$\underline{\boldsymbol{f}}, \underline{\boldsymbol{g}}$ の条件を満たす解空間の特定

黒澤雅治

2025/12/21

目次

1　ブロックサイクルが閉かどうかの判定

サイクルの関数が $f(x) = ax + b$ であるとする。このとき、サイクルが閉であることはある $x \in [P]$ について $ax + b = x$ が成り立つことである。よって、$(a-1)x + b = 0$ を満たす x が存在するならブロックサイクルは閉である。この条件は、

$$b \equiv 0 \pmod{\gcd(a-1, P)}$$

と書き換えられる。つまり、$a = 1$ のとき、$b = 0$ ならばすべての x が解である。$a \neq 1$ のとき、b が $\gcd(a-1, P)$ で割り切れる時のみ解が存在、すなわちサイクルは閉である。

2　笠井先生の論文 Breaking the Orthogonality Barrier in Quantum LDPC Codes について

2.1　従来の行列の構成方法

定義 2.1. $\hat{H}_X, \hat{H}_Z$ を母行列、H_X, H_Z をアクティブ行列、$\tilde{H}_X, \tilde{H}_Z$ を潜在部と呼ぶ。以下が成り立つ。

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

$\hat{H}_X, \hat{H}_Z$ は 2 つの直交する正方 (ブロック巡回) 母行列である。これらにより構成される母行列のレートは 0 である。よってレートを調整するのに内部行を消去する。

ここで、母行列の直交性は潜在部の行に強い制約を課し、最小距離を劣化させる。

定義 2.2. 最小距離を以下で定義する。

$$d_Z := \min\{\mathrm{wt}(z) : z \in C_X \backslash C_Z^\top\}, \qquad d_X := \min\{\mathrm{wt}(x) : x \in C_Z \backslash C_X^\top\}$$

定理 2.3. 母行列の直交性 $\hat{H}_X(\hat{H}_Z)^\top = 0$ は、アクティブ部の直交性 $H_X(H_Z)^\top = 0$ だけでなく、

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

も強要する。

これは、$\mathrm{Row}(\hat{H}_X) \subset C_Z$ および $\mathrm{Row}(\hat{H}_Z) \subset C_X$ であることを暗示している。したがって、$\tilde{H}_X$ の各行 $\boldsymbol{x}$ について $\boldsymbol{x} \in C_Z$、$\tilde{H}_Z$ の各行 $\boldsymbol{z}$ について $\boldsymbol{z} \in C_X$ が成り立つ。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。

2.2 新しい行列の構成方法

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。

定義 2.4. 潜在ベースの X, Z 距離の上界を以下で定義する。

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

まとめると、

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

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 $\tilde{H}_X, \tilde{H}_Z$ を構成したい。一般化した萩原・今井符号、つまりブロック巡回構造の母行列のペアを定義し、アクティブ部の直交性 $H_X (H_Z)^\top = 0$ のみを課す。行重み J、列重み L のプロトグラフ LDPC 符号はサイズ P の $J \times L$ の置換行列により定義される。

定義 2.5. サイズ $LP/2 \times LP$ の母行列を以下で定義する。

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

アクティブ行列は母行列の上 J ブロック行を取ることで得られる。

潜在部がアクティブ部と可換でないようにすることで、低重みの潜在部の組は自動的に論理演算子にならない。

ブロック巡回構造は $H_X (H_Z)^\top$ が差分のみに依存するようにし、結果である Interaction MatrixΨ_r により、可換性制約を小さな差分集合に位置づけられる。

$\hat{H}_X$ 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、母行列の積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。

2.3 アクティブ部の直交性の十分条件

定義 2.6.

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

定理 2.7. 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。

2.4 潜在部の非直交性の必要条件

定義 2.8. 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。

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

$L \ge 4J$ および $\Psi_r \neq 0$ を満たすような $r \in [L/2] \backslash \Delta$ が存在することが、潜在部の非直交性の必要条件である。

2.5 ガーズの上界

長さ 8 のサイクルは必ず存在する。

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

は UTCBC である。他にも UTCBC の形があるかもしれない。

2.6 行列構築の方法

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。

A' f_i, G_j は $(i,j) \in \Delta$ に対して可換である
B' 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
C' 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)

可換表テーブル：

3 この論文での条件を満たす F_i, G_i の構成

目標は、f_0 と g_3、f_1 と g_2 が非可換であり、他がすべて可換であるような F_i, G_i を見つけることである。(他が厳密に可換である必要があるのかはわからないが、今は条件から解空間を特定す

	G_0	G_1	G_2	G_3	G_4	G_5
F_0	1	1	1	0	1	1
F_1	1	1	0	1	1	1
F_2	1	1	1	1	1	1
F_3	1	1	1	1	1	1
F_4	1	1	1	1	1	1
F_5	1	1	1	1	1	1

ることに集中する。)

これまでと同様、$f_i(x) = a_{f_i}x + b_{f_i}$ のようにあらわす。

3.1 条件 A'

$$(a_{f_i} - 1)b_{g_j} - (a_{g_j} - 1)b_{f_i} \equiv 0 \pmod{P} \quad \text{for } (i,j) \in [L/2]^2 \backslash \{(0,3),(1,2)\}$$

3.2 条件 B'

$$(a_{f_i} - 1)b_{g_j} - (a_{g_j} - 1)b_{f_i} \not\equiv 0 \pmod{P} \quad \text{for } (i,j) = (0,3),(1,2)$$

3.3 条件 C'

条件 C' を考える前に、今回の $\hat{H}_X, \hat{H}_Z$ における UTCBC を特定する。$\hat{H}_X, \hat{H}_Z$ は以下である。

$$\hat{H}_X = \left(\begin{array}{cccccc|cccccc} F_0 & F_1 & F_2 & F_3 & F_4 & F_5 & G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ F_5 & F_0 & F_1 & F_2 & F_3 & F_4 & G_5 & G_0 & G_1 & G_2 & G_3 & G_4 \\ F_4 & F_5 & F_0 & F_1 & F_2 & F_3 & G_4 & G_5 & G_0 & G_1 & G_2 & G_3 \\ \hline F_3 & F_4 & F_5 & F_0 & F_1 & F_2 & G_3 & G_4 & G_5 & G_0 & G_1 & G_2 \\ F_2 & F_3 & F_4 & F_5 & F_0 & F_1 & G_2 & G_3 & G_4 & G_5 & G_0 & G_1 \\ F_1 & F_2 & F_3 & F_4 & F_5 & F_0 & G_1 & G_2 & G_3 & G_4 & G_5 & G_0 \end{array}\right).$$

$$\hat{H}_Z = \left(\begin{array}{cccccc|cccccc} G'_0 & G'_5 & G'_4 & G'_3 & G'_2 & G'_1 & F'_0 & F'_5 & F'_4 & F'_3 & F'_2 & F'_1 \\ G'_1 & G'_0 & G'_5 & G'_4 & G'_3 & G'_2 & F'_1 & F'_0 & F'_5 & F'_4 & F'_3 & F'_2 \\ G'_2 & G'_1 & G'_0 & G'_5 & G'_4 & G'_3 & F'_2 & F'_1 & F'_0 & F'_5 & F'_4 & F'_3 \\ \hline G'_3 & G'_2 & G'_1 & G'_0 & G'_5 & G'_4 & F'_3 & F'_2 & F'_1 & F'_0 & F'_5 & F'_4 \\ G'_4 & G'_3 & G'_2 & G'_1 & G'_0 & G'_5 & F'_4 & F'_3 & F'_2 & F'_1 & F'_0 & F'_5 \\ G'_5 & G'_4 & G'_3 & G'_2 & G'_1 & G'_0 & F'_5 & F'_4 & F'_3 & F'_2 & F'_1 & F'_0 \end{array}\right).$$

3.3.1 サイクルの定義について

[1] によると、”In this construction, each step in the path moves either to a different row or to a different column, but not both simultaneously. That is, consecutive blocks must differ in exactly one of their row or column indices” とあり、サイクルの隣り合う要素は行か列いずれか 1 つが異ならなければならない。よって、行インデックスシーケンス、列インデックスシーケンスともに同じ要素が連続してはいけない、という前提とする。(要確認)

サイクルは最初の位置から、1 つおきに位置を指定することで、サイクルを一意に特定できる。

3.3.2 検査すべきサイクルの個数

■長さ 4 のサイクル 長さ 4 のサイクルは、2 つの位置を与えれば、一意に特定される。2 つの位置を $[r_1, c_1], [r_2, c_2]$ とすると、サイクルは

$$[r_1, c_1] \to [r_1, c_2] \to [r_2, c_2] \to [r_2, c_1] \to [r_1, c_1]$$

である。この時、位置 $[r_1, c_2], [r_2, c_1]$ により指定されるサイクルは、

$$[r_1, c_2] \to [r_1, c_1] \to [r_2, c_1] \to [r_2, c_2] \to [r_1, c_2]$$

である。このサイクルはサイクル 3.3.2 とは異なるが、辿る順番が逆であるだけなので、3.3.2 が閉であることと 3.3.2 が閉であることは同値である。

以上を踏まえ、検査すべきサイクルの個数を考える。まず、2 つの位置の選び方は、列、行ともに異なるものを選ぶ必要があることを考えると、1 つ目が $L/2 \times L$ 通り、2 つ目は $(L/2-1) \times (L-1)$ 通りであり、全部で $L/2 \times (L/2-1) \times L \times (L-1)$ 通りである。長さ 4 のサイクルについて、構成する 4 つの位置が決まれば、その辿り方は一意に定まるので、同値な条件を導く位置選択は 4 つずつ存在する。よって、検査すべきサイクルの個数は

$$L/2 \times (L/2-1) \times L \times (L-1)/4$$

個である。

■長さ 6 のサイクル 長さ 6 のサイクルは、長さ 3 の行インデックスシーケンス及び長さ 3 の列インデックスシーケンスを与えれば、一意に特定される。**??**より、行インデックスシーケンスは $(L/2-1)^3 - (L/2-1)$ 通り、列インデックスシーケンスは $(L-1)^3 - (L-1)$ 通りある。ここで、同一のサイクルを形成する行インデックスシーケンスと列インデックスシーケンスの組み合わせは、3 つずつ存在する。($\mathcal{C}_{[0,1,2],[0,1,2],X}$ と、$\mathcal{C}_{[1,2,0],[1,2,0],X}$、$\mathcal{C}_{[2,1,0],[2,1,0],X}$ は同一) よって、考えるべきサイクル数は

$$((L/2-1)^3 - (L/2-1)) \times ((L-1)^3 - (L-1))/3 \times 2$$

通りある。

$L = 12$ で考えると、

$$((L/2-1)^3 - (L/2-1)) \times ((L-1)^3 - (L-1))/3 \times 2 = 105600$$

通りとなる。

■長さ 8 のサイクル　長さ 8 のサイクルは、長さ 4 の行インデックスシーケンス及び長さ 4 の列インデックスシーケンスを与えれば、一意に特定される。同様に考えると**??**より、行インデックスシーケンスは $(L/2-1)^4 + (L/2-1)$ 通り、列インデックスシーケンスは $(L-1)^4 + (L-1)$ 通りある。ここで、同一のサイクルを形成する行インデックスシーケンスと列インデックスシーケンスの組み合わせは、4 つずつ存在する。($\mathcal{C}_{[0,1,2,3],[0,1,2,3],X}$ と、$\mathcal{C}_{[3,0,1,2],[3,0,1,2],X}$、$\mathcal{C}_{[2,3,0,1],[2,3,0,1],X}$、$\mathcal{C}_{[1,2,3,0],[1,2,3,0],X}$ は同一) よって、考えるべきサイクル数は

$$((L/2-1)^4 + (L/2-1)) \times ((L-1)^4 + (L-1))/4 \times 2 \text{ 通りある。}$$

$L = 12$ で考えると、

$$((L/2-1)^4 + (L/2-1)) \times ((L-1)^4 + (L-1))/2 = 4615380$$

通りとなる。

以上合わせると、検査すべきサイクルは $10368 + 105600 + 4615380 = 4731348$ 個である。

4　行列を用いた条件 A',B' の定式化

??節と同様に、条件 A' および B' を行列を用いて表現する。

$$\underline{\boldsymbol{a}} = [a_{f_0}, a_{f_1}, \ldots, a_{f_5}, a_{g_0}, a_{g_1}, \ldots, a_{g_5}]^\top, \qquad \underline{\boldsymbol{b}} = [b_{f_0}, b_{f_1}, \ldots, b_{f_5}, b_{g_0}, b_{g_1}, \ldots, b_{g_5}]^\top$$

とする。$\underline{\boldsymbol{a}}$ を定数として固定することで条件を満たす $\underline{\boldsymbol{b}}$ の解空間を求める。

行列 G' を以下の L, R を用いて $G' = [L \mid R]$ と定義する。

$$L_{(6i+j,k)} = \begin{cases} 1 - a_{g_i} & \text{if } k = i \\ 0 & \text{otherwise} \end{cases}$$

$$R_{(6i+j,k)} = \begin{cases} a_{f_j} - 1 & \text{if } k = j \\ 0 & \text{otherwise} \end{cases}$$

■条件 A'　G' から 3,8 行目 ($(i,j) = (0,3), (1,2)$ に対応する行) を除いたものを G'_a とすると、条件 A' は以下で表される。

$$G'_a \underline{\boldsymbol{b}} \equiv O \pmod{P}$$

■条件 B'　G' の 3,8 行目のみを取り出したものを G'_b とすると、条件 B' は、

$$G'_b \underline{\boldsymbol{b}} \not\equiv \underline{\boldsymbol{c}}'_b \pmod{P}$$

かつ $\underline{\boldsymbol{c}}'_b$ の要素がすべて非ゼロであることである。

■条件 C'　条件 C' は、4731348 個ものサイクルについて考える必要があるので、代表として合成関数が $f_C(x) = a_C x + b_C$ であるサイクルを考える。条件は、

$$b_C \not\equiv 0 \pmod{\gcd(a_C - 1, P)} \tag{1}$$

が成り立つことで、b_C は $\underline{\boldsymbol{b}}$ の線形結合として $b_C = c_C \underline{\boldsymbol{b}}$ で表せる。これを用いると、(1) は以下のように表せる。

$$\begin{aligned} & c_C \underline{\boldsymbol{b}} \not\equiv 0 \pmod{\gcd(a_C - 1, P)} \\ \iff & \frac{P}{\gcd(a_C - 1, P)} c_C \underline{\boldsymbol{b}} \not\equiv 0 \pmod{P} \end{aligned}$$

これをすべてのサイクルについて連結することで行列 G'_c を得ることで、条件 C' は

$$G'_c \underline{\boldsymbol{b}} \not\equiv \underline{\boldsymbol{c}}'_c \pmod{P}$$

かつ $\underline{\boldsymbol{c}}'_c$ の要素がすべて非ゼロであることである。

参考文献

[1] Kenta Kasai. Quantum error correction exploiting degeneracy to approach the hashing bound. *arXiv preprint arXiv:2506.15636*, 2025.