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

黒澤雅治

2025/12/21

目次

1 $\underline{f}, \underline{g}$ の満たすべき条件

A. 要請 1.1 を満たす。つまり、f_i と g_j は可換である。($L = 6$ のときはすべての i, j で可換)
B. ある $i \neq j$ について、f_i と f_j は可換でない。g についても同様。
C. UTCBC$\underline{\boldsymbol{u}}(k)$ for $k \in \{0, 1, 2\}$ 以外に長さ $2L$ 以下の閉ブロックサイクルを含まない。

要請 1.1. 以下の可換性条件が成り立つことを要請する。

$$g_{\ell-j}\, f_{k-\ell} = f_{k-\ell}\, g_{\ell-j} \quad (\text{for all } \ell \in [L/2],\ j, k \in [J])$$

ここで、f と g のインデックスは $L/2$ を法として解釈される。これは、以下の 3 つの記述のいずれとも等価である。

$f_{\ell-j}\, g_{k-\ell} = g_{k-\ell}\, f_{\ell-j} \quad (\text{for all } \ell \in [L/2],\ j, k \in [J])$,
すべての $\ell \in [L/2]$ および $j \in \{0, \pm 1, \ldots, \pm(J-1)\}$ に対して f_ℓ は $g_{-\ell+j}$ と可換である。
すべての $\ell \in [L/2]$ および $j \in \{0, \pm 1, \ldots, \pm(J-1)\}$ に対して g_ℓ は $f_{-\ell+j}$ と可換である。

2 可換性条件の分析

定義 2.1. 関数 f の係数を

$$f = a_f x + b_f$$

で表す。$(a_f, b_f \in [P], \quad \gcd(a_f, P) = 1)$

可換性条件は、すべての $x \in [P]$ に対して

$$\begin{aligned}
& f(g(x)) = g(f(x)) \\
\iff & a_f(a_g x + b_g) + b_f = a_g(a_f x + b_f) + b_g \\
\iff & a_f a_g x + a_f b_g + b_f = a_g a_f x + a_g b_f + b_g \\
\iff & a_f b_g + b_f = a_g b_f + b_g \\
\iff & (a_f - 1) b_g = (a_g - 1) b_f \qquad (1)
\end{aligned}$$

が成り立つことである。式 (1) を、b_g に関する方程式とみなす。この方程式は $(\text{mod } P)$ 上の 1 次合同方程式であることに注意する。$A = a_f - 1$ および $C = (a_g - 1) b_f$ と定義する。このとき、加法成分 b_g に関する 1 次合同方程式

$$A b_g \equiv C \pmod{P}$$

の解は以下の通りである。

ケース 1：$a_f \neq 1$ かつ $a_g \neq 1$ の場合

- $\gcd(A, P) = 1$ **のとき**
  解は法 P において一意に定まる。

$$b_g \equiv A^{-1}C \pmod{P}$$

- $\gcd(A, P) = d > 1$ **のとき**
  - $C \not\equiv 0 \pmod{d}$ ならば、**解なし**。
  - $C \equiv 0 \pmod{d}$ ならば、法 P において以下の d 個の解が存在する。

$$b_g \equiv x_0 + n\frac{P}{d} \pmod{P} \quad (n = 0, 1, \ldots, d-1)$$

    ただし、x_0 は法 P/d における合同方程式 $(A/d)x \equiv (C/d) \pmod{P/d}$ の一意な解である。

ケース 2：$a_f = 1$ かつ $a_g \neq 1$ の場合

- $C \equiv 0 \pmod{P}$ **のとき**
  任意の $b_g \in [P]$ が解となる（全解）。
- $C \not\equiv 0 \pmod{P}$ **のとき**
  解なし。

ケース 3：$a_g = 1$ の場合（$C = 0$）

- $a_f = 1$ **のとき**
  任意の $b_g \in [P]$ が解となる。
- $a_f \neq 1$ **のとき**
  - $\gcd(A, P) = 1$ ならば、$b_g \equiv 0 \pmod{P}$ のみ。
  - $\gcd(A, P) = d > 1$ ならば、以下の d 個の解が存在する。

$$b_g \equiv n\frac{P}{d} \pmod{P} \quad (n = 0, 1, \ldots, d-1)$$

詳細な導出は付録**??**を参照。

3　サイクル

サイクルは、L 列から偶数個の列を選び、開始行を指定することで一意に特定される。以下、$L = 6, J = 2$ に固定して考える。

3.1 同一とみなせるサイクル

■シフト ℓ のサイクルは、$\ell/2$ 個の列から構成される。よって、長さ $2L$ 以下のサイクルを考慮するには、$2, 4, \ldots, L$ 個の列からなるサイクルを考えればよい。

定義 3.1. 列シーケンス ℓ により構成され、開始位置が j 行目であるサイクルを $C_{\ell,j}$ で表し、サイクルは行列における (0 から始まる) インデックスの列として表現する。

$\ell = [a, b, c, d]$ について考える。このとき、

$$C_{\ell,0} = ([0,a],[0,b],[1,b],[1,c],[0,c],[0,d],[1,d],[1,a])$$
$$C_{\ell,1} = ([1,a],[1,b],[0,b],[0,c],[1,c],[1,d],[0,d],[0,a])$$

定義 3.2. 1 つの左シフトを $S(\cdot)$ で表現し、i 個左シフトする操作は $S^i(\cdot)$ で表す。右シフトは $S^{-1}(\cdot)$ で表す。

1 つシフトしたもの、2 つシフトしたものについて考える (それ以上のシフトはこれらの組み合わせで再現できる。) $\ell = [a, b, c, d]$ を 1 つシフトした $S(\ell) = [b, c, d, a]$ について、

$$C_{S(\ell),0} = ([0,b],[0,c],[1,c],[1,d],[0,d],[0,a],[1,a],[1,b]) = C_{\ell,1}$$
$$C_{S(\ell),1} = ([1,b],[1,c],[0,c],[0,d],[1,d],[1,a],[0,a],[0,b]) = C_{\ell,0}$$

$\ell = [a, b, c, d]$ を 2 つシフトした $S^2(\ell) = [c, d, a, b]$ について、

$$C_{S^2(\ell),0} = ([0,c],[0,d],[1,d],[1,a],[0,a],[0,b],[1,b],[1,c]) = C_{\ell,0}$$
$$C_{S^2(\ell),1} = ([1,c],[1,d],[0,d],[0,a],[1,a],[1,b],[0,b],[0,c]) = C_{\ell,1}$$

以上から、以下の定理が成り立つ。

定理 3.3.

$$C_{(\ell),0} = C_{(S(\ell)),1} = C_{S^2(\ell),0}$$
$$C_{(\ell),1} = C_{(S(\ell)),0} = C_{S^2(\ell),1}$$

よって、ある列シーケンス ℓ について、開始行が 0,1 行目である 2 つのサイクルを考えれば、列シーケンスをシフトしたものから構成されるサイクルすべてを網羅できる。

3.2 同じ列の選択

同じ列を連続で含むときを考える。この列に含まれる 2 つの関数を f, g とする。この時、サイクルの関数の中でこの列に関与する部分は、$f^{-1}gg^{-1}f = \mathrm{id}$ となる。よって、この部分はサイクルが閉であるかには影響しないことが分かる。これを利用することで、例えば $[1, 2, 3, 3, 4, 5]$ の列

選択の検査と $[1,2,4,5]$ の検査をまとめることができる。ここで、$[1,2,3,3,2,5]$ のような形の場合、同じ列を取り除いた結果、$[1,2,2,5]$ のように同じ列の連続が生じることもあることに注意する。また、今回サイクルを形成する列選択なので、$[1,2,3,4,3,1]$ のように先頭と最後の要素が等しいときも、$[2,3,4,3]$ と同一視することができる。

4 UTCBC

ここでサイクルの表記を定義する。

定義 4.1. 行列 $\hat{H}_X(\hat{H}_Z)$ における、列選択 ℓ、開始行 $0(1)$ 行目のサイクルを $\mathcal{C}_{X(Z),\ell,0(1)}$ で表す

論文では、開始行が 0 行目であるとき、列選択 $\ell = [0, 3+j\%3, 1, 3+(j-1)\%3, 2, 3+(j-2)\%3]$ からなるサイクルが UTCBC であることが示されている。確認として、開始行が 1 行目の場合についても考える。

$$\mathcal{C}_{X,\ell,1} = f_2 \to g_{j-1} \to g_j \to f_1 \to f_0 \to g_{j+1} \to g_{j-1} \to f_2 \to f_1 \to g_j \to g_{j+1} \to f_0 \to f_2$$

$$\begin{aligned} f_{\mathcal{C}_{X,\ell,1}}(x) &= (f_0^{-1} g_{j+1} g_j^{-1} f_1)(f_2^{-1} g_{j-1} g_{j+1}^{-1} f_0)(f_2 g_{j-1}^{-1} g_j f_1^{-1})(x) \\ &= (f_1 g_j^{-1} g_{j+1} f_0^{-1})(f_0 g_{j+1}^{-1} g_{j-1} f_2^{-1})(f_2 g_{j-1}^{-1} g_j f_1^{-1})(x) = x \end{aligned}$$

よって、開始行に関わらず、この列選択から構成されるサイクルは UTCBC である。

5 条件 C で検査する列シーケンスの個数

3.1 節に基づき、検査する必要のある列シーケンスの個数を考える。ここでは、隣り合う要素が異なり、かつ始点と終点が異なる（円環状に接続された）長さ L の列シーケンスを考える。使用できる列の総数を $k = 6$ とする。

定理 5.1. 円環状に並べた際に隣り合うものが異なる列シーケンスの総数は、

$$(k-1)^L + (-1)^L (k-1)$$

で表される。ただし、L は列シーケンスの長さ、k は列の選択肢の数。

証明は、付録付録 A を参照。まず、$L = 6$ の場合を考える。$k = 6, L = 6$ を代入すると、

$$5^6 + 5 = 15630$$

通りとなる。3.1 節を考慮し、シフトにより重なるものを同一視する。この際、周期的なパターン（$ababab$ のような周期 2 の列や、$abcabc$ のような周期 3 の列）は、シフトにより生成される同値類のサイズが小さくなるため、区別して数える必要がある。

- 周期 2 の列（例：$ababab$）：a, b の選び方は $6 \times 5 = 30$ 通り。これらはシフトにより 2 つの列と同一視されるため、検査対象は $30/2 = 15$ 通り。

- 周期 3 の列（例：$abcabc$）：a, b, c が条件を満たす選び方は $5^3 - 5 = 120$ 通り。これらはシフトにより 3 つの列と同一視されるため、検査対象は $120/3 = 40$ 通り。
- 周期 6 の列（上記のいずれでもないもの）：総数から周期的な列を除くと $15630 - 30 - 120 = 15480$ 通り。これらはシフトにより 6 つの列と同一視されるため、検査対象は $15480/6 = 2580$ 通り。

以上より、検査すべき列シーケンスは $15 + 40 + 2580 = 2635$ 通りとなる。

次に、$L = 4$ の場合を考える。同様に列シーケンス（始点指定あり）の総数は、

$$5^4 + 5 = 630$$

通りとなる。シフトによる同一視を考慮する。

- 周期 2 の列（例：$abab$）：$6 \times 5 = 30$ 通り。シフトにより 2 つの列と同一視されるため、$30/2 = 15$ 通り。
- 周期 4 の列（周期 2 でないもの）：$630 - 30 = 600$ 通り。シフトにより 4 つの列と同一視されるため、$600/4 = 150$ 通り。

以上より、検査すべき列シーケンスは $15 + 150 = 165$ 通りとなる。

最後に、$L = 2$ の場合を考える。列シーケンス（始点指定あり）の総数は、

$$5^2 + 5 = 30$$

通りとなる。周期 1 の列（aa）は条件を満たさないため存在しない。すべての列が周期 2（最小周期が長さと一致）であるため、単純に $L = 2$ で割ることができる。検査すべき列シーケンスは $30/2 = 15$ 通りとなる。

以上より、検査する列シーケンスの総数は $2635 + 165 + 15 = 2815$ 通り。

6 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、

$$b \equiv 0 \pmod{\gcd(a - 1, P)} \tag{2}$$

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。

7 $\hat{H}_X$ におけるチェックと $\hat{H}_Z$ におけるチェックの等価性

これは証明ができていない (そもそも等価かわからない) ので現時点では両方をチェック。

8　行列を用いた条件 A,B を満たす解空間の特定

条件 A,B を式に表すと以下である。

- 条件 A:

$$(a_{f_i}-1)b_{g_j}-(a_{g_j}-1)b_{f_i}\equiv 0 \pmod P \quad \text{for all } i,j\in[P]$$

- 条件 B:

$$(a_{f_i}-1)b_{f,j}-(a_{f,j}-1)b_{f_i}\not\equiv 0 \pmod P \quad \text{for any } i\neq j\in[P]$$
$$(a_{g,i}-1)b_{g_j}-(a_{g_j}-1)b_{g,i}\not\equiv 0 \pmod P \quad \text{for any } i\neq j\in[P]$$

定義 8.1. $\underline{\boldsymbol{a}}=[\underline{\boldsymbol{a}}_f,\underline{\boldsymbol{a}}_g]^\top=[a_{f_0},a_{f_1},a_{f_2},a_{g_0},a_{g_1},a_{g_2}]^\top, \underline{\boldsymbol{b}}=[\underline{\boldsymbol{b}}_f,\underline{\boldsymbol{b}}_g]^\top=[b_{f_0},b_{f_1},b_{f_2},b_{g_0},b_{g_1},b_{g_2}]^\top$ とする。

定義 8.2. 行列を以下のように定義する。

$$G_a=\begin{bmatrix}
1-a_{g_0} & 0 & 0 & a_{f_0}-1 & 0 & 0\\
1-a_{g_1} & 0 & 0 & 0 & a_{f_0}-1 & 0\\
1-a_{g_2} & 0 & 0 & 0 & 0 & a_{f_0}-1\\
0 & 1-a_{g_0} & 0 & a_{f_1}-1 & 0 & 0\\
0 & 1-a_{g_1} & 0 & 0 & a_{f_1}-1 & 0\\
0 & 1-a_{g_2} & 0 & 0 & 0 & a_{f_1}-1\\
0 & 0 & 1-a_{g_0} & a_{f_2}-1 & 0 & 0\\
0 & 0 & 1-a_{g_1} & 0 & a_{f_2}-1 & 0\\
0 & 0 & 1-a_{g_2} & 0 & 0 & a_{f_2}-1
\end{bmatrix}$$

$$G_{b,f}=\begin{bmatrix}
1-a_{f_1} & a_{f_0}-1 & 0 & 0 & 0 & 0\\
1-a_{f_2} & 0 & a_{f_0}-1 & 0 & 0 & 0\\
0 & 1-a_{f_2} & a_{f_1}-1 & 0 & 0 & 0
\end{bmatrix}$$

$$G_{b,g}=\begin{bmatrix}
0 & 0 & 0 & 1-a_{g_1} & a_{g_0}-1 & 0\\
0 & 0 & 0 & 1-a_{g_2} & 0 & a_{g_0}-1\\
0 & 0 & 0 & 0 & 1-a_{g_2} & a_{g_1}-1
\end{bmatrix}$$

これを用いると、条件 A は以下で表される。

$$G_a\underline{\boldsymbol{b}}\equiv O \pmod P \tag{3}$$

これを用いると、条件 B は以下で表される。

$$G_{b,f}\underline{\boldsymbol{b}}\not\equiv \underline{0} \pmod P \tag{4}$$
$$G_{b,g}\underline{\boldsymbol{b}}\not\equiv \underline{0} \pmod P \tag{5}$$

まずは、$\underline{\boldsymbol{a}}$ を定数として固定した状態で条件 a,b を満たす $\underline{\boldsymbol{b}}$ の解空間を特定することを考える。まずは簡単のため、$a_{f_i}\neq 0$、$a_{g,i}\neq 0$ として考える。式 (3) を解くと、基底 $\underline{\boldsymbol{v}}_0,\ldots,\underline{\boldsymbol{v}}_5$ 及係数

$\underline{\boldsymbol{c}} = [c_0, \ldots, c_5]^\top$ により、解空間として

$$\underline{\boldsymbol{b}} = \sum_{j=0}^{5} c_j \underline{\boldsymbol{v}}_j = V\underline{\boldsymbol{c}}$$

が求められる。ただし、$V = [\underline{\boldsymbol{v}}_0, \ldots, \underline{\boldsymbol{v}}_5^\top], c_i \in [P]$ である。

これにより、式 (4) と (5) は

$$\begin{aligned} & G_{b,f} V\underline{\boldsymbol{c}} \not\equiv \underline{0} \\ \iff & M_f \underline{\boldsymbol{c}} \not\equiv \underline{0} (M_f = G_{b,f} V) \end{aligned} \tag{6}$$

$$\begin{aligned} & G_{b,g} V\underline{\boldsymbol{c}} \not\equiv \underline{0} \\ \iff & M_g \underline{\boldsymbol{c}} \not\equiv \underline{0} (M_g = G_{b,g} V) \end{aligned} \tag{7}$$

9 条件 C の分析

定義 9.1. サイクル $\mathcal{C}$ の関数 $f_{\mathcal{C}}(x)$ について、

$$f_{\mathcal{C}}(x) = A_{\mathcal{C}} x + B_{\mathcal{C}}$$

と表すこととする。

6 節より、このブロックサイクルが閉とならないための条件は

$$B_{\mathcal{C}} \not\equiv 0 \pmod{\gcd(A_{\mathcal{C}} - 1, P)}$$

である。

定義 9.2. ここで、$B_{\mathcal{C}}$ は $\underline{\boldsymbol{b}}$ の線形結合なので、

$$B_{\mathcal{C}} = V_{\mathcal{C}} \underline{\boldsymbol{b}}$$

と表すこととする。

式 (2) に当てはめると、

$$\begin{aligned} & B_{\mathcal{C}} \not\equiv 0 \\ \iff & V_{\mathcal{C}} \underline{\boldsymbol{b}} \not\equiv 0 \\ \iff & V_{\mathcal{C}} V \underline{\boldsymbol{c}} \not\equiv 0 \pmod{\gcd(A_{\mathcal{C}} - 1, P)} \end{aligned}$$

現在、この式は mod$gcd(A_{\mathcal{C}} - 1, P)$ 上の方程式であるが、これを mod$P$ 上の方程式に持ち上げる。

$$\begin{aligned} & V_{\mathcal{C}} V \underline{\boldsymbol{c}} \not\equiv 0 \pmod{\gcd(A_{\mathcal{C}} - 1, P)} \\ \iff & \frac{P}{\gcd(A_{\mathcal{C}} - 1, P)} V_{\mathcal{C}} V \underline{\boldsymbol{c}} \not\equiv 0 \pmod{P} \\ \iff & V'_{\mathcal{C}} \underline{\boldsymbol{c}} \not\equiv 0 \pmod{P} \left(V'_{\mathcal{C}} = \frac{P}{\gcd(A_{\mathcal{C}} - 1, P)} V_{\mathcal{C}} \right) \end{aligned} \tag{8}$$

9.1 長さ 4 のサイクル

例として、長さ 4 のサイクル $\mathcal{C}$ に関する方程式を考える。

$$\mathcal{C} = f \to g \to h \to l \to f$$

とすると、

$$f_{\mathcal{C}}^{-1}(x) = f^{-1}gh^{-1}l(x)$$

であり、$f_i(x) = a_{f_i}x + b_{f_i}$ および $f_i^{-1}(x) = a_{f_i}^{-1}(x - b_{f_i})$ であるから、

$$\begin{aligned} f_{\mathcal{C}}^{-1}(x) &= f^{-1}fh^{-1}l(x) \\ &= a_f^{-1}(a_g a_h^{-1}(a_l x + b_l - b_h) + b_g - b_f) \\ &= a_f^{-1}a_g a_h^{-1}a_l x + a_f^{-1}(b_g - b_f) + a_f^{-1}a_g a_h^{-1}(b_l - b_h) \end{aligned}$$

とかける。

この表現を用いると、

$$\begin{aligned} A_{\mathcal{C}} &= a_f^{-1}a_g a_h^{-1}a_l \\ B_{\mathcal{C}} &= a_f^{-1}(b_g - b_f) + a_f^{-1}a_g a_h^{-1}(b_l - b_h) \end{aligned}$$

と書ける。

実際のサイクルで考えてみる。

例 9.3. まず、

$$\hat{H}_X = \left(\begin{array}{ccc\|ccc} f_0 & f_1 & f_2 & g_0 & g_1 & g_2 \\ f_2 & f_0 & f_1 & g_2 & g_0 & g_1 \end{array}\right)$$

$$\hat{H}_Z = \left(\begin{array}{ccc\|ccc} g_0^{-1} & g_2^{-1} & g_1^{-1} & f_0^{-1} & f_2^{-1} & f_1^{-1} \\ g_1^{-1} & g_0^{-1} & g_2^{-1} & f_1^{-1} & f_0^{-1} & f_2^{-1} \end{array}\right)$$

である。列選択 [0,1] について

$$\mathcal{C}_{X,[0,1],0} = f_0 \to f_1 \to f_0 \to f_2 \to f_0$$

なので、

$$\begin{aligned} A_{\mathcal{C}_{X,[0,1],0}} &= a_{f_0}^{-1}a_{f_1}a_{f_0}^{-1}a_{f_2} \\ B_{\mathcal{C}_{X,[0,1],0}} &= a_{f_0}^{-1}(b_{f_1} - b_{f_0}) + a_{f_0}^{-1}a_{f_1}a_{f_0}^{-1}(b_{f_2} - b_{f_0}) \end{aligned}$$

$$B_{\mathcal{C}_{X,[0,1],0}} = \begin{bmatrix} -a_{f_0}^{-1}(1 + a_{f_1}a_{f_0}^{-1}) & a_{f_0}^{-1} & -a_{f_0}^{-1}a_{f_1}a_{f_0}^{-1} & 0 & 0 & 0 \end{bmatrix} \underline{\boldsymbol{b}}$$

であるから、

$$V_{\mathcal{C}_{X,[0,1],0}} = \begin{bmatrix} -a_{f_0}^{-1}(1 + a_{f_1}a_{f_0}^{-1}) & a_{f_0}^{-1} & -a_{f_0}^{-1}a_{f_1}a_{f_0}^{-1} & 0 & 0 & 0 \end{bmatrix}$$

である。

条件 C では、確認すべき列選択が 2815 個あり、これを開始行 0,1 行目、行列 $\hat{H}_X, \hat{H}_Z$ について確認する必要があるので、総計で $2815 \times 4 = 11260$ 個のサイクルに関して方程式を立てる必要がある。

以上まとめると、(3) を解いて求めた基底 $\underline{\boldsymbol{v}}_0, \ldots$ について、(6) と (7) および、11260 個のサイクルに対応する (8) の計 11262 個の合同不等式を満たすような係数 $c_0, \ldots$ を求めればよいことが分かった。

10　2026/01/16 のゼミ

10.1　ここまでの進捗

- $\underline{\boldsymbol{a}}$ を固定したときの条件 A,B を満たす $\underline{\boldsymbol{b}}$ を見つけるための方法を考えた。
- 条件 C について、すべてのサイクルを網羅でする方法を明確にした。
- 最終的に解となる $\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}$ が満たすべき数式を出した。

10.2　これからのタスク

- 11262 個の不等式をそれぞれ解くことで $\equiv 0$ になってしまう c_i は出し、これらを除外して残ったものを解とする、というのは現実的ではない？
- サイクル同士で依存関係 (サイクル $\mathcal{C}_1$ が CBC ならサイクル $\mathcal{C}_2$ も CBC) が見つけられれば式の数を削減できる。
- $\underline{\boldsymbol{b}}$ に関する条件式ならば一次だが、$\underline{\boldsymbol{a}}$ に関する条件式とみなすと次数が上がるので $\underline{\boldsymbol{a}}, \underline{\boldsymbol{b}}$ すべてを変数とみなすときにこの方式を使うのは難しそう。

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

11.1 従来の行列の構成方法

定義 11.1. $\hat{H}_X, \hat{H}_Z$ 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 11.2. 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 11.3. 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。

11.2 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 11.4. 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 11.5. 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。

11.3 アクティブ部の直交性の十分条件

定義 11.6.

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

定理 11.7. 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。

11.4 潜在部の非直交性の必要条件

定義 11.8. 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。

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

$L \geq 4J$ 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。

11.5 ガーズの上界

長さ 8 のサイクルは必ず存在する。

11.6 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。

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)

可換表テーブル：

	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

12 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

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。

12.1 条件 A'

$$(a_{f_i} - 1)b_{g_j} - (a_{g_j} - 1)b_{f_i} \not\equiv 0 \pmod{P} \quad \text{for } (i,j) \in [L/2]^2 \backslash \{(0,3),(1,2)\}$$

12.2 条件 B'

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

12.3 条件 C'

条件 3 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。

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

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

論文の通り、

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

は UTCBC である。他にも UTCBC の形があるかもしれない。

定義 12.1. 行インデックスシーケンス c、列インデックスシーケンス r により特定される $\hat{H}_X(\hat{H}_Z)$ でのサイクルを $\mathcal{C}_{c,r,X(Z)}$ と表す。

12.3.1　長さ 4 のサイクル

長さ 4 のサイクルは、長さ 2 の行インデックスシーケンス及び長さ 2 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。例えば、

$$\begin{aligned}\mathcal{C}_{[0,7],[0,1],X} &= (\hat{H}_X)_{0,0} \to (\hat{H}_X)_{0,7} \to (\hat{H}_X)_{1,7} \to (\hat{H}_X)_{1,0} \\ &= F_0 \to G_1 \to G_0 \to F_5\end{aligned}$$

となる。

行インデックスシーケンス $c = [c_1, c_2]$、列インデックスシーケンス $r = [r_1, r_2]$ とする。ただし、$c_1, c_2 \in [L]$、$r_1, r_2 \in [L/2]$ である。

■同一とみなせるサイクル　$c_1 = c_2$ または $r_1 = r_2$ のとき、このサイクルの関数は明らかに恒等関数となる。$\mathcal{C}_{[c_1,c_2],[r_1,r_2],X}$ が閉ならば、$\mathcal{C}_{[c_1,c_2],[r_2,r_1],X}, \mathcal{C}_{[c_2,c_1],[r_1,r_2],X}, \mathcal{C}_{[c_2,c_1],[r_2,r_1],X}$ も閉である。

以上を踏まえると、$c_1 < c_2, r_1 < r_2$ としてよく、列インデックスシーケンスは $(L^2 - L)/2$ 通り、列インデックスシーケンスは $((L/2)^2 - L/2)/2$ 通りあり、これらを $\hat{H}_X, \hat{H}_Z$ で考えるので、長さ 4 のサイクルは $(L^2 - L)/2 \times ((L/2)^2 - L/2)/2 \times 2$ 通りある。$L = 12$ で考えると、$12^4/2 = 10368$ 通りとなる。

12.3.2　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。例えば、

$$\begin{aligned}\mathcal{C}_{[0,7,1,5],[0,1,2,3],X} &= (\hat{H}_X)_{0,0} \to (\hat{H}_X)_{0,7} \to (\hat{H}_X)_{1,7} \to (\hat{H}_X)_{1,1} \\ &\quad \to (\hat{H}_X)_{2,1} \to (\hat{H}_X)_{2,5} \to (\hat{H}_X)_{3,5} \to (\hat{H}_X)_{3,0} \\ &= F_0 \to G_1 \to G_0 \to F_0 \to F_5 \to F_3 \to F_2 \to F_3\end{aligned}$$

となる。行インデックスシーケンスは $(L/2)^4$ 通り、列インデックスシーケンスは L^4 通りあり、これらを $\hat{H}_X, \hat{H}_Z$ で考えるので、長さ 4 のサイクルは $(L/2)^4 \times L^4 \times 2 = L^8/8$ 通りある。$L = 12$ で考えると、$12^8/8 = 53747712$ 通りとなる。

付録 A　定理 5.1 の証明

Proof. まず、円環状にする前の、長さ n の直線の列 $x_1, x_2, \ldots, x_n$ を考える。隣り合う要素 x_i, x_{i+1} は常に異なるとする。この直線の列全体における色の塗り分けの総数は、先頭 x_1 が k 通り、それ以降の $x_2, \ldots, x_n$ がそれぞれ直前の要素と異なるため $k - 1$ 通りであることから、

$$W_n = k(k-1)^{n-1}$$

である。

ここで、W_n を以下の 2 つのケースに分割する。

- a_n：始点と終点が同じ色である場合の数 $(x_1 = x_n)$
- b_n：始点と終点が異なる色である場合の数 $(x_1 \neq x_n)$

すなわち、

$$a_n + b_n = k(k-1)^{n-1} \tag{9}$$

である。円環状に接続した際に条件を満たすのは、$x_1 \neq x_n$ の場合であるため、求める値は b_L となる。

次に、n から $n+1$ への漸化式を考える。長さ n の列に、条件を満たすように新たな要素 x_{n+1} を追加する。

1. $x_1 = x_{n+1}$ となる場合（a_{n+1} を構成する場合）：x_{n+1} は x_n と異なる必要がある。また、x_{n+1} は x_1 と同じ色になるため、必然的に $x_n \neq x_1$ でなければならない。つまり、$x_1 \neq x_n$ である状態（b_n 通り）の末尾に、x_1 と同じ色（1 通り）を追加する場合のみ発生する。

$$a_{n+1} = b_n \times 1 = b_n \tag{10}$$

2. $x_1 \neq x_{n+1}$ となる場合（b_{n+1} を構成する場合）：これは全事象から a_{n+1} を引いたものである。式 ((9)) より、

$$b_{n+1} = k(k-1)^n - a_{n+1}$$

式 ((10)) を代入すると、以下の b_n に関する漸化式が得られる。

$$b_{n+1} = k(k-1)^n - b_n$$

この漸化式を解く。

$$\begin{aligned} b_{n+1} - (k-1)^{n+1} &= -(b_n - (k-1)^n) \\ b_n - (k-1)^n &= (-1)^{n-2}(b_2 - (k-1)^2) \end{aligned}$$

ここで、$n = 2$ の場合、隣り合う要素は異なるため必ず $x_1 \neq x_2$ となる。よって $a_2 = 0, b_2 = k(k-1)$ である。

$$\begin{aligned} b_2 - (k-1)^2 &= k(k-1) - (k-1)^2 \\ &= (k-1)(k-(k-1)) \\ &= k-1 \end{aligned}$$

したがって、

$$\begin{aligned} b_n - (k-1)^n &= (-1)^{n-2}(k-1) \\ b_n &= (k-1)^n + (-1)^n(k-1) \end{aligned}$$

以上より、長さ L の円環状の列シーケンスの総数は $(k-1)^L + (-1)^L(k-1)$ となる。 □

付録 B　2 の解の導出

■$a_f \neq 1$ かつ $a_g \neq 1$ のとき

$\gcd(a_f - 1, P) = 1$ のとき、$(a_f - 1)^{-1}$ が存在するので、$b_g = (a_f - 1)^{-1}(a_g - 1)b_f$ により解が一意に決まる。

$\gcd(a_f - 1, P) = d > 1$ のとき、

$$\begin{aligned} A &= a_f - 1 \\ C &= (a_g - 1)b_f \\ x &= b_g \end{aligned}$$

とする。これにより、式 ((1)) は以下の 1 次合同方程式となる。

$$Ax \equiv C \pmod{P}$$

合同式の定義より、ある整数 k が存在して $Ax - C = Pk$ が成り立つ。これを変形すると、以下の 1 次不定方程式が得られる。

$$Ax - Pk = C \tag{11}$$

A と P はともに d の倍数であるため、互いに素な整数 A', P' を用いて以下のように表せる。

$$A = dA', \quad P = dP'$$

これらを式 ((11)) に代入すると、

$$\begin{aligned} dA'x - dP'k &= C \\ d(A'x - P'k) &= C \end{aligned} \tag{12}$$

左辺は整数 d と整数の積であるため d の倍数である。したがって、等式が成立するためには、右辺 C も d で割り切れなければならない。これより、以下の 2 つのケースに分類される。

$C \not\equiv 0 \pmod{d}$ 等式を満たす整数 x, k は存在しない。したがって、この場合、元の合同方程式の解は存在しない。

$C \equiv 0 \pmod{d}$ $C = dC'$ となる整数 C' が存在する。式 ((12)) の両辺を d で割ると、

$$A'x - P'k = C'$$

となる。これを合同式に戻すと、法 P' における方程式が得られる。

$$A'x \equiv C' \pmod{P'} \tag{13}$$

ここで $\gcd(A', P') = 1$ であるため、法 P' において A' の逆元 $(A')^{-1}$ が一意に存在する。よって、式 ((13)) は法 P' においてただ 1 つの解 x_0 を持つ。

$$x \equiv x_0 \pmod{P'} \implies x = x_0 + mP' \quad (m \in \mathbb{Z})$$

元の法 $P\ (=dP')$ における解 x を求めるため、$0 \leq x < P$ の範囲にある解を探す。

$$0 \leq x_0 + mP' < dP'$$
$$0 \leq \frac{x_0}{P'} + m < d$$

x_0 を $0 \leq x_0 < P'$ と選べば、これを満たす整数 m は $0, 1, \ldots, d-1$ の計 d 個存在する。したがって、解は $b_g = x_0 + nP'(n = 0, 1, \ldots, d-1)$

■$a_f = 1$ **かつ** $a_g \neq 1$ **のとき**　$A = 0$ より左辺が 0 になるので、右辺が 0、すなわち $C = 0$ であれば任意の b_g が解となり、そうでない場合は解なしとなる。

■$a_g = 1$ **のとき**

このとき、$a_g - 1 = 0$ より $C = 0$ である。よって、右辺の Ax が P の倍数であればよい。

$a_f = 1$ の時、$A = 0$ より $Ax = 0$ となるため、任意の b_g で式 (1) は成り立つ。

$a_f \neq 1$ のとき、以下の 2 つの場合に分けて考える。

$\gcd(A, P) = 1$ 解は $b_g = 0$ のみ

$\gcd(A, P) = d > 1$ $A = dA', P = dP'$ とすると、x は $dA'x = mP = mdP'$ を満たせばよい $(m \in \mathbb{Z})$。A' と P' は互いに素なので、x は P' の倍数であればよい。よって、解は $b_g = nP'(n = 0, 1, \ldots, d-1)$ となる。