# Fast Erasure Decoder for a Class of Quantum LDPC Codes


**Nicholas Connolly*[1], Vivien Londe[2], Anthony Leverrier[1], and Nicolas Delfosse[3]**

[1]Inria Paris, [2]Microsoft France, [3]Microsoft Quantum



https://arxiv.org/abs/2208.01002


## Main Result


We consider the decoding problem for HGP codes, one of the most popular families of quantum LDPC codes. We propose a decoder which closely approximates the maximum likelihood decoder, but with computational complexity reduced by an order of magnitude.


## Classical Codes and Tanner Graphs

A classical binary linear **code** $C$ is a vector space over $\mathbb{Z}_2$. A code of **length** $n$ is defined to be the kernel of an $r \times n$ **parity check matrix** $H$. Vectors $x \in C \subseteq \mathbb{Z}_2^n$ are known as **codewords**, and $C$ has **dimension** $k$ as a subspace of $\mathbb{Z}_2^n$. A code $C = \ker(H)$ may be visualized by its **Tanner graph** $T(H)$.

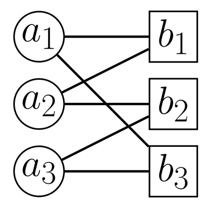
| Code | Parity Check Matrix | Tanner Graph |
|---|---|---|
| $\ker(H) = \left\{ \begin{bmatrix}0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix} \right\}$ | $H = \begin{bmatrix}1&1&0\\0&1&1\\1&0&1\end{bmatrix}$ | $T(H) =$  |

**Figure 1:** The 3-bit repetition code, its parity check matrix, and its Tanner graph.

- $T(H)$ is a bipartite graph with vertex set $A \cup B$.
  - $A = \{a_1, \cdots a_n\}$ is the set of **bits** in $C$ (one vertex for each column in $H$).
  - $B = \{b_1, \cdots, b_r\}$ is the set of **checks** in $C$ (one vertex for each row in $H$).
- There exists an edge between $b_i$ and $a_j$ if and only if $H_{i,j} \neq 0$.
- $C = \ker(H)$ is a **low density parity check (LDPC) code** if $H$ is a sparse matrix.

## Classical Error Correction

1. An initial codeword $x \in C = \ker(H) \subseteq \mathbb{Z}_2^n$ is sent.
2. A corrupted codeword $y = x + e \in \mathbb{Z}_2^n$ is received.
3. A syndrome measurement $s = Hy = He \in \mathbb{Z}_2^r$ is made.
4. The decoder predicts an error $\hat{e}$ satisfying $s = H\hat{e}$.
5. Error correction $y + \hat{e}$ is performed.
6. The original codeword is recovered if $y + \hat{e} = x$.

message, noise, syndrome

$$\underbrace{\begin{bmatrix}1\\1\\1\end{bmatrix}}_{x} \Rightarrow \underbrace{\begin{bmatrix}1\\1\\1\end{bmatrix} + \begin{bmatrix}0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\1\\0\end{bmatrix}}_{x+e=y} \Rightarrow \underbrace{\begin{bmatrix}0\\1\\1\end{bmatrix}}_{s=Hy}$$

**Figure 2:** Example of a message corrupted by a noisy channel, and the resulting syndrome measurement.

## The Erasure Channel and the Peeling Decoder

- An **erasure** refers to the loss of a *known* subset of bits $\mathcal{E}$.
  - $\mathcal{E}$ induces a subgraph of the Tanner graph $T(H)$.
  - **Figure:** $H = \begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}$ with $\mathcal{E} = \{a_3, a_4, a_5\}$.
- Erasure correction can be achieved using error correction.
  - Erased bits in $\mathcal{E}$ are assigned random values.
- The **Peeling Decoder** does this efficiently for LDPC codes.

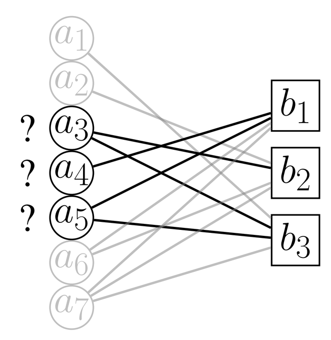


**Figure 3:** Erasure-induced subgraph of the Tanner graph $T(H)$.

1. Given erasure pattern $\mathcal{E}$, a **dangling** (degree 1) check in the erasure induced subgraph of $T(H)$ is selected.
2. The adjacent erased bit is corrected and then removed from $\mathcal{E}$, shrinking the erasure and the subgraph.
3. The algorithm terminates when $\mathcal{E} = \emptyset$, or fails when $\mathcal{E}$ is a **stopping set** (contains no dangling checks).

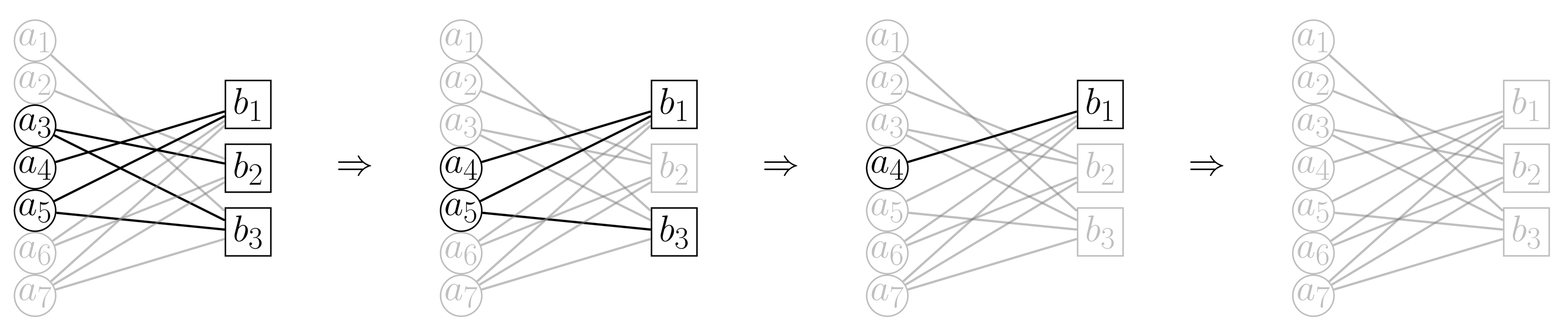
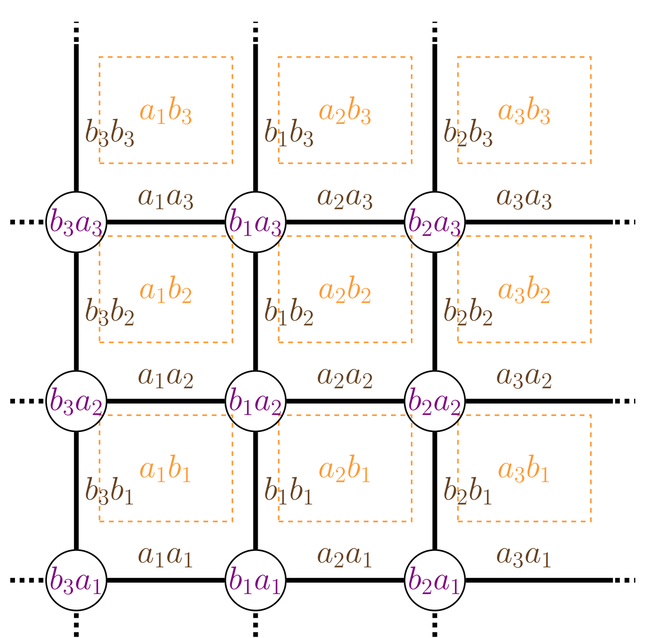


**Figure 4:** Example of a sequence of stages in the peeling decoder; each "peel" reduces the size of the erasure $\mathcal{E}$ until empty.

## Families of Quantum Codes

A **quantum code** of length $N$ and dimension $K$ is a subspace of a Hilbert space; vectors are $N$-qubit states $|\psi\rangle \in \mathbb{C}^N$. Errors on a state $|\psi\rangle$ are described discretely by $N$-qubit Pauli operators in $P_N = \{I, X, Z, Y\}^{\otimes N}$.

- **Stabilizer codes** are defined as the space of states left fixed by some subgroup of the Pauli-group $P_N$.
- **CSS codes** are a subclass of stabilizer codes defined by *commuting* $N$-qubit $X$- and $Z$-Pauli operators.
  - $X$- and $Z$-Pauli **stabilizer generators** define the rows of matrices $H_X$ and $H_Z$ (where $H_X H_Z^T = 0$).
  - CSS $Z$ and $X$ error correction is modeled using the classical codes $C_X = \ker(H_X)$ and $C_Z = \ker(H_Z)$.
- **Surface codes** are a subclass of CSS codes defined from a cellulation of a surface.



### Example of the $3 \times 3$ Toric Code

- Edges define qubits.
- Vertices define $X$-stabilizer generators.
  - $X^{b_1 a_2} = X_{a_1a_2} X_{a_2a_2} X_{b_1b_1} X_{b_1b_2}$
  - Detect $Z$-errors on adjacent qubits.
- Plaquettes define $Z$-stabilizer generators.
  - $Z^{a_2b_2} = Z_{a_2a_2} Z_{a_2a_3} Z_{b_1b_2} Z_{b_2b_2}$
  - Detect $X$-errors on adjacent qubits.
- $X$- and $Z$-stabilizers overlap on 0 or 2 qubits.
  - Commutivity: $X^{b_1a_2} Z^{a_2b_2} = Z^{a_2b_2} X^{b_1a_2}$

**Figure 5:** Standard lattice visualization of the $3 \times 3$ toric code, with labels matching the HGP Tanner graph of Figure 6.

## Hypergraph Product Codes

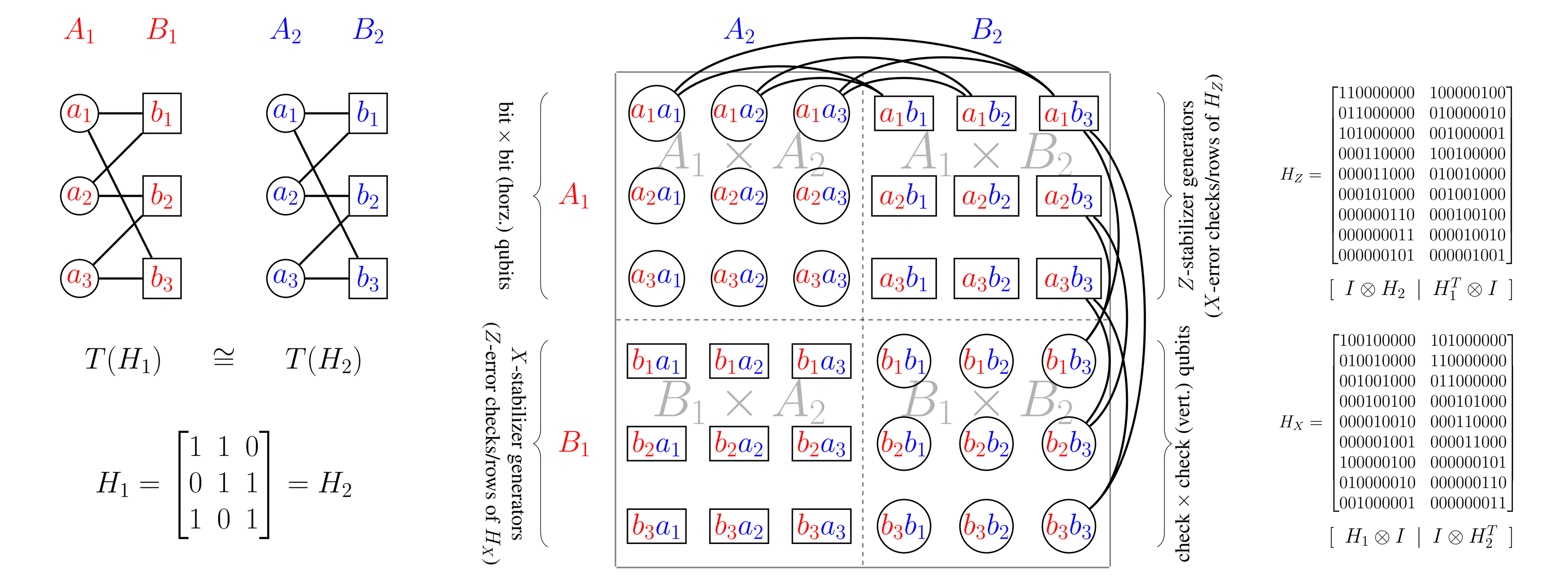


**Figure 6:** Geometric structure of the Tanner graph of a HGP of two 3-bit repetition codes (equivalent to the $3 \times 3$ toric code).

### Theorem (Tillich-Zémor):

The **hypergraph product** (HGP) code of two classical codes $C_1 = \ker(H_1)$ and $C_2 = \ker(H_2)$ is the quantum code $C = \mathrm{CSS}(C_X, C_Z)$, where $C_X = \ker(H_X)$ and $C_Z = \ker(H_Z)$ have parity check matrices $H_X$ and $H_Z$ defined from $H_1$ and $H_2$ by the formulas shown in Figure 6.

- $C$ has length $N = n_1 n_2 + r_1 r_2$, where $H_1 = [r_1 \times n_1]$ and $H_2 = [r_2 \times n_2]$ are the matrix sizes.
- $C$ has dimension $K = N - \mathrm{rank}(H_X) - \mathrm{rank}(H_Z)$.
- $C$ has minimum distance $\min(d_1, d_2)$, where $d_1$ and $d_2$ are the minimum distances of $C_1$ and $C_2$.

## Generalized Peeling Decoder for HGP Codes

By mapping Pauli errors $X_i, Z_i \in P_N$ onto binary strings $e_i \in \mathbb{Z}_2^N$, the erasure decoding problem for a CSS code can be modeled as a classical erasure problem using $H_Z$ or $H_X$, and the peeling decoder directly applied.

- We try to use the classical peeling decoder with HGP codes, but observe that it does not perform well.
- This poor performance results from the presence of stopping sets unique to HGP codes.
- We design different versions of a generalized peeling decoder to overcome these stopping sets.
- Numerical simulations show that we can achieve a performance close to the maximum likelihood decoder.

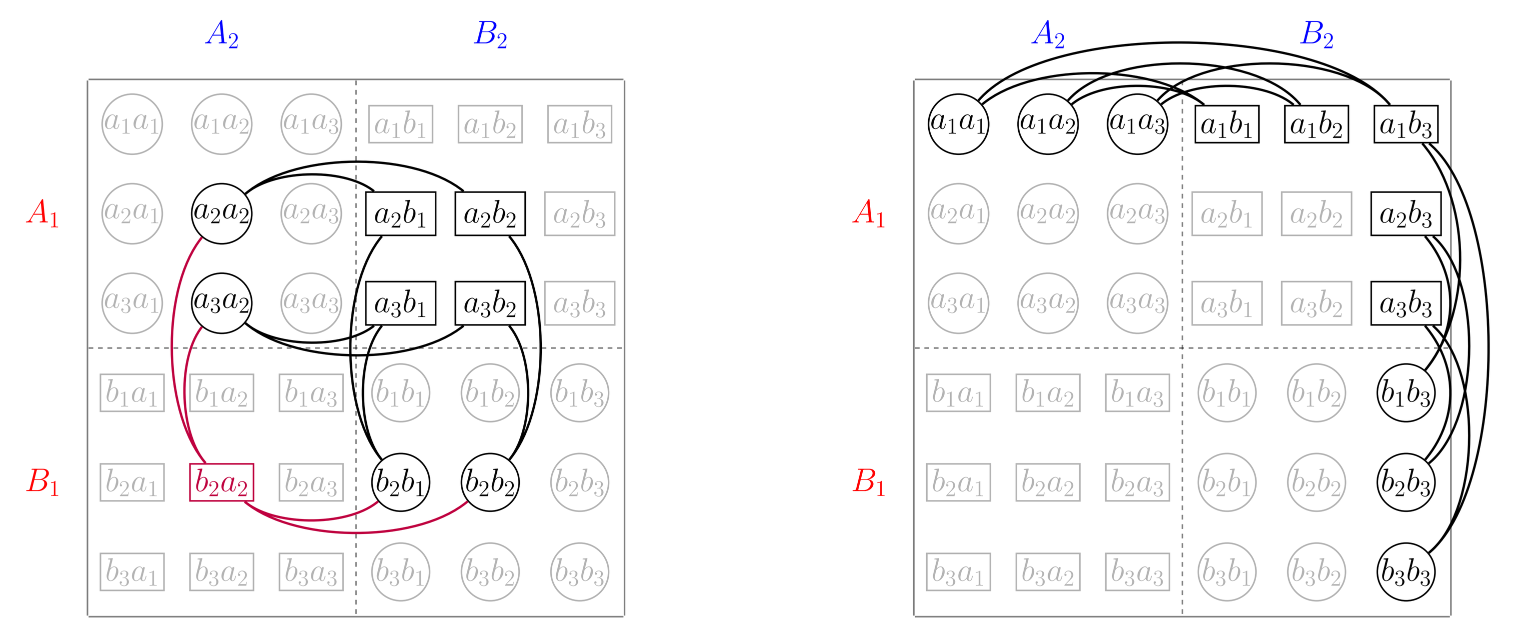


**Figure 7:** Two types of HGP stopping sets for the peeling decoder: stabilizer (left) and classical (right)

### Stabilizer Stopping Sets and the Pruned Peeling Decoder

1. Given erasure pattern $\mathcal{E}$, apply the peeling decoder algorithm until $\mathcal{E}$ contains no remaining dangling checks.
2. If $\mathcal{E}$ contains the qubit-support $S$ of an $X$-type stabilizer, then $S \subseteq \mathcal{E}$ is a **stabilizer stopping set** of $T(H_Z)$.
3. Remove a qubit in $S$ from $\mathcal{E}$ and continue peeling (errors are corrected *up to multiplication by a stabilizer*).

### Classical Stopping Sets and the Vertical-Horizontal (VH) Decoder

1. Apply the pruned peeling decoder algorithm until $\mathcal{E}$ contains no dangling checks and no erased stabilizers.
2. $\mathcal{E}$ contains a **classical stopping set** if it contains a stopping set for $T(H_1)$ (vertical) or $T(H_2)$ (horizontal).
3. Apply the Gaussian (ML) decoder on classical stopping sets in sequence and continue peeling.
4. The VH decoder will terminate provided clusters of classical stopping sets do not form a closed loop.

## Numerical Simulations and Computational Complexity

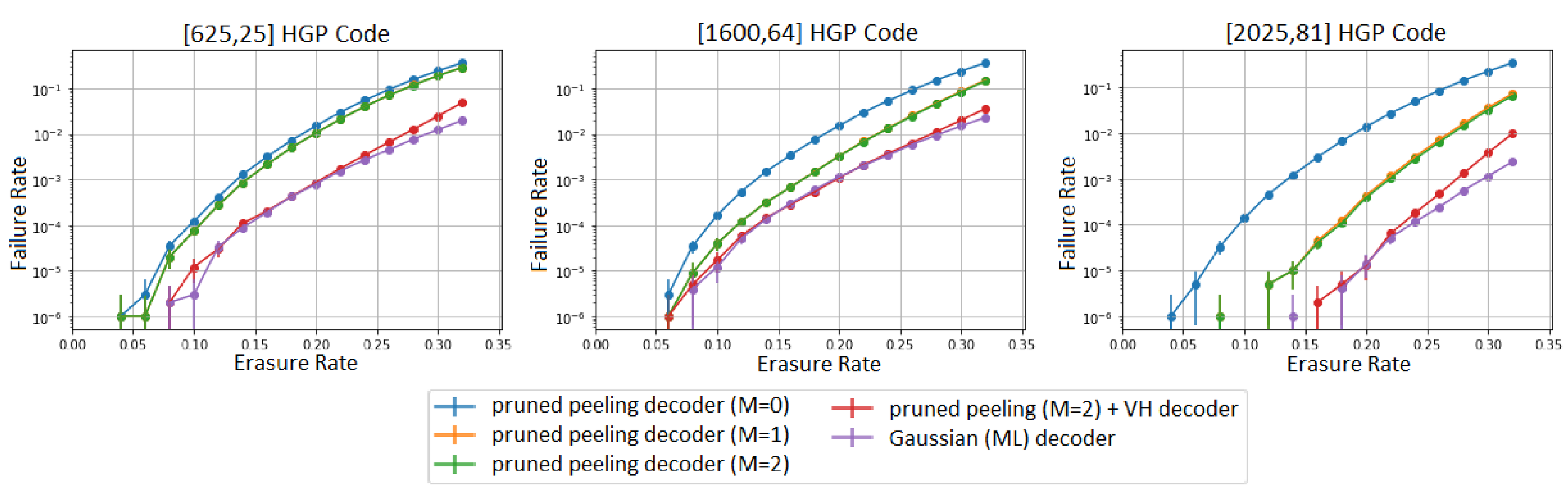



**Figure 8:** Comparison of performance for Pruned Peeling, VH, and ML decoders for three randomly generated HGP codes.

### VH Decoder Performance

Simulations show that pruned peeling (with $M$ stabilizer generators) combined with the VH decoder performs almost as well as the Gaussian (ML) decoder applied to random LDPC HGP codes at low erasure rates.

### Complexity of the VH Decoder

For a HGP code of length $N$, the classical codes used in the construction have length on the order of $\sqrt{N}$.

- The VH decoder is dominated by the cubic complexity Gaussian decoder on these classical codes.
- Complexity grows as $O(N^{\frac{3}{2}})$ per classical code and $O(N^2)$ across all classical codes.
- Probabilistic implementation of the Gaussian decoder in quadratic complexity reduces this to $O(N^{1.5})$.