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 1.1 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)
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。

要請 1.1. 以下の可換性条件が成り立つことを要請する。

$$g_{\ell-j}\, f_{k-\ell} = f_{k-\ell}\, g_{\ell-j} \quad (\text{for all } \ell \in [L/2],\ j, k \in [J]) \tag{1}$$

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。

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

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。 (3)

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。 (4)

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

■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 1.2. 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、

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

定義 1.3. 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、

$$C_{S(\ell),0} = ([0, b], [0, c], [1, c], [1, d], [0, d], [0, a], [1, a], [1, b]) = C_{\ell,1} \tag{7}$$
$$C_{S(\ell),1} = ([1, b], [1, c], [0, c], [0, d], [1, d], [1, a], [0, a], [0, b]) = C_{\ell,0} \tag{8}$$

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

$$C_{S^2(\ell),0} = ([0, c], [0, d], [1, d], [1, a], [0, a], [0, b], [1, b], [1, c]) = C_{\ell,0} \tag{9}$$
$$C_{S^2(\ell),1} = ([1, c], [1, d], [0, d], [0, a], [1, a], [1, b], [0, b], [0, c]) = C_{\ell,1} \tag{10}$$

以上から、以下の定理が成り立つ。

定理 1.4.

$$C_{(\ell),0} = C_{(S(\ell)),1} = C_{S^2(\ell),0} \tag{11}$$
$$C_{(\ell),1} = C_{(S(\ell)),0} = C_{S^2(\ell),1} \tag{12}$$
$$\tag{13}$$

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。

1.2.2 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。

1.3 条件 3 で検査する列シーケンスの個数

1.2.1 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 1.5. 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。

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、

$$W_n = k(k-1)^{n-1} \tag{14}$$

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、

$$a_n + b_n = k(k-1)^{n-1} \tag{15}$$

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。

$$a_{n+1} = b_n \times 1 = b_n \tag{16}$$

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 (15) より、

$$b_{n+1} = k(k-1)^n - a_{n+1} \tag{17}$$

式 (16) を代入すると、以下の b_n に関する漸化式が得られる。

$$b_{n+1} = k(k-1)^n - b_n \tag{18}$$

この漸化式を解く。

$$b_{n+1} - (k-1)^{n+1} = -(b_n - (k-1)^n) \tag{19}$$

$$b_n - (k-1)^n = (-1)^{n-2}(b_2 - (k-1)^2) \tag{20}$$

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。

$$b_2 - (k-1)^2 = k(k-1) - (k-1)^2 \tag{21}$$
$$= (k-1)(k-(k-1)) \tag{22}$$
$$= k-1 \tag{23}$$

したがって、

$$b_n - (k-1)^n = (-1)^{n-2}(k-1) \tag{24}$$
$$b_n = (k-1)^n + (-1)^n(k-1) \tag{25}$$

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。 □

まず、$L = 6$ の場合を考える。$k = 6, L = 6$ を代入すると、

$$5^6 + 5 = 15630 \tag{26}$$

通りとなる。1.2.1 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、

$$5^4 + 5 = 630 \tag{27}$$

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、

$$5^2 + 5 = 30 \tag{28}$$

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。

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。

$$\underline{u}(j)_1 = f_2 \to g_{j-1} \to g_j \to f_1 \to f_0 \to g_{j+1} \to g_{j-1} \to f_2 \to f_1 \to g_j \to g_{j+1} \to f_0 \to f_2 \tag{29}$$

$$f_{\underline{u}(j)_1}(x) = (f_0^{-1} g_{j+1} g_j^{-1} f_1)(f_2^{-1} g_{j-1} g_{j+1}^{-1} f_0)(f_2 g_{j-1}^{-1} g_j f_1^{-1})(x) \tag{30}$$

$$= (f_1 g_j^{-1} g_{j+1} f_0^{-1})(f_0 g_{j+1}^{-1} g_{j-1} f_2^{-1})(f_2 g_{j-1}^{-1} g_j f_1^{-1})(x) = x \tag{31}$$

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

$$f(g(x)) = g(f(x)) \tag{32}$$

$$\iff a_1(a_2 x + b_2) + b_1 = a_2(a_1 x + b_1) + b_2 \tag{33}$$

$$\iff a_1 a_2 x + a_1 b_2 + b_1 = a_2 a_1 x + a_2 b_1 + b_2 \tag{34}$$

$$\iff a_1 b_2 + b_1 = a_2 b_1 + b_2 \tag{35}$$

$$\iff (a_1 - 1) b_2 = (a_2 - 1) b_1 \tag{36}$$

式 36 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、

$$A = a_1 - 1 \tag{37}$$
$$C = (a_2 - 1)b_1 \tag{38}$$
$$x = b_2 \tag{39}$$

とする。これにより、式 (36) は以下の 1 次合同方程式となる。

$$Ax \equiv C \pmod{P} \tag{40}$$

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。

$$Ax - Pk = C \tag{41}$$

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。

$$A = dA', \quad P = dP' \tag{42}$$

これらを式 (41) に代入すると、

$$dA'x - dP'k = C \tag{43}$$
$$d(A'x - P'k) = C \tag{44}$$

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 (44) の両辺を d で割ると、

$$A'x - P'k = C' \tag{45}$$

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。

$$A'x \equiv C' \pmod{P'} \tag{46}$$

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 (46) 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、$0 \le x < P$ の範囲にある解を探す。

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

x_0 を $0 \le x_0 < P'$ 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 36 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。

1.7　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。

$a = 1$ 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。

1.8　AI に相談

1.8.1　問題の定式化

$\mathbb{Z}_P$ 上のアフィン置換行列（APM）の構成を考える。行重みを L とし、左右それぞれのブロック数を $L/2$ とする。アフィン置換の列を以下のように定義する。

$$\underline{f} = (f_0, \ldots, f_{L/2-1}), \quad \underline{g} = (g_0, \ldots, g_{L/2-1})$$

ここで、各置換は $f_i(x) = a_{f,i}x + b_{f,i} \pmod P$ および $g_i(x) = a_{g,i}x + b_{g,i} \pmod P$ で定義される。

本手法の目的は、乗法成分（傾き）$\mathbf{a}$ を固定した状態で、可換性条件およびサイクル回避条件を満たす加法成分（シフト項）$\mathbf{b}$ を決定することである。すべてのシフト変数をまとめたベクトルを

次のように定義する。

$$\mathbf{b} = [b_{f,0}, \ldots, b_{f,L/2-1}, b_{g,0}, \ldots, b_{g,L/2-1}]^\top \in \mathbb{Z}_P^L. \tag{47}$$

1.8.2 線形部分空間としての可換性

パリティ検査行列の直交性のために要求される可換性条件は $f_i \circ g_i = g_i \circ f_i$ で与えられる。アフィン置換において、これは以下と等価である。

$$a_{f,i}(a_{g,i}x + b_{g,i}) + b_{f,i} \equiv a_{g,i}(a_{f,i}x + b_{f,i}) + b_{g,i} \pmod{P}$$

x を含む項を整理すると、シフトパラメータに関する以下の線形制約が得られる。

$$(a_{f,i} - 1)b_{g,i} - (a_{g,i} - 1)b_{f,i} \equiv 0 \pmod{P}. \tag{48}$$

この式はすべての $i \in \{0, \ldots, L/2-1\}$ に対して成立する。これらの方程式を行列形式でまとめると次のようになる。

$$M_{\mathrm{comm}}\mathbf{b} \equiv \mathbf{0} \pmod{P}, \tag{49}$$

ここで、M_{comm} は $(L/2) \times L$ 行列である。可換性条件の解空間は M_{comm} の**核**（カーネル、零空間）に対応する。この核の基底を $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ とすると、条件を満たす任意の $\mathbf{b}$ は次のように表現できる。

$$\mathbf{b} = \sum_{j=1}^{k} c_j \mathbf{v}_j \pmod{P}, \quad c_j \in \mathbb{Z}_P. \tag{50}$$

1.8.3 禁止超平面としてのサイクル回避

タナーグラフ上のサイクルは、列遷移の系列によって形成される合成アフィン写像 $\Phi(x)$ に対応する。長さ 2ℓ のサイクル $\mathcal{C}$ が ℓ 個の写像 $T_1, \ldots, T_\ell$ の合成で表されるとする。

$$\Phi_{\mathcal{C}}(x) = T_\ell \circ \cdots \circ T_1(x) = A_{\mathcal{C}}x + B_{\mathcal{C}} \pmod{P}.$$

ここで、$A_{\mathcal{C}}$ は傾き係数の積であり、$B_{\mathcal{C}}$ は累積されたシフト量である。重要な点は、$B_{\mathcal{C}}$ が元のシフトパラメータ $\mathbf{b}$ の**線形結合**であることである。したがって、ある係数ベクトル $\mathbf{w}_{\mathcal{C}} \in \mathbb{Z}^L$ が存在し、次式が成り立つ。

$$B_{\mathcal{C}}(\mathbf{b}) = \mathbf{w}_{\mathcal{C}}^\top \mathbf{b} \pmod{P}. \tag{51}$$

サイクル（不動点 x）が存在するための条件は、合同式 $(A_{\mathcal{C}} - 1)x \equiv -B_{\mathcal{C}} \pmod{P}$ が解を持つことである。逆に、このサイクルの形成を**回避**するためには、この合同式が解を持たないようにすればよい。すなわち、以下の条件が必要となる。

$$B_{\mathcal{C}}(\mathbf{b}) \not\equiv 0 \pmod{\gcd(A_{\mathcal{C}} - 1, P)}. \tag{52}$$

ここで $G_{\mathcal{C}} = \gcd(A_{\mathcal{C}} - 1, P)$ とおく。式 (50) をこの不等式に代入すると、自由パラメータ c_j に対する制約が得られる。

$$\mathbf{w}_{\mathcal{C}}^{\top} \left(\sum_{j=1}^{k} c_j \mathbf{v}_j \right) \not\equiv 0 \pmod{G_{\mathcal{C}}}. \tag{53}$$

これはパラメータ空間 $\{c_j\}$ における**禁止超平面**を定義する。

1.8.4 提案する構成的アルゴリズム（ふるい法）

ランダムサンプリングに代わり、以下の構成的アルゴリズムを提案する。

Algorithm 1 サイクルフリー符号構成のための代数的ふるい法

入力: 行重み L, 法 P.
合成写像において $\gcd(a-1, P)$ が大きくなるよう、傾きベクトル $\mathbf{a}_f, \mathbf{a}_g$ を選択する.
M_{comm} を構築し、その核の基底 $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ を計算する.
禁止制約の集合を $\mathcal{F} \leftarrow \emptyset$ で初期化する.
for 長さ 4, 8 の各サイクル候補トポロジー $\mathcal{T}$ **do**
    記号的な合成写像 $\Phi_{\mathcal{T}}$ を構築する.
    線形依存ベクトル $\mathbf{w}_{\mathcal{T}}$ と法 $G_{\mathcal{T}}$ を抽出する.
    制約 $(\mathbf{w}_{\mathcal{T}}^{\top} V \mathbf{c} \not\equiv 0 \mod G_{\mathcal{T}})$ を $\mathcal{F}$ に追加する.
end for
求解: $\mathcal{F}$ 内のすべての制約を満たすパラメータベクトル $\mathbf{c} = (c_1, \ldots, c_k)$ を探索する.
出力: $\mathbf{b} = V\mathbf{c}$.

本手法は、探索問題を線形合同式上の制約充足問題（CSP）に変換するものであり、解空間の体積を直接計算し、短いサイクルを決定論的に回避することを可能にする。

1.9 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:

$$(a_{f,i} - 1) b_{g,j} - (a_{g,j} - 1) b_{f,i} \equiv 0 \pmod{P} \quad \text{for all } i, j \in [P] \tag{54}$$

- 条件 b:

$$(a_{f,i} - 1) b_{f,j} - (a_{f,j} - 1) b_{f,i} \not\equiv 0 \pmod{P} \quad \text{for any } i \neq j \in [P] \tag{55}$$
$$(a_{g,i} - 1) b_{g,j} - (a_{g,j} - 1) b_{g,i} \not\equiv 0 \pmod{P} \quad \text{for any } i \neq j \in [P] \tag{56}$$

$\underline{a} = [\underline{a}_f, \underline{a}_g] = [a_{f,0}, a_{f,1}, a_{f,2}, a_{g,0}, a_{g,1}, a_{g,2}], \underline{b} = [\underline{b}_f, \underline{b}_g] = [b_{f,0}, b_{f,1}, b_{f,2}, b_{g,0}, b_{g,1}, b_{g,2}]$ とする。

条件 a を行列を用いて表すと、

$$\begin{bmatrix} 1-a_{g,0} & 0 & 0 & a_{f,0}-1 & 0 & 0 \\ 1-a_{g,1} & 0 & 0 & 0 & a_{f,0}-1 & 0 \\ 1-a_{g,2} & 0 & 0 & 0 & 0 & a_{f,0}-1 \\ 0 & 1-a_{g,0} & 0 & a_{f,1}-1 & 0 & 0 \\ 0 & 1-a_{g,1} & 0 & 0 & a_{f,1}-1 & 0 \\ 0 & 1-a_{g,2} & 0 & 0 & 0 & a_{f,1}-1 \\ 0 & 0 & 1-a_{g,0} & a_{f,2}-1 & 0 & 0 \\ 0 & 0 & 1-a_{g,1} & 0 & a_{f,2}-1 & 0 \\ 0 & 0 & 1-a_{g,2} & 0 & 0 & a_{f,2}-1 \end{bmatrix} \underline{b} \equiv O \pmod{P} \tag{57}$$

条件 b を行列を用いて表すと、

$$\begin{bmatrix} 1-a_{f,1} & a_{f,0}-1 & 0 & 0 & 0 & 0 \\ 1-a_{f,2} & 0 & a_{f,0}-1 & 0 & 0 & 0 \\ 0 & 1-a_{f,2} & a_{f,1}-1 & 0 & 0 & 0 \end{bmatrix} \underline{b} \equiv \underline{c}_f \pmod{P} \tag{58}$$

$$\begin{bmatrix} 0 & 0 & 0 & 1-a_{g,1} & a_{g,0}-1 & 0 \\ 0 & 0 & 0 & 1-a_{g,2} & 0 & a_{g,0}-1 \\ 0 & 0 & 0 & 0 & 1-a_{g,2} & a_{g,1}-1 \end{bmatrix} \underline{b} \equiv \underline{c}_g \pmod{P} \tag{59}$$

この時、$\underline{c}_f \neq \underline{0}$ かつ $\underline{c}_g \neq \underline{0}$ である。

まずは、$\underline{a}$ を定数として固定した状態で条件 a,b を満たす $\underline{b}$ 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 57 の解空間を求め、そこからランダムに選んだものが式 58,59 を満たすか確かめる。

1.10 条件 c の分析