研究ノート

黒澤雅治

2025/12/21

1 $\underline{f}, \underline{g}$ の条件を満たす解空間の特定

1.1 $\underline{f}, \underline{g}$ の満たすべき条件

1. 要請 1.4 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)
2. 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。
3. UTCBC$\underline{u}(k)$ 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。

1.2 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。

1.2.1 同一とみなせるサイクル

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 1.1. 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、

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

定義 1.2. 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、

$$C_{S(\ell),0} = ([0, b], [0, c], [1, c], [1, d], [0, d], [0, a], [1, a], [1, b]) = C_{\ell,1} \tag{3}$$
$$C_{S(\ell),1} = ([1, b], [1, c], [0, c], [0, d], [1, d], [1, a], [0, a], [0, b]) = C_{\ell,0} \tag{4}$$

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

$$C_{S^2(\ell),0} = ([0, c], [0, d], [1, d], [1, a], [0, a], [0, b], [1, b], [1, c]) = C_{\ell,0} \tag{5}$$
$$C_{S^2(\ell),1} = ([1, c], [1, d], [0, d], [0, a], [1, a], [1, b], [0, b], [0, c]) = C_{\ell,1} \tag{6}$$

以上から、以下の定理が成り立つ。

定理 1.3.

$$C_{(\ell),0} = C_{(S(\ell)),1} = C_{S^2(\ell),0} \tag{7}$$
$$C_{(\ell),1} = C_{(S(\ell)),0} = C_{S^2(\ell),1} \tag{8}$$
$$\tag{9}$$

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。

要請 1.4. 以下の可換性条件が成り立つことを要請する。

$$g_{\ell-j}\, f_{k-\ell} = f_{k-\ell}\, g_{\ell-j} \quad (\text{for all } \ell \in [L/2],\ j, k \in [J]) \tag{10}$$

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。

$$f_{\ell-j}\, g_{k-\ell} = g_{k-\ell}\, f_{\ell-j} \quad (\text{for all } \ell \in [L/2],\ j, k \in [J]), \tag{11}$$
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。
$$\tag{12}$$
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。
$$\tag{13}$$

1.3 条件 3

1.2 節に基づき、検査する必要のあるサイクルの個数を考える。長さ $2l$ のサイクル、つまり長さ l の列シーケンスを考える。定理 1.3 より、開始行として 0,1 行目の 2 通りを考えれば、シフトして等しい列選択は同一視できる。長さ l のシーケンスは L^l 通りあり、それぞれ $0\ l-1$ つのシフトを同一視できるので、検査すべき列シーケンスの総数は L^l/l 個である。これに開始行が 0,1 行目の 2 通りあることを加えて、考慮すべきサイクルの総数は $2L^l/l$ 通りである。ゆえに、条件 3 で検査すべきサイクルの総数は $\sum_{l=1}^{L/2} \frac{2L^{2l}}{2l} = \sum_{l=1}^{L/2} \frac{L^{2l}}{l}$ である。

1.4 UTCBC

論文では、開始行が 0 行目であるとき、列選択 $[0, 3+j\%3, 1, 3+(j-1)\%3, 2, 3+(j-2)\%3]$ 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。

$$\underline{u}(j)_1 = f_2 \to g_{j-1} \to g_j \to f_1 \to f_0 \to g_{j+1} \to g_{j-1} \to f_2 \to f_1 \to g_j \to g_{j+1} \to f_0 \to f_2$$

$$f_{\underline{u}(j)_1}(x) = (f_0^{-1} g_{j+1} g_j^{-1} f_1)(f_2^{-1} g_{j-1} g_{j+1}^{-1} f_0)(f_2 g_{j-1}^{-1} g_j f_1^{-1})(x) \tag{14}$$

$$= (f_1 g_j^{-1} g_{j+1} f_0^{-1})(f_0 g_{j+1}^{-1} g_{j-1} f_2^{-1})(f_2 g_{j-1}^{-1} g_j f_1^{-1})(x) = x \tag{15}$$

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。

1.5 $\hat{H}_X$ 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。

1.6 可換性条件の分析

$f = a_1 x + b_1, g = a_2 x + b_2$ とする。$(a_1, b_1, a_2, b_2 \in [P], a_1, a_2 \neq 0)$ 可換性条件は、すべての $x \in [P]$ に対して

$$f(g(x)) = g(f(x)) \tag{16}$$

$$\iff a_1(a_2 x + b_2) + b_1 = a_2(a_1 x + b_1) + b_2 \tag{17}$$

$$\iff a_1 a_2 x + a_1 b_2 + b_1 = a_2 a_1 x + a_2 b_1 + b_2 \tag{18}$$

$$\iff a_1 b_2 + b_1 = a_2 b_1 + b_2 \tag{19}$$

$$\iff (a_1 - 1) b_2 = (a_2 - 1) b_1 \tag{20}$$

式 20 を、b_2 に関する方程式とみなす。この方程式は $\pmod P$ 上の 1 次合同方程式であることに注意する。

■$a_1 \neq 1$ かつ $a_2 \neq 1$ のとき

$\gcd(a_1 - 1, P) = 1$ のとき、$(a_1 - 1)^{-1}$ が存在するので、$b_2 = (a_1 - 1)^{-1}(a_2 - 1) b_1$ により解が一意に決まる。

$\gcd(a_1 - 1, P) = d > 1$ のとき、

$$A = a_1 - 1 \tag{21}$$

$$C = (a_2 - 1) b_1 \tag{22}$$

$$x = b_2 \tag{23}$$

とする。これにより、式 (20) は以下の 1 次合同方程式となる。

$$Ax \equiv C \pmod P \tag{24}$$

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。

$$Ax - Pk = C \tag{25}$$

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。

$$A = dA', \quad P = dP' \tag{26}$$

これらを式 (25) に代入すると、

$$dA'x - dP'k = C \tag{27}$$
$$d(A'x - P'k) = C \tag{28}$$

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 (28) の両辺を d で割ると、

$$A'x - P'k = C' \tag{29}$$

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。

$$A'x \equiv C' \pmod{P'} \tag{30}$$

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 (30) 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 $b_2 = x_0 + nP' (n = 0, 1, \ldots, d-1)$

■$a_1 = 1$ **かつ** $a_2 \neq 1$ **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_2 が解となり、そうでない場合は解なしとなる。

■$a_2 = 1$ のとき

このとき、$a_2 - 1 = 0$ 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。

$a_1 = 1$ の時、$A = 0$ より $Ax = 0$ となるため、任意の b_2 で式 20 は成り立つ。

$a_1 \neq 1$ のとき、以下の 2 つの場合に分けて考える。

$\gcd(A, P) = 1$　解は $b_2 = 0$ 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 $b_2 = nP'(n = 0, 1, \ldots, d-1)$ となる。