf{S}_j \rangle = 0.$$

- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ defined by stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $\mathbf{E} \in \{I, X, Y, Z\}^n$ of $\mathrm{wt}(\mathbf{E}) \leq d - 1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : \mathbf{S}|\psi\rangle = |\psi\rangle, \forall \mathbf{S} \in \mathcal{S}\}.$$

- For $\mathbf{S} \in \mathcal{S}$, $\mathbf{ES}$ and $\mathbf{E}$ have the same effect on the code space:

$$\mathbf{ES}|\psi\rangle = \mathbf{E}|\psi\rangle.$$

They are degenerate errors!

Quantum Stabilizer Codes

- $\mathcal{S} = \langle \mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_m \rangle$: an Abelian subgroup of $\{I, X, Y, Z\}^n$ and $-I \notin \mathcal{S}$.

$$\langle \mathbf{S}_i, \mathbf{S}_j \rangle = 0.$$

- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ defined by stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $\mathbf{E} \in \{I, X, Y, Z\}^n$ of $\mathrm{wt}(\mathbf{E}) \leq d - 1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : \mathbf{S}|\psi\rangle = |\psi\rangle, \forall \mathbf{S} \in \mathcal{S}\}.$$

- For $\mathbf{S} \in \mathcal{S}$, **ES** and **E** have the same effect on the code space:

$$\mathbf{ES}|\psi\rangle = \mathbf{E}|\psi\rangle.$$

They are degenerate errors!

Quantum Stabilizer Codes

- $\mathcal{S} = \langle \mathbf{S}_1, \mathbf{S}_2, \cdots, \mathbf{S}_m \rangle$: an Abelian subgroup of $\{I, X, Y, Z\}^n$ and $-I \notin \mathcal{S}$.

$$\langle \mathbf{S}_i, \mathbf{S}_j \rangle = 0.$$

- An $[[n, k, d]]$ quantum stabilizer code $\mathcal{C}(\mathcal{S})$ defined by stabilizer group $\mathcal{S}$ is the 2^k-dimensional subspace of the n-qubit state space $\mathbb{C}^{2^n}$ fixed by $\mathcal{S}$ so that any error $\mathbf{E} \in \{I, X, Y, Z\}^n$ of $\mathrm{wt}(\mathbf{E}) \leq d - 1$ is detectable.

$$\mathcal{C}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : \mathbf{S}|\psi\rangle = |\psi\rangle, \forall \mathbf{S} \in \mathcal{S}\}.$$

- For $\mathbf{S} \in \mathcal{S}$, **ES** and **E** have the same effect on the code space:

$$\mathbf{ES}|\psi\rangle = \mathbf{E}|\psi\rangle.$$

They are degenerate errors!

- An error $\mathbf{E}$ can be detected if it anticommutes with some $\mathbf{S}_j \in \mathcal{S}$:

$$\mathbf{S}_j(\mathbf{E}|\psi\rangle) = -\mathbf{E}\mathbf{S}_j|\psi\rangle = -(\mathbf{E}|\psi\rangle).$$

- An error $\mathbf{E}$ can be detected if it anticommutes with some $\mathbf{S}_j \in \mathcal{S}$:

$$\mathbf{S}_j(\mathbf{E}|\psi\rangle) = -\mathbf{E}\mathbf{S}_j|\psi\rangle = -(\mathbf{E}|\psi\rangle).$$

- The error syndrome of E is a binary $(n-k)$-tuple of the measurement outcome of $\mathbf{S}_1, \ldots, \mathbf{S}_m$, given by

$$\langle \mathbf{E}, \mathbf{S}_1 \rangle, \langle \mathbf{E}, \mathbf{S}_2 \rangle, \ldots, \langle \mathbf{E}, \mathbf{S}_m \rangle$$

- Stabilizer parity-check matrix

$$H = \begin{bmatrix} \mathbf{S}_1 \\ \mathbf{S}_2 \\ \vdots \\ \mathbf{S}_M \end{bmatrix}$$

Decoding a stabilizer code: Given

- a check matrix $H \in \{I, X, Y, Z\}^{M \times N}$;
- a binary syndrome $z \in \{0, 1\}^M$ of some (unknown) $e \in \{I, X, Y, Z\}^N$;
- certain characteristics of the error model,

the decoder has to infer a vector $\hat{e} \in \{I, X, Y, Z\}^N$ such that

- $\langle \hat{e}, H_m \rangle = z_m$ for $m = 1, 2, \ldots, M$;
- $\hat{e} - e \in \mathcal{S}$

with probability as high as possible.

Quantum Low-Density Parity-Check (LDPC) Codes

- A desired quantum code has two important features:
  1. feasible syndrome measurements:
     - only a small subset of qubits are involved in a syndrome bit (sparse interaction)
     - the involved qubits are close (locality)
  2. efficient decoder (decoding time polynomial in n, preferably linear in n)

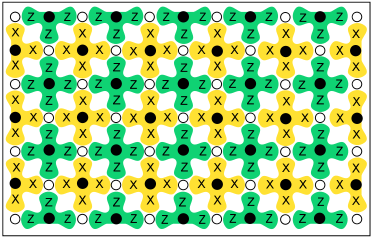
Quantum Low-Density Parity-Check (LDPC) Codes

- A desired quantum code has two important features:
  1. feasible syndrome measurements:
     - only a small subset of qubits are involved in a syndrome bit (sparse interaction)
     - the involved qubits are close (locality)
  2. efficient decoder (decoding time polynomial in n, preferably linear in n)

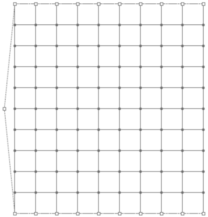
- Quantum version of LDPC codes are a good candidate for quantum error correction.
  - low-weight parity-checks
  - Belief propagation (BP) decoding

Surface Codes

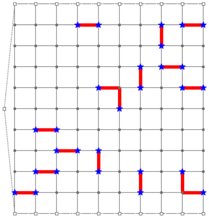
- Surface codes have the highest known simulated error threshold of about $0.1 \sim 0.5\%$. arXiv:0905.0531, arXiv:1208.0928



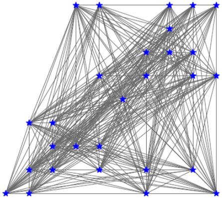
- Qubits are located at the white circles.
- The stabilizers (black circles) are of low-weight 4 or 3 and have local support.
- The minimum distance of the code is proportional to the side length of the lattice.
- Decoding by the minimum-weight perfect matching (MWPM) algorithm: $O(d^4 \log d)$



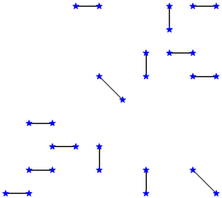
(a) Matching graph



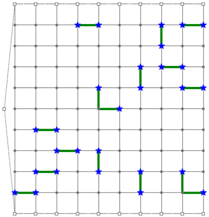
(b) Error



(c) Syndrome graph



(d) Minimum-weight perfect matching



(e) Correction

Oscar Higgott, “PyMatching: A Python package for decoding quantum codes with minimum-weight perfect matching,” 2021. arXiv:2105.13082

N. Delfosse and N. Nickerson. “Almost-linear time decoding algorithm for topological codes,"2017. arXiv:1709.06218

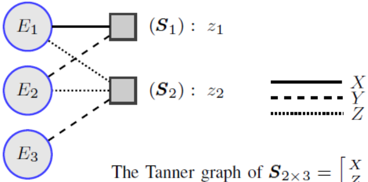
N. Delfosse and N. Nickerson. “Almost-linear time decoding algorithm for topological codes,"2017. arXiv:1709.06218

Good BP decoding algorithm for quantum error correction?

Potential: $O(d^2 \log d)$

Belief Propagation for Quantum Codes

- Sparse-graph quantum codes can be decoded by the belief propagation (BP) algorithm.

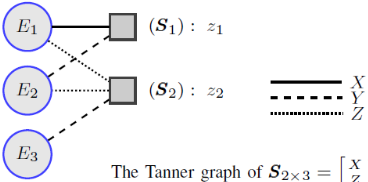


The Tanner graph of $S_{2\times 3} = \begin{bmatrix} X & Y & I \\ Z & Z & Y \end{bmatrix}$.

- A binary quantum code (that handles Pauli errors I, X, Y, Z) is decoded using **GF(4)-based BP**.

Belief Propagation for Quantum Codes

- Sparse-graph quantum codes can be decoded by the belief propagation (BP) algorithm.



The Tanner graph of $S_{2\times 3} = \begin{bmatrix} X & Y & I \\ Z & Z & Y \end{bmatrix}$.

- A binary quantum code (that handles Pauli errors I, X, Y, Z) is decoded using **GF(4)-based BP**.
- An independent depolarizing channel with rate ϵ so that a single qubit independently suffers a Pauli error I, X, Y, or Z with probability $(p^I, p^X, p^Y, p^Z) = (1-\epsilon, \epsilon/3, \epsilon/3, \epsilon/3)$,
- Estimate $(q_n^I, q_n^X, q_n^Y, q_n^Z)$, where $q_n^W = P(E_n = W|z)$.
- The log-likelihood ratios (LLRs) $\Gamma_n^X = \ln \frac{q_n^I}{q_n^X}$, $\Gamma_n^Y = \ln \frac{q_n^I}{q_n^Y}$, $\Gamma_n^Z = \ln \frac{q_n^I}{q_n^Z}$
- Output $\hat{E} = (\hat{E}_1, \hat{E}_2, \ldots, \hat{E}_N)$ such that

$$\hat{E}_n = \underset{W\in\{I,X,Y,Z\}}{\arg\max}\ \hat{P}(E_n = W|z).$$

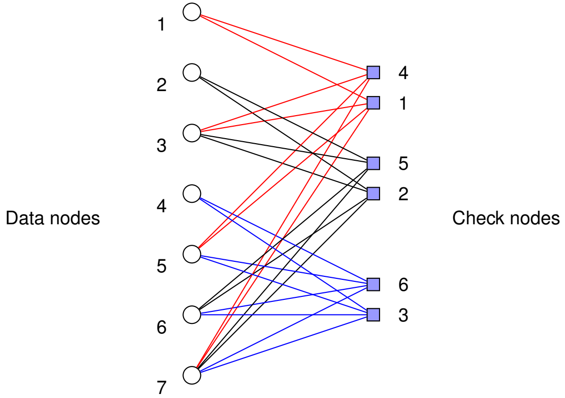
Issues of BP for Quantum Codes

- For complexity, GF(2)-based BP is usually used with necessary approximation to GF(4)
  - The computational cost for decoding in $GF(q)$ scales as $q \log q$.
    (Mackay, *Information Theory, Inference, and Learning Algorithms*, 2003)

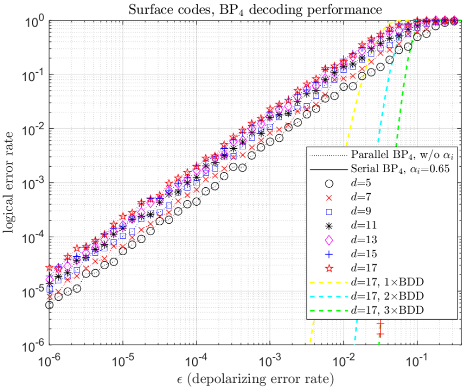
Issues of BP for Quantum Codes

- For complexity, GF(2)-based BP is usually used with necessary approximation to GF(4)
  - The computational cost for decoding in $GF(q)$ scales as $q \log q$.
    (Mackay, *Information Theory, Inference, and Learning Algorithms*, 2003)

- Quantum codes inevitably have many 4-cycles, which greatly degrade the performance of BP.



Decoding the Surface Codes–A Naive Trial



Belief Propagation for Quantum Codes

- Sparse-graph quantum codes can be decoded by the belief propagation (BP) algorithm.
- A binary quantum code (that handles Pauli errors I, X, Y, Z) is decoded using **GF(4)-based BP**.
- For complexity, GF(2)-based BP is usually used with necessary approximation to GF(4)
- The computational cost for decoding in $GF(q)$ scales as $q \log q$.
  (Mackay, *Information Theory, Inference, and Learning Algorithms*, 2003)

It is possible to **adapt** the required $GF(4)$-based BP to a $GF(2)$**-like BP** algorithm without additional cost.

K.-Y. Kuo and C.-Y. Lai, “Refined belief propagation decoding of sparse graph quantum codes,” IEEE J. Sel. Areas Inf. Theory, vol. 1, no. 2, pp. 487–498, Aug. 2020

An interpretation of the decoding problem on an energy function topography.

Decoding problem as Energy Function Minimization

- Given a syndrome s, the energy of $\mathbf{E} = E_1 \otimes E_2 \otimes \cdots \otimes E_n$ is

$$J(\mathbf{E}) = -\sum_{i=1}^{n-k} (-1)^{s_i} (-1)^{\langle \mathbf{E}, \mathbf{S}_i \rangle} \left(p^{\mathrm{wt}(\mathbf{E})} (1-p)^{n-\mathrm{wt}(\mathbf{E})} \right).$$

J. Bruck and M. Blaum, “Neural networks, error-correcting codes, and polynomials over the binary n-cube," IEEE Trans. Inf. Theory (Volume: 35, Issue: 5, Sep 1989)

Quantum Energy Function Minimization

- Let

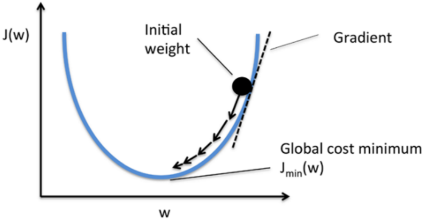
$$\lambda_W(\gamma^X, \gamma^Y, \gamma^Z) \triangleq \ln \frac{1 + e^{-\gamma^W}}{e^{-\gamma^X} + e^{-\gamma^Y} + e^{-\gamma^Z} - e^{-\gamma^W}}.$$

-

$$J(\Gamma) = \frac{1}{2} \|\Gamma - \Lambda\|_2^2$$
$$- \eta \sum_{m=1}^{M} 2 \tanh^{-1} \left((-1)^{z_m} \prod_{n \in \mathcal{N}(m)} \tanh \left(\frac{\lambda_{S_{mn}}(\Gamma_n)}{2} \right) \right)$$

where $\eta > 0 \in \mathbb{R}$.

Belief Propagation as a Gradient Decent



- Belief propagation can be considered as a **gradient descent algorithm** on the energy topography.

R. Lucas, M. Bossert, M. Breitbach, “On iterative soft-decision decoding of linear binary block codes and product codes," IEEE J. Sel. Areas Commun. 16, 276 (1998).

$$\frac{\partial J}{\partial \Gamma_n^W} = \Gamma_n^W - \Lambda_n^W + \sum_{\substack{m\in\mathcal{M}(n)\\ S_{mn}=W}} \frac{\eta g_{mn}(\Gamma) e^{-\Gamma_n^W}}{1+e^{-\Gamma_n^W}} \widetilde{\Delta}_{m\to n}$$

$$- \sum_{\substack{m\in\mathcal{M}(n)\\ \langle W, S_{mn}\rangle=1}} \frac{\eta g_{mn}(\Gamma) e^{-\Gamma_n^W}}{e^{-\Gamma_n^X} + e^{-\Gamma_n^Y} + e^{-\Gamma_n^Z} - e^{-\Gamma_n^{S_{mn}}}} \widetilde{\Delta}_{m\to n},$$

where

$$g_{mn}(\Gamma) = \frac{1-\tanh^2 \frac{\lambda_{S_{mn}}(\Gamma_n)}{2}}{1-\left(\prod_{l\in\mathcal{N}(m)} \tanh \frac{\lambda_{S_{ml}}(\Gamma_l)}{2}\right)^2} > 0,$$

and

$$\widetilde{\Delta}_{m\to n} = (-1)^{z_m} \prod_{n'\in\mathcal{N}(m)\setminus n} \tanh \frac{\lambda_{S_{mn'}}(\Gamma_{n'})}{2}.$$

Input: A check matrix $S \in \{I, X, Y, Z\}^{M\times N}$, a syndrome vector $z \in \{0,1\}^M$, and initial LLR values $\{\Lambda_n^X, \Lambda_n^Y, \Lambda_n^Z\}_{n=1}^N$.

Initialization. For $n = 1, 2, \ldots, N$, $W \in \{X, Y, Z\}$, and $m \in \mathcal{M}(n)$, let

$$\Gamma_{n\to m}^W = \Lambda_n^W.$$

Horizontal Step. For $m = 1, 2, \ldots, M$ and $n \in \mathcal{N}(m)$, compute

$$\Delta_{m\to n} = (-1)^{z_m} \boxplus_{n'\in\mathcal{N}(m)\setminus\{n\}} \lambda_{S_{mn'}}(\Gamma_{n'\to m}). \tag{9}$$

Vertical Step. For $n = 1, 2, \ldots, N$ and $W \in \{X, Y, Z\}$, compute

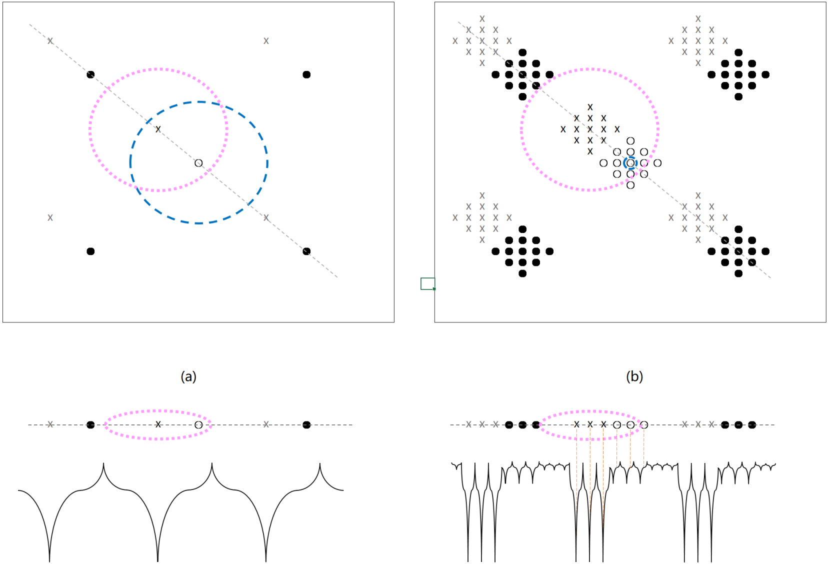
$$\Gamma_n^W = \Lambda_n^W + \sum_{\substack{m\in\mathcal{M}(n)\\ \langle W, S_{mn}\rangle=1}} \Delta_{m\to n} \tag{10}$$

- **(Hard Decision.)** Let $\hat{E} = \hat{E}_1\hat{E}_2\cdots\hat{E}_N$, where $\hat{E}_n = I$ if $\Gamma_n^W < 0$ for all $W \in \{X, Y, Z\}$, and $\hat{E}_n = \arg\max_{W\in\{X,Y,Z\}} \Gamma_n^W$, otherwise.
- If $\langle \hat{E}, S_m\rangle = z_m \ \forall\ m$, halt and return "SUCCESS";
- Otherwise, if a maximum number of iterations is reached, halt and return "FAIL";
- Otherwise, for $n = 1, 2, \ldots, N$, $W \in \{X, Y, Z\}$, and $m \in \mathcal{M}(n)$, compute

$$\Gamma_{n\to m}^W = \Gamma_n^W - \langle W, S_{mn}\rangle \Delta_{m\to n}. \tag{11}$$

- Repeat from the horizontal step.

Energy Topography



New Ingradients

- Large step size: Choose α_i to be smaller than 1.
  - This contradicts to what people will do in classical coding theory.

New Ingradients

- Large step size: Choose α_i to be smaller than 1.
  - This contradicts to what people will do in classical coding theory.
- Memory effects
  - By slightly changing the original algorithm, the BP can have a memory effect without additional complexity.
  - The memory effect provides resistance to wrong belief and maintain a momentum to escape from a local barrier.

New Ingradients

- Large step size: Choose α_i to be smaller than 1.
  - This contradicts to what people will do in classical coding theory.
- Memory effects
  - By slightly changing the original algorithm, the BP can have a memory effect without additional complexity.
  - The memory effect provides resistance to wrong belief and maintain a momentum to escape from a local barrier.

Our MBP converges significantly better than conventional BP.

New Ingradients

- Large step size: Choose α_i to be smaller than 1.
  - This contradicts to what people will do in classical coding theory.
- Memory effects
  - By slightly changing the original algorithm, the BP can have a memory effect without additional complexity.
  - The memory effect provides resistance to wrong belief and maintain a momentum to escape from a local barrier.

Our MBP converges significantly better than conventional BP.

- Initial physical error rate matters.

M. Hagiwara, M. P. C. Fossorier, and H. Imai, “Fixed initialization decoding of LDPC codes over a binary symmetric channel," IEEE Trans. Inf. Theory 58, 2321 (2012).

Input: A check matrix $S \in \{I, X, Y, Z\}^{M\times N}$, a syndrome vector $z \in \{0,1\}^M$, and initial LLR values $\{\Lambda_n^X, \Lambda_n^Y, \Lambda_n^Z\}_{n=1}^N$.

Initialization. For $n = 1, 2, \ldots, N$, $W \in \{X, Y, Z\}$, and $m \in \mathcal{M}(n)$, let

$$\Gamma_{n\to m}^W = \Lambda_n^W.$$

Horizontal Step. For $m = 1, 2, \ldots, M$ and $n \in \mathcal{N}(m)$, compute

$$\Delta_{m\to n} = (-1)^{z_m} \boxplus_{n'\in\mathcal{N}(m)\setminus\{n\}} \lambda_{S_{mn'}}(\Gamma_{n'\to m}). \tag{9}$$

Vertical Step. For $n = 1, 2, \ldots, N$ and $W \in \{X, Y, Z\}$, compute

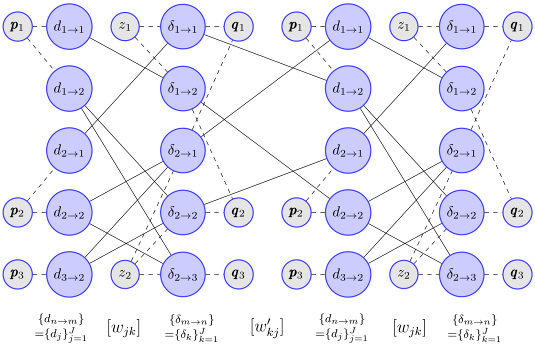
$$\Gamma_n^W = \Lambda_n^W + \frac{1}{\alpha} \sum_{\substack{m\in\mathcal{M}(n)\\ \langle W, S_{mn}\rangle = 1}} \Delta_{m\to n} - \beta \sum_{\substack{m\in\mathcal{M}(n)\\ S_{mn}=W}} \Delta_{m\to n}. \tag{10}$$

- **(Hard Decision.)** Let $\hat{E} = \hat{E}_1\hat{E}_2\cdots\hat{E}_N$, where $\hat{E}_n = I$ if $\Gamma_n^W < 0$ for all $W \in \{X, Y, Z\}$, and $\hat{E}_n = \arg\max_{W\in\{X,Y,Z\}} \Gamma_n^W$, otherwise.
- If $\langle \hat{E}, S_m\rangle = z_m \ \forall\, m$, halt and return "SUCCESS";
- Otherwise, if a maximum number of iterations is reached, halt and return "FAIL";
- Otherwise, for $n = 1, 2, \ldots, N$, $W \in \{X, Y, Z\}$, and $m \in \mathcal{M}(n)$, compute

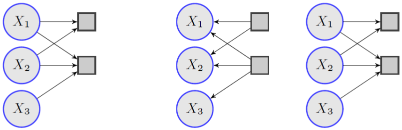
$$\Gamma_{n\to m}^W = \Gamma_n^W - \langle W, S_{mn}\rangle \Delta_{m\to n}. \tag{11}$$

- Repeat from the horizontal step.

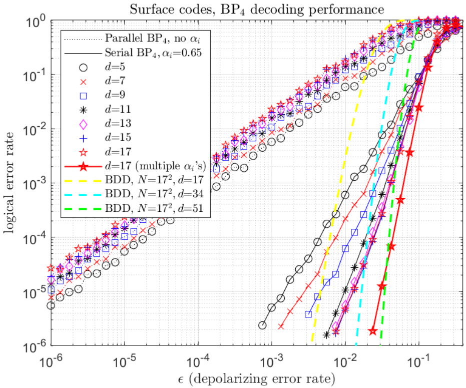
BP as an RNN

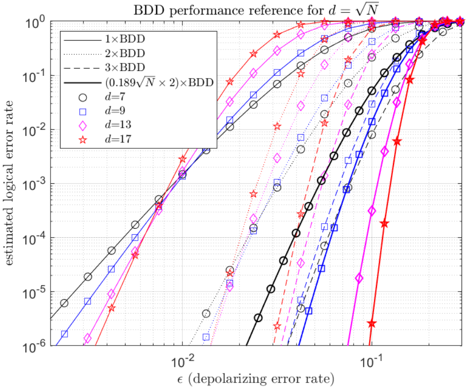


p_1
$d_{1\to1}$
z_1
$\delta_{1\to1}$
q_1
$d_{1\to2}$
$\delta_{1\to2}$
$d_{2\to1}$
$\delta_{2\to1}$
p_2
$d_{2\to2}$
$\delta_{2\to2}$
q_2
p_3
$d_{3\to2}$
z_2
$\delta_{2\to3}$
q_3
$\{d_{n\to m}\} = \{d_j\}_{j=1}^{J}$
$[w_{jk}]$
$\{\delta_{m\to n}\} = \{\delta_k\}_{k=1}^{J}$
$[w'_{kj}]$



X_1
X_2
X_3





Kao-Yueh Kuo and C.-Y. Lai, "Exploiting Degeneracy in Belief Propagation Decoding of Quantum Codes," in preparation.

TABLE 1. Most significant modified decoding strategies for QLDPC codes.

Year	Decoding strategy
2004	Initial Proposal for a Modified SPA-based decoding Strategy [16].
2005	Correlation Exploiting Decoder [20].
2008	Freezing, Collision & Random Perturbation Decoders [53].
2012	Enhanced Feedback Decoder [113].
2015	Supernode Decoder [18].
2019	Adjusted & Augmented Decoders [115].
2019/2020	Ordered Statistics Decoder [116], [117].
2020	Refined Belief Propagation Decoding [118].

P. Fuentes et al., "Degeneracy and Its Impact on Decoding of Sparse Quantum Codes," *IEEE Access*, vol. 9, pp. 89093–89119, 2021.

[16] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," IEEE Trans. Inf. Theory, vol. 50, no. 10, pp. 2315–2330, Oct. 2004

[20] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low density generator matrix over different quantum channels," in Proc. 4th Int. Symp. Turbo Codes Related Topics, 2006, pp. 1–6.

[53] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," Quant. Inf. Comput., vol. 8, no. 10, p. 987, 2008.

[113] Y.-J. Wang, B. C. Sanders, B.-M. Bai, and X.-M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 1231–1241, Feb. 2012

[18] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," IEEE Access, vol. 3, pp. 2492–2519, Nov. 2015

[115] A. Rigby, J. C. Olivier, and P. Jarvis, "Modified belief propagation decoders for quantum low-density parity-check codes," Phys. Rev. A, vol. 100, no. 1, Jul. 2019

[116] P. Panteleev and G. Kalachev, "Degenerate quantum LDPC codes with good finite length performance," 2019, arXiv:1904.02703.

[117] J. Roffe, D. R. White, S. Burton, and E. Campbell, "Decoding across the quantum low-density parity-check code landscape," Phys. Rev. Res., vol. 2, no. 4, Dec. 2020

[118] K.-Y. Kuo and C.-Y. Lai, "Refined belief propagation decoding of sparsegraph quantum codes," IEEE J. Sel. Areas Inf. Theory, vol. 1, no. 2, pp. 487–498, Aug. 2020

TABLE 1. **Most significant modified decoding strategies for QLDPC codes.**

2004	Initial Proposal for a Modified SPA-based decoding Strategy [16].
2005	Correlation Exploiting Decoder [20].
2008	Freezing, Collision & Random Perturbation Decoders [53].
2012	Enhanced Feedback Decoder [113].
2015	Supernode Decoder [18].
2019	Adjusted & Augmented Decoders [115].
2019/2020	Ordered Statistics Decoder [116], [117].
2020	Refined Belief Propagation Decoding [118].

P. Fuentes et al., "Degeneracy and Its Impact on Decoding of Sparse Quantum Codes," *IEEE Access*, vol. 9, pp. 89093–89119, 2021.

[16] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," IEEE Trans. Inf. Theory, vol. 50, no. 10, pp. 2315–2330, Oct. 2004

[20] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low density generator matrix over different quantum channels," in Proc. 4th Int. Symp. Turbo Codes Related Topics, 2006, pp. 1–6.

[53] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," Quant. Inf. Comput., vol. 8, no. 10, p. 987, 2008.

[113] Y.-J. Wang, B. C. Sanders, B.-M. Bai, and X.-M. Wang, "Enhanced feedback iterative decoding of sparse quantum codes," IEEE Trans. Inf. Theory, vol. 58, no. 2, pp. 1231–1241, Feb. 2012

[18] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," IEEE Access, vol. 3, pp. 2492–2519, Nov. 2015

[115] A. Rigby, J. C. Olivier, and P. Jarvis, "Modified belief propagation decoders for quantum low-density parity-check codes," Phys. Rev. A, vol. 100, no. 1, Jul. 2019

[116] P. Panteleev and G. Kalachev, "Degenerate quantum LDPC codes with good finite length performance," 2019, arXiv:1904.02703.

[117] J. Roffe, D. R. White, S. Burton, and E. Campbell, "Decoding across the quantum low-density parity-check code landscape," Phys. Rev. Res., vol. 2, no. 4, Dec. 2020

[118] K.-Y. Kuo and C.-Y. Lai, "Refined belief propagation decoding of sparsegraph quantum codes," IEEE J. Sel. Areas Inf. Theory, vol. 1, no. 2, pp. 487–498, Aug. 2020

K.-Y. Kuo and C.-Y. Lai, "Log-domain decoding of quantum LDPC codes over binary finite fields," `arXiv:2104.00304`
K.-Y. Kuo and C.-Y. Lai, "Exploiting Degeneracy in Belief Propagation Decoding of Quantum Codes," `arXiv:2104.13659`

Thank you!