Breaking the Orthogonality Barrier: Large-Girth Regular LDPC Structures with Favorable Distance for Quantum Error Correction

Kenta Kasai

Institute of Science Tokyo

2026 Information Theory and Applications Workshop (ITA)
Bahia Resort Hotel, San Diego
February 8–13, 2026

Motivation: Classical vs Quantum LDPC

Classical: sparse+random+large girth $\Rightarrow$ strong BP, large distance.

Quantum: CSS constraint $H_X H_Z' = 0$ couples H_X, H_Z.

Issue: naive orthogonality $\Rightarrow$ short cycles, small distance.

Goal: keep classical structure *without* the orthogonality distance penalty.

Problem:

Parent construction

$$\hat{H}_X = \begin{bmatrix} H_X \\ \tilde{H}_X \end{bmatrix}, \qquad \hat{H}_Z = \begin{bmatrix} H_Z \\ \tilde{H}_Z \end{bmatrix}, \qquad \hat{H}_X(\hat{H}_Z)' = 0$$

- Full orthogonality forces $H_X(\tilde{H}_Z)' = 0$, $H_Z(\tilde{H}_X)' = 0$.
- Removed rows $\tilde{H}_X, \tilde{H}_Z$ become logicals.
- $d_{\min} \leq$ row weight.

Design Principle

- Active orthogonality only: $H_X H_Z' = 0$.
- Latent blocks non-orthogonal: $H_X(\tilde{H}_Z)' \neq 0$, $H_Z(\tilde{H}_X)' \neq 0$.
- Latent distances: $d_X^{(\mathrm{lat})}, d_Z^{(\mathrm{lat})}$.

Latent-based distances

$$d_X^{(\mathrm{lat})} := \min\{\big(C_Z \cap \mathrm{Row}(\tilde{H}_X)\big) \setminus C_X^{\perp}\},$$
$$d_Z^{(\mathrm{lat})} := \min\{\big(C_X \cap \mathrm{Row}(\tilde{H}_Z)\big) \setminus C_Z^{\perp}\}.$$

Code Construction

Example $J = 3, L = 12.$

$$\hat{H}_X = \left(\begin{array}{cccccc|cccccc}
F_0 & F_1 & F_2 & F_3 & F_4 & F_5 & G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\
F_5 & F_0 & F_1 & F_2 & F_3 & F_4 & G_5 & G_0 & G_1 & G_2 & G_3 & G_4 \\
F_4 & F_5 & F_0 & F_1 & F_2 & F_3 & G_4 & G_5 & G_0 & G_1 & G_2 & G_3 \\
\hline
F_3 & F_4 & F_5 & F_0 & F_1 & F_2 & G_3 & G_4 & G_5 & G_0 & G_1 & G_2 \\
F_2 & F_3 & F_4 & F_5 & F_0 & F_1 & G_2 & G_3 & G_4 & G_5 & G_0 & G_1 \\
F_1 & F_2 & F_3 & F_4 & F_5 & F_0 & G_1 & G_2 & G_3 & G_4 & G_5 & G_0
\end{array}\right), \qquad
\hat{H}_X(\hat{H}_Z)' = \left(\begin{array}{ccc|ccc}
\Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 & \Psi_5 \\
\Psi_5 & \Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 \\
\Psi_4 & \Psi_5 & \Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 \\
\hline
\Psi_3 & \Psi_4 & \Psi_5 & \Psi_0 & \Psi_1 & \Psi_2 \\
\Psi_2 & \Psi_3 & \Psi_4 & \Psi_5 & \Psi_0 & \Psi_1 \\
\Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 & \Psi_5 & \Psi_0
\end{array}\right),$$

$$\hat{H}_Z = \left(\begin{array}{cccccc|cccccc}
G'_0 & G'_5 & G'_4 & G'_3 & G'_2 & G'_1 & F'_0 & F'_5 & F'_4 & F'_3 & F'_2 & F'_1 \\
G'_1 & G'_0 & G'_5 & G'_4 & G'_3 & G'_2 & F'_1 & F'_0 & F'_5 & F'_4 & F'_3 & F'_2 \\
G'_2 & G'_1 & G'_0 & G'_5 & G'_4 & G'_3 & F'_2 & F'_1 & F'_0 & F'_5 & F'_4 & F'_3 \\
\hline
G'_3 & G'_2 & G'_1 & G'_0 & G'_5 & G'_4 & F'_3 & F'_2 & F'_1 & F'_0 & F'_5 & F'_4 \\
G'_4 & G'_3 & G'_2 & G'_1 & G'_0 & G'_5 & F'_4 & F'_3 & F'_2 & F'_1 & F'_0 & F'_5 \\
G'_5 & G'_4 & G'_3 & G'_2 & G'_1 & G'_0 & F'_5 & F'_4 & F'_3 & F'_2 & F'_1 & F'_0
\end{array}\right), \quad
\Psi_r := \sum_{u=0}^{L/2-1} \left(F_u G_{r-u} + G_{r-u} F_u\right), \quad r \in [L/2].$$

Code Construction (Cont.)

Example $J = 3, L = 12.$

$$\hat{H}_X(\hat{H}_Z)' = \left(\begin{array}{ccc|ccc} \Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 & \Psi_5 \\ \Psi_5 & \Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 \\ \Psi_4 & \Psi_5 & \Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 \\ \hline \Psi_3 & \Psi_4 & \Psi_5 & \Psi_0 & \Psi_1 & \Psi_2 \\ \Psi_2 & \Psi_3 & \Psi_4 & \Psi_5 & \Psi_0 & \Psi_1 \\ \Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 & \Psi_5 & \Psi_0 \end{array}\right)$$

Γ	G_0	G_1	G_2	G_3	G_4	G_5
F_0	C	C	C		C	C
F_1	C	C		C	C	C
F_2	C		C	C	C	C
F_3		C	C	C	C	C
F_4	C	C	C	C	C	
F_5	C	C	C	C		C

Code Construction (Cont.)

Required constraints on F_i, G_j:

- Commute on Γ
- Avoid short cycles
- Full search is combinatorial.

Search strategy:

- Restrict to affine permutations on $\mathbb{Z}_P$.
- Checks are P-independent.
- Sequential construction is fast[1].

[1] `github.com/kasaikenta/joint_BP_plus_PP`

Constructed Code Example

- Girth-8 $(3, 12)$-regular $[[9216, 4612, \leq 48]]$ with $P = 768$.
- Explicit weight-48 logicals $\Rightarrow d_{\text{min}} \leq 48$.
- $d_X^{(\text{lat})} = d_Z^{(\text{lat})} = 48$ (proof omitted).
- No logical failures observed $\Rightarrow d_{\text{min}}$ likely near 48.

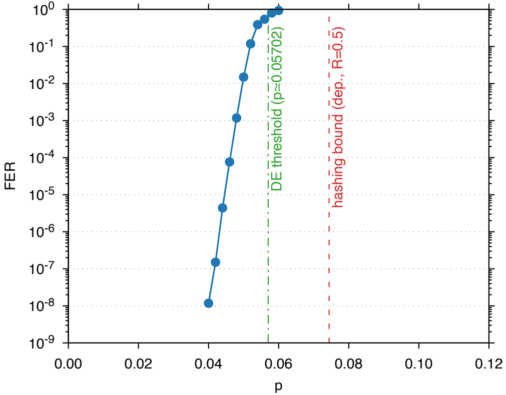
Decoding Algorithm (BP + Post-Processing)

1. **Joint BP:** decode on H_X, H_Z using X/Z correlations.
2. **Trigger:** if unsatisfied checks are small (e.g., ≤ 10), estimate a suspect set K (OSD + flip-history + ETS library).
3. **PP:** solve the restricted residual and apply only if small-weight.

$$\mathbf{s}_X = (H_Z)_K(\mathbf{x})_K \oplus (H_Z)_{\overline{K}}(\hat{\mathbf{x}})_{\overline{K}}$$

Performance

- **Code:** girth-8, (3,12)-regular $[[9216, 4612, \leq 48]]$.
- **Decoding:** joint BP + PP[a] reaches FER 10^{-8} at $p = 4\%$.
- **Benchmark:** BP aligns with DE (cycle-free, random non-orthogonal (3,12) code).



[a] github.com/kasaikenta/joint_BP_plus_PP

Conclusion

- Active-only orthogonality avoids the distance penalty.
- APMs control commutativity and short cycles.
- Girth-8 $(3, 12)$-regular $[[9216, 4612, \leq 48]]$ with strong BP performance.