Breaking the Orthogonality Barrier in Quantum LDPC Codes

2026 年 1 月 20 日

目次

1 概要

古典的な低密度パリティ検査（LDPC）符号は、現代の通信およびストレージシステムの基盤を形成する、広く普及し確立された技術である。この古典的な設定において、正則な次数分布を維持しつつタナーグラフのガース（girth）を大きくすることが、良好な信念伝搬（BP）復号性能と大きな最小距離の両立につながることはよく知られている。しかし、量子設定においては、量子 LDPC 符号がそのパリティ検査行列間に付加的な直交性制約を満たさなければならないため、この原理を直接適用することはできない。直交性と正則性の両方を単純な手法で強制すると、通常はガースが減少し、最小距離が構造的に上界（アッパーバウンド）に制限されてしまう。

本研究では、正則な検査行列構造を維持しつつ、交換性が制御された置換行列を用い、かつ構成

における必要な部分にのみ直交性制約を限定することで、この制限を克服する。この設計は、直交性、正則性、ガース、および最小距離の間の従来のトレードオフを打破し、大きなガースを持ち、かつ従来の距離上界に縛られない量子 LDPC 符号の構成を可能にする。具体的な実証として、ガース 8、(3,12) 正則な $[[9216, 4612, \leq 48]]$ 量子 LDPC 符号を構成した。この符号は、BP 復号と低計算量の後処理アルゴリズムを組み合わせることで、誤り確率 4% の脱分極チャネルにおいて、10^{-8} という極めて低いフレーム誤り率（FER）を達成することを示す。

2 はじめに

古典的な低密度パリティ検査（LDPC）符号は、現代の通信およびストレージシステムにおいて広く展開されている確立された技術であり、信念伝搬（BP）復号によって通信路容量を達成できる。その性能はタナーグラフの次数分布に強く依存する。正則符号は良好な性能を示し、慎重に設計された非正則分布は BP 性能をさらに向上させることができるが、不用意な非正則化は性能を劣化させる。変数ノードの次数が 3 以上のランダム LDPC 符号は、ブロック長に対して線形に増大する最小距離を持つため、古典 LDPC の研究では最小距離自体の増大には焦点が当てられてこなかった。さらに、BP 復号はトラッピングセットと呼ばれるタナーグラフ内の小さな構造に捕らわれることがあり、これが復号失敗の原因となる。有害なトラッピングセットを抑制するには、通常、大きなガース（girth：グラフ内の最小閉路長）が必要とされる。

希薄グラフ量子誤り訂正符号（QLDPC 符号）は 2004 年に提案され、反復復号の振る舞いや縮退の役割が議論されてきた。正の符号率と距離 $\Theta(\sqrt{n})$ を持つ符号族も知られている。クロネッカー和および積に基づく構成、一般化バイシクル（GB）符号の距離下界、有限長評価、および復号プロトコルが報告されており、CSS 型 QLDPC 符号の理論的理解が進んでいる。しかし、CSS パリティ検査行列 H_X と H_Z の間の直交性条件、すなわち $H_X H_Z^T = 0$ は古典符号には存在しない制約である。直交性と正則性の両方を単純な手法で強制しようとすると、通常はガースが減少し、構造的な距離の上界が誘発される。

表面符号やハイパーグラフ積（HGP）符号は幾何学的構造や積構造に依存しているため、古典 LDPC 符号で開発された設計原理とは異なる原理に従っている。その結果、古典的な次数分布やガース設計技術を直接適用することは容易ではない。本研究の目的は、古典 LDPC のパリティ検査構造を維持しつつ、それらを CSS 検査行列として直接利用可能にする構成原理を提供することである。具体的には、大きなガースと 3 以上の変数次数を持ち、最小距離が自明な上界に制限されない正則 LDPC 符号を目指す。

先行研究では、正則タナーグラフの次数分布を明示的に制御できる巡回パリティ検査行列が探索されてきた。代表的な構成には、萩原・今井符号やバイシクル構成がある。しかし、これらの構成には既知の限界がある。古典符号であっても、プロトグラフの一段階リフティング（巡回置換行列（CPM）によるリフティング）は、プロトグラフの構造に起因してガースに固定の上界を課すことがある。一段階リフティングが最小距離とガースに固定の制限を課すこと、および二段階リフティングがそれらを改善できることが指摘されている。CSS 符号の場合、パリティ検査行列 H_X

と H_Z は準巡回（QC）であり、タナーグラフのガースは $g = \min\{g(H_X), g(H_Z)\}$ を満たすため、各行列に QC ガースの上界が適用される。一般的な量子 CPM-LDPC 符号では、ガースは列重み 2 で 12 以下、列重み 3 以上で 6 以下に制限される。代数的置換行列（APM）LDPC 符号を用いることで、これらの上界を打破することが可能である。

CSS 型 LDPC の構成において、パリティ検査行列 H_X または H_Z から行を削除しても交換条件 $H_X H_Z^T = 0$ は維持されるが、スタビライザー制約が弱まり、符号空間が拡大する可能性がある。行削除は符号率の調整や行・列重みの制御に用いられるが、一般に距離の保持は保証されない。特に行削除は、低重みのベクトルが $C_X \setminus C_Z^{\perp}$ または $C_Z \setminus C_X^{\perp}$ に入ることを許し、新たな低重みの論理演算子を生成して最小距離を減少させることがある。CSS 符号において、$C_X = \ker(H_X)$ および $C_Z = \ker(H_Z)$ とすると、$C_X \setminus C_Z^{\perp}$ または $C_Z \setminus C_X^{\perp}$ 内の低重みベクトルは非自明な論理演算子となる。その結果、削除された検査行が論理演算子となり、距離を行重みで上界付ける可能性がある。

本研究では、まず、行削除が CSS 符号の最小距離を劣化させる一般的なメカニズムについて議論する。次に、一般化萩原・今井符号に対して、行削除による距離劣化を避けるために部分行列の交換性を制御する符号設計手法を確立する。具体的には、APM-LDPC 符号の代数的構造を用いて、アクティブな部分のみで直交性を保証し、交換が必要な行ペアの集合を導入して交換条件を局所化する。さらに、相互作用行列の非ゼロパターンを制御することで、削除された行が低重みの論理演算子として出現しないようにし、APM 合成規則に基づく逐次構成アルゴリズムを提示する。具体的な実証として、(3,12) 正則な $[[9216, 4612, \leq 48]]$ 量子 LDPC 符号を構成し、低計算量の後処理アルゴリズムを組み合わせた BP 復号の下で、誤り率 4 の脱分極チャネルにおいて 10^{-8} という低いフレーム誤り率（FER）を達成することを示す。また、交換制御の有無による構成を比較し、低重み論理演算子の抑制を実証する。

2 問題設定：検査行の削除によって誘発される低重み論理演算子

本論文で用いる従来の CSS-LDPC 符号の構成をまとめる。互いに直交な 2 つの母正方 (巡回) 行列 $\hat{H}_X, \hat{H}_Z$ を構成する。これらの母行列により定義される CSS 符号は一般的にレートが 0 であるため、内部の行を削除し、残った行を H_X, H_Z をアクティブ行列として用いることでレートを調整する。つまり、

$$\hat{H}_X = \begin{bmatrix} H_X \\ \tilde{H}_X \end{bmatrix}, \hat{H}_Z = \begin{bmatrix} H_Z \\ \tilde{H}_Z \end{bmatrix}$$

であり、H_X, H_Z がアクティブ行列、$\tilde{H}_X, \tilde{H}_Z$ が潜在行列である。

しかしながら、この構成では、母行列の直交性は潜在行に制約を課し、最小距離を劣化させる。最小距離は

$$d_Z := \min(wt\boldsymbol{z} : \boldsymbol{z} \in C_X \backslash C_Z^{\perp}), \quad d_X := \min(wt\boldsymbol{x} : \boldsymbol{x} \in C_Z \backslash C_X^{\perp})$$

により $d_{\min} = \min(d_X, d_Z)$ で定義される。母行列の直交性

$$\hat{H}_X(\hat{H}_Z)^\top = 0$$

は、アクティブ行列 H_X, H_Z 間の直交性、つまり $H_X H_Z^\top = 0$ だけでなく、以下も強制する。

$$H_X(\tilde{H}_Z)^\top = 0, \quad H_Z(\tilde{H}_X)^\top = 0$$

つまり、$\mathrm{Row}(\tilde{H}_X) \in C_Z$ および $\mathrm{Row}(\tilde{H}_Z) \in C_X$ である。したがって $\tilde{H}_X$ の各行 $\boldsymbol{x}$ は $\boldsymbol{x} \in C_Z$ であり、$\tilde{H}_Z$ の各行 $\boldsymbol{z}$ は $\boldsymbol{z} \in C_X$ である。一般的には $\boldsymbol{x}$ は $C_X^\top$ に属する必要はなく、$\boldsymbol{z}$ も $C_Z^\perp$ に属する必要はなく、このときこれらは論理演算子となる。最小行重み (我々の構成では L) が d_X および d_Z の上界となる。

本研究では、母行列から行を削除することでアクティブ行列 H_X, H_Z を得るが、潜在行列の低重み行が、H_X, H_Z と直交しないようにこれらを設計する。つまり、低重みの $\boldsymbol{x} \in \mathrm{Row}(\tilde{H}_X)$ に対し $H_Z \boldsymbol{x}^\top \neq 0$ を、$\boldsymbol{z} \in \mathrm{Row}(\tilde{H}_Z)$ に対し $H_X \boldsymbol{z}^\top \neq 0$ を強制し、つまり $\mathrm{Row}(\tilde{H}_X) \not\subset C_Z$ および $\mathrm{Row}(\tilde{H}_Z) \not\subset C_X$ を強制する。同じ議論は、個々の潜在行だけでなく、低重みの線形結合にも適用される。

したがって、潜在ベースの X, Z 距離の上階を以下で定義する。

$$\begin{aligned}
d_X^{\mathrm{lat}} &:= \min\left\{\mathrm{wt}(\boldsymbol{x}) : \boldsymbol{x} \in \mathrm{Row}(\tilde{H}_X) \cap C_Z \backslash C_X^\perp\right\} \\
&= \min\left\{\mathrm{wt}(\boldsymbol{x}) : \boldsymbol{x} \in C_Z, \boldsymbol{x} = (\tilde{H}_X)^\top \boldsymbol{u} \text{ for some } \boldsymbol{u}, \boldsymbol{x} \notin C_X^\top\right\} \\
d_Z^{\mathrm{lat}} &:= \min\left\{\mathrm{wt}(\boldsymbol{z}) : \boldsymbol{z} \in \mathrm{Row}(\tilde{H}_Z) \cap C_X \backslash C_Z^\perp\right\} \\
&= \min\left\{\mathrm{wt}(\boldsymbol{z}) : \boldsymbol{z} \in C_X, \boldsymbol{z} = (\tilde{H}_Z)^\top \boldsymbol{u} \text{ for some } \boldsymbol{u}, \boldsymbol{z} \notin C_Z^\top\right\}
\end{aligned}$$

提案された設計は、これらの境界を可能な限り大きくすることを目的としている。[26] では、符号語に対応する二進部分行列を非二進体へ持ち上げることで、それらがもはや符号語を表さなくなるようにしている。これは非二進持ち上げによる潜在ベース境界の拡大と見なすことができる。

3 行列の設計方法

この章では、上記の問題設定に基づき、

$$H_X H_Z^\top = 0, \quad H_X(\tilde{H}_Z)^\top \neq 0, \quad H_Z(\tilde{H}_X)^\top \neq 0$$

かつ $d_X^{(\mathrm{lat})}, d_Z^{(\mathrm{lat})}$ が大きい、を満たすような潜在行列 $\tilde{H}_X, \tilde{H}_Z$ を構成することを目指す。我々は一般化した萩原-今井符号、つまり巡回行列構造の母行列のペアとを定義し、アクティブ行列 H_X, H_Z 間の直交性 $H_X H_Z^\top = 0$

列重み J、行重み L プロトグラフ LDPC 符号はサイズ P の $J \times L$ 置換行列からなるパリティ検査行列により定義される。置換 $f : [P] \to [P]$ に対し、対応する $P \times P$ の置換行列 $F = P(f)$ は

$F_{x,y} = 1 \iff f(x) = f(y)$ で定義される。各行と列は丁度 1 つの 1 を持ち、したがってブロック構造がコンパクトであるため母行列は疎である。

我々は一般化された萩原・今井符号を、萩原・今井準巡回 CSS 符号のプロトグラフ一般化として紹介する。サイズ P の置換行列 $F_i, G_i (i \in [L_2])$ に対し、サイズ $(L_2P) \times (LP)$ の母行列 $\hat{H}_X, \hat{H}_Z$ を以下で定義する。

$$(\hat{H}_X)_{i,j} = F_{j-i}, \quad (\hat{H}_X)_{i,L_2+j} = G_{j-i},$$
$$(\hat{H}_Z)_{i,j} = G_{i-j}^\top, \quad (\hat{H}_Z)_{i,L_2+j} = F_{i-j}^\top,$$

すべての添え字は $\mathrm{mod} L_2$ で計算される。全体を通して、$[L/2]$ 内のインデックスは $\mathrm{mod} L/2$ で計算され、つまり $[L/2]$ を $\mathbb{Z}_{L/2}$ と同一視する。直交性の十分条件は以下で与えられる。アクティブ行列 H_X, H_Z は上の J ブロック行から構成される。従来の設計は、H_X, H_Z と $\hat{H}_X, \hat{H}_Z$ がいずれも直交するように F_i, G_j に可換性を課した。我々の関心は、母行列の直交性を課さずにアクティブ行列の直交性 $H_X H_Z^\top = 0$ を満たすことである。

$\hat{H}_X$ の各ブロック行は、左側は $(F_0, F_1, \ldots, F_{L/2-1})$ の巡回シフトであり、右側は $(G_0, G_1, \ldots, G_{L/2-1})$ の巡回シフトである。したがってブロックは差分 $(j-i)$ のみに依存し、母行列の席も差分のみに依存する。任意の $i, k \in [L_2]$ に対して、(i,k) ブロックは

$$(\hat{H}_X(\hat{H}_Z)^\top)_{i,k} = \sum_{u=0}^{L_2-1} (F_u G_{k-u} + G_{k-u} F_u) =: \Psi_r$$

で与えられ、これは $r = (k-i) \mod L_2$ のみに依存する。$r \in [L/2]$ に対し、すべての $u \in [L/2]$ に対し F_u と G_{r-u} が可換ならば、$\Psi_r = 0$ である。

3.1 アクティブ直交性の十分条件

我々は、$H_X H_Z \top = 0$ の十分証券の便利な形を再び導く。

$$\Delta := \{(k-i) \mod L/2 \mid 0 \le i, k \le J-1\} \subseteq [L/2]$$

を定義する。以下の定理はこれらの差分で制限される可換性がアクティブ直交性をどのように保証するかを明らかにする。

定理 3.1. もし F_u と G_{r-u} がすべての $r \in \Delta, u \in [L/2]$ に対し可換ならば、$H_X H_Z^\top = 0$ である。

Proof. すべての $i, k \in [J]$ に対し、$r = (k-i) \mod L/2 \in \Delta$ である。仮定より $\Psi_r = 0$ なので、すべての $i, k \in [J]$ に対し $(\hat{H}_X(\hat{H}_Z)^\top)_{i,k} = \Psi_{(k-i) \mod L/2} = 0$ であり、$H_X H_Z^\top = 0$ である。 □

3.2 潜在部の非直交性の必要条件

可換性が必要な (F_i, G_j) のインデックスペアを以下で定義する。

$$\Gamma := \bigcup_{r\in\Delta} \Gamma_r, \quad \Gamma_r := \{(i,j) \mid (i,j) = (u, r-u), u \in [L/2]\}$$

ここで、添え字は $\bmod L/2$ で計算する。ここで、Γ_r は Ψ_r に寄与するインデックスの集合であり、$r \neq s$ に対し $\Gamma_r \hat{\Gamma}_s = \emptyset$ である。

もし $J \geq L/2$ であればレートは 0 なので、$J < L/2$ を仮定する。まず、基本的で実現可能な制約を述べる：十分なブロックなしでは、潜在部の非直交性は強制できない。

定理 3.2. アクティブ部の直交性 $H_X H_Z^\top = 0$ を仮定する、一般できなアクティブ部の選択 (上 J ブロック行) に対し、$H_X(\tilde{H}_Z)^\top \neq 0$ および $H_Z(\tilde{H}_X)^\top \neq 0$ を満たすために、$L \geq 4J$ が必要である。

Proof. $L < 4J$ を仮定する。このアクティブ部の選択に対して、$\Delta = [L/2]$ である。アクティブ部の直交性 $H_X H_Z^\top = 0$ はすべての $r \in \Delta$ に対して $\Psi_r = 0$ を意味し、したがってすべての $r \in [L/2]$ に対して $\Psi_r = 0$ を意味する。ゆえに、$\hat{H}_X(\hat{H}_Z)^\top$ のすべてのブロックが消滅し、特にアクティブ部と潜在部の行の混合ブロックについて、$H_X(\tilde{H}_Z)^\top = 0$ と $H_Z(\tilde{H}_X)^\top = 0$ が成り立ち、前提と矛盾する。 □

次に、潜在部の非直交性に対する最小の代数的障害を分離する。

定理 3.3. $H_X(\tilde{H}_Z)^\top \neq 0, \quad H_Z(\tilde{H}_X)^\top \neq 0$ を満たすために、$\Psi_r \neq 0$ が成り立つ $r \in [L/2]\backslash\Delta$ が存在する必要がある。

Proof. すべての $r \in [L/2]\backslash\Delta$ に対し $\Psi_r = 0$ を仮定する。任意の $i \in [L/2]\backslash[J]$ と $k \in [J]$ に対し、$r = (k-i) \mod L/2$ が Δ に含まれない。$\Psi_r = 0$ の仮定により、このようなすべての i, k に対し、$(\tilde{H}_X(\tilde{H}_Z)^\top)_{i,k} = \Psi_{(k-i) \bmod L/2} = 0$ である。したがって、$H_X(\tilde{H}_Z)^\top = 0$ であり、同様に $H_Z(\tilde{H}_X)^\top = 0$ であり、矛盾する。すべてのペア $(i,j) \in [L/2]^2\backslash\Delta$ が可換ならば、各部分 $F_u G_{r-u} + G_{r-u} F_u$ は $\mathbb{F}_2$ 上で消滅し、すべての $r \notin \Delta$ に対して $\Psi_r = 0$ である。 □

3.3 ガースの上界

最後に、必要なすべての差分において可換性が成立する場合に適用される構造的制約を想起する。

定理 3.4. L を偶数とし、$2 \leq J \leq L/2$ を仮定する。もしすべての $r \in \Delta$ と $u \in [L/2]$ に対し F_u と G_{r-u} が可換ならば、H_X, H_Z のターナーグラフはそれぞれ 8-サイクルを有する。

Proof. $J \geq 2$ より、$0,1 \in \Delta$ である。また $L/2 \geq 2$ なので、$[L/2]$ の中に $i \neq i'$ が存在する。$r = 0, s = 1$ および $j = r - i, j' = s - i$(インデックスは $\mathrm{mod} L/2$) とする。定義より、$(i,j),(i,j') \in \Gamma_r \cup \Gamma_s$ であり、同様に $(i',j),(i',j') \in \Gamma_r \cup \Gamma_s$ である。対応する F, G の可換性の仮定より、2 つの F 列と 2 つの G 列から構成される 8 サイクル語は以下である。

$$W = F_i G_j^{-1} G_{j'} F_i^{-1} F_{i'} G_{j'}^{-1} G_j F_{i'}^{-1}$$

可換性を用いて並び替えると、$W = (F_i F_i^{-1})(F_{i'} F_{i'}^{-1})(G_j G_j^{-1})(G_{j'} G_{j'}^{-1}) = I$ となり、H_X, H_Z のタナーグラフには必ず 8-サイクルが存在する。

□

4　行列構成の方法

以前の章で導いた可換性条件とアクティブ部の直交性に基づき、短サイクルを回避しつつこれらの制約を満たす置換ブロックを構築する具体的な逐次手順を提示する。与えられた $(L/2, P, J)$ に対して、以下を同時に満たす $\{F_i\}, \{G_i\}$ を構築する。

1. f_i, G_j は $(i,j) \in \Delta$ に対して可換である
2. 少なくとも一つの $(i,j) \in [L/2]^2 \backslash \Delta$ に対して非可換である
3. アクティブ行列 H_X, H_Z 内の短いサイクルを避ける (長さ 8 以下の UTCBC 以外のサイクル)

循環置換行列（CPM）から準循環 LDPC ブロックを構築する枠組みは、Fossorier によって体系化された。我々はアフィン置換行列（APM）を採用する：APM-LDPC の枠組みは CPM を拡張し、その代数的形態により合同条件を通じて可換性の制御が容易となる。古典的な設定において、吉田と笠井は線形置換多項式（APM ベース）符号がプロトグラフ LDPC 符号に匹敵する性能を達成すると報告した。一方、ワンステップ CPM リフティングとは異なり、APM ベースの構成法については固定ガース上限が報告されていない。長さ及びガースを拡張するために APM-LDPC 符号を組み合わせる手法も提案されている。群論的観点から、整数体上の APM はアフィン群 $\mathrm{AGL}(1, \mathbb{Z}_P) = \mathbb{Z}_P \rtimes \mathbb{Z}_P^\times$ を形成する。これは単位群による平行移動の半直積であり、可換性は線形部分と平行移動部分の相互作用によって規定される。

$\mathbb{Z}_P$ 上のアフィン置換を考える。

$$f(x) = ax + b, \quad a \in \mathbb{Z}_P^\times, b \in \mathbb{Z}_P$$

$f_i(x) = a_i x + b_i$ および $g_j(x) = c_j x + d_j$ とし、対応する置換行列を $F_i := P(f_i), G_j := P(g_j)$ で表す。

この表現の下で、AP の可換性は二次合同式によって検証される：

$$f_i g_j = g_j f_i \iff d_j(a_i - 1) - b_i(c_j - 1) \equiv 0 \mod P$$

この条件は a_i, c_j と b_i, d_j の積を含む。したがって交換表は合同式系として表現可能であり、特に a_i, c_j を先に選択した場合、交換制約は b_i, d_j における線形合同式に還元され、一貫性のある探索を可能とする。

我々は、交換表と短サイクル条件の両方を満たす候補を順次選択し、候補が失敗した場合にはバックトラッキングを用いる。試行回数は直近の成功率に基づいて動的に調整される。各候補生成器を多腕バンディットの腕として解釈し、それに応じて試行を割り当てる。

短サイクル検出は、複合写像 Σ の固定点をブロックサイクルパターンに沿って調べることに帰着する。AP の合成関数は再び AP であり、$\Sigma(x) = Ax + B$ となるため、

$$\Sigma(x) = x \iff \gcd(A - 1, P) \mid B$$

はタナーグラフを列挙せずにテストを提供する。

5 復号方式

6 結果

第 3 節の一般理論と第 4 節の逐次構築法を、構築可能な最小ケースである $J = 3, L = 12, P = 768$ に対して具体化する。まず明示的な Δ, Γ, Ψ_r を与え、アクティブ行列 H_X, H_Z のアクティブ直交条件を明確化した後、交換表と APM パラメータを設計し、最後に距離境界と FER を評価する。