位数 120 の 2 つの群の difference set について

梶浦　大起（hikajiura@hiroshima-u.ac.jp）

2021/10/16

1　導入

G を位数 v の有限群とする。G の k 点部分集合 D が (v,k,λ)-difference set であるとは，任意の非単位元 $a \in G$ に対して，$a = x^{-1}y$ となる $x, y \in D$ の数が a の取り方によらず λ 通りであるときを指す。difference set は，群軌道が対称 $2(v,k,\lambda)$-design になる部分集合の特徴づけとして [1] で示されて以来，様々な研究が行われている。良い性質を持つ群のクラスには非常にいろいろなことが知られており，特に巡回群の difference set などではいくつかの無限系列が実際に構成されている [4]。しかし，具体的に群をひとつ与えたときに，その群の difference set の存在・非存在を決定する問題は非常に難しく，まだまだわかっていないことも多い。

本講演では，以下のふたつの群で difference set の存在・非存在を決定する問題を考えたい:

$$\begin{aligned} G_1 &:= \left\langle x,y,z \mid y^3, x^5, z^8, xy(yx)^{-1}, zx(xz)^{-1}, zyz^{-1}y \right\rangle \\ &= (C_3 \rtimes C_8) \times C_5, \\ G_3 &:= \left\langle x,y,z \mid y^3, x^5, z^8, zyz^{-1}y, zxz^{-1}x, yx(xy)^{-1} \right\rangle \\ &= C_3 \rtimes (C_5 \rtimes C_8). \end{aligned}$$

ここで，C_n は n 次巡回群とする。

言い換えると，本講演における中心的な問題は以下のものになる:

■問　G_1 と G_3 に $(120,35,10)$-difference set が存在するか判定せよ。

上の問いについて，我々は以下のように存在しないことを示した:

定理 1 (主結果)**.** G_1 と G_3 には $(120,35,10)$-difference set は存在しない。

■背景　研究の背景のひとつとして，我々はパラメータ v，k，λ を与えたときに，対称 $2(v,k,\lambda)$-design を分類したいという意識がある。前述の通り difference set は対称 2-design の便利な構成法としてよく知られており，もし (v,k,λ)-difference set が存在することを示せれば対応する対称 $2(v,k,\lambda)$-デザインを構成することができる。

今回の話は以下の予想に興味がある:

予想 A　対称 $2(120,35,10)$-design は非存在である。

予想 A を解くことは非常に難しい。そこで，まずは部分的な問題として，difference set で非存在であることを示したい。つまり次の予想をときたい:

予想 B　$(120,35,10)$-difference set は非存在である。

本講演はこの予想 B について部分的な解決ができたことを報告するものである。予想 B についての先行研究と本研究の結果の位置づけを簡単に述べる。位数 120 の有限群は同型を除いて 47 種類，可解群 44 種類，非可解群 3 種類がある。この内，可解群については 3 つの群を除いて $(120,35,10)$-difference set が存在しないことが示されている [5]。本講演の主結果は，この未解決であった位数 120 の可解群のうち 2 つについて非存在であることを示した。

2　準備

2.1　等分布函数とその準同型

ここでは主定理の証明を理解するための用語と記号を準備する。最初に，difference set を一般化した等分布函数という概念を導入する:

定義 2 (relation parititon)**.** X と I を有限集合とする。$R : X \times X \longrightarrow I$ が全射であるとき，(X,I,R) を relation partiton とおく。

特に,

- I の元 i_0 が存在して，$R(i_0) = \{(x,x) \in X \times X \mid x \in X\}$ のとき，unital relation parititon と呼び,
- 任意の $i \in \{0,\ldots,d\}$ に対して，ある $k_i \in \mathbb{Z}$ が存在して以下が成り立つとき，regular relation parititon と呼ぶ:

$$k_i = \#\{z \in X \mid R(x,z) = i\} = \#\{z \in X \mid R(z,x) = i\} \quad \text{for any } x \in X.$$

k_i を分岐指数と呼ぶ。

■注意　分岐指数は簡単な計算で，任意の i で $k_i \# X = \# R_i$ であることがわかる。

■例

1. X を有限群，$I := X$，$R(x,y) := x^{-1}y$ とする。このとき，(X, I, R) は unital regular relation parition となる。これを thin relation partition と呼ぶ。
2. 有限群 G が X に可移に作用しているとする。このとき，I を $X \times X$ の対角作用（i.e., $X \times X$ に $g \cdot (x,y) := (gx, gy)$）による軌道分解とする。このとき，$R(x,y)$ を $(x,y) \in X \times X$ を含む I の元に対応させる写像とすると，(X, I, R) も regular unital relation partition であり，特に Schurian relation parition と呼ぶ。本講演では，簡単のために G の部分集合 H について，左剰余類 G/H のなす Schurian relation partition も簡単のために G/H と書くことにする。
3. より一般に association scheme は regular unital relation parition である。

定義 3 (等分布函数)**.** (X, I, R) を unital regular relation paritition とする。$f \in \mathbb{Z}^X$ が (X, I, R) 上の (v, k, λ)-等分布函数であるとは，以下を満たすこと:

- $v = \# X$,
- $k = \sum_{x \in X} f(x)$,
- 任意の $i \in I \backslash \{i_0\}$ に対して，$\lambda = (A_i f | f)_X / k_i$ が成り立つ。

ここで, $f_1, f_2 \in \mathbb{Z}$ に対し $(f_1 | f_2)_X := \sum_{x \in X} f(x) g(x)$ (i.e., $\mathbb{Z}^X$ の ℓ^2-内積), $A_i \in \mathbb{Z}^{X \times X}$ を i に対応する隣接行列（i.e., $R(x,y) = i$ ならば $A_i(x,y) = 1$，それ以外で 0）とする。

等分布函数は以下の命題から difference set の一般化であることがわかる:

命題 4. 空でない有限群 G の部分集合 Y が (v, k, λ)-difference set であることと，Y の特性函数が G の thin relation partition 上の (v, k, λ)-等分布函数であることは同値である。

証明) thin relation partition の分岐指数は全て 1 であることと，Y の特性函数を δ_Y とおけば，各 $g \in G$ に対して

$$(A_g \delta_Y, \delta_Y)_G = \# \{(x,y) \in Y \times Y \mid x^{-1}y = g\}$$

であることから言える。　(証明了)

この節の最後に，この講演で非常に重要になる relation paritition の準同型を以下で定める:

定義 5 (relation paritition の準同型)**.** (X_1, I_1, R_1)，(X_2, I_2, R_2) を relation paritition とする。このとき，$(t, \tau) \in \mathrm{Map}(X, Y) \times \mathrm{Map}(I_1, I_2)$ が relation paritition の準同型であるとは，任意の $x, y \in X_1$ に対して以下を満たすこと:

$$R_2(t(x), t(y)) = \tau(R_1(x, y)).$$

■例

1. 群準同型 φ の組 (φ, φ) は thin relation paritition の間の準同型となる。
2. G を有限群として，部分群の列 $H < K < G$ とする。このとき，$X_1 := G/H$，$I_1 := H\backslash G/H$，$X_2 := G/K$，$I_2 := K\backslash G/K$ としてそれぞれの Schurian relation paritition (X_1, I_1, R_1)，(X_2, I_2, R_2) を考える。
   写像 $\theta : X_1 \longrightarrow X_2$ を G/H から G/K への標準射影，$\tau : I_1 \longrightarrow I_2$ を以下のように定めたとき，組 (θ, τ) は準同型となる:

$$\tau(HaH) := KaK \quad \text{for any } a \in G.$$

命題 6. (t, τ) を (X_1, I_1, R_1) から (X_2, I_2, R_2) の準同型とする。このとき，t が全射ならば τ も全射である。

証明) 準同型の定義は，$R_1 \circ (t \times t) = \tau \circ R_2$ ともかける[*1]。いま，relation paritition の定義から R_1 と R_2 は全射であり，更に仮定から $t \times t$ も全射なので，τ が全射になることが直ちにわかる。 (証明了)

特に t が全射のとき (t, τ) を全射準同型と呼ぶ。

[*1] $t \times t : X_1 \times X_1 \longrightarrow X_2 \times X_2;\ (x, y) \longmapsto (t(x), t(y))$ で定める。

3 主結果の証明

3.1 証明の概略

主結果の証明の概略を述べる。証明の中心は以下のアルゴリズムである:

Algorithm 1 Difference set の存在問題決定アルゴリズム

Input: $v, k, \lambda \in \mathbb{Z}_{>0}$, 有限群 G（ただし $\#G = v$）;

Output: True or False;

1: **read**(G の部分群列 $G = H_0 > H_1 > H_2 > \dots H_m = 1$);
2: Let $\mathcal{D}_0 := \{k\} \subset \mathbb{Z}^{G/H_0} = \mathbb{Z}$;
3: **for** $i = 1$ **to** m **do**
4: Let θ: G/H_i から G/H_{i-1} への標準射影;
5: $\mathcal{D}_i := \{f \in \theta_*^{-1}(\mathcal{D}_{i-1}) \mid (v/\#H_i, k, \lambda\#H_i)$-等分布函数かつ $0 \leq f \leq \#H_i\}$;
6: **if** $\mathcal{D}_i = \emptyset$ **then**
7: **return** False;
8: **end if**
9: **end for**
10: **return** True;

ここで各 i について $\theta_* : \mathbb{Z}^{G/H_i} \longrightarrow \mathbb{Z}^{G/H_{i-1}}$ は θ の押出し，i.e., 各 $f \in \mathbb{Z}^{G/H_i}$ に対し

$$\theta_*(f)(y) := \sum_{x \in \theta^{-1}(y)} f(x).$$

と定める。上記のアルゴリズムについて，以下の定理が成り立つ:

定理 7. $\mathcal{D}_m$ は G の (v, k, λ)-difference set の特性函数の全体である。特に，アルゴリズムの計算結果が True であれば G に (v, k, λ)-difference set は存在し，False であれば G に (v, k, λ)-difference set は存在しない。

この定理は以下の補題から直ちに示される（証明は後述）:

補題 8. ふたつの unital regular relation paritition (X_1, I_1, R_1)，(X_2, I_2, R_2) とその間の全射準同型 (θ, τ) を考える。このとき，任意の (X_1, I_1, R_1) 上の $(\#X_1, k, \lambda)$-等分布函数 $f \in \mathbb{Z}^{X_1}$ に対し，$\theta_*(f)$ は (X_2, I_2, R_2) 上の $(\#X_2, k, \lambda\#X_1/\#X_2)$-等分布函数と

なる。

■定理 7 の証明　上記の補題から任意の i に対して以下の命題が示される:

$$\mathcal{D}_i = \{f \in \mathbb{Z}^{G/H_i} \mid (v/\#H_i, k, \lambda\#H_i)\text{-等分布函数かつ } 0 \leq f \leq \#H_i\}.$$

実際, 右辺が左辺を含むのは明らかで, 左辺が右辺を含む (i.e., 任意の $(v/\#H_i, k, \lambda\#H_i)$-等分布函数 f が $0 \leq f \leq \#H_i$ を満たせば $\theta_*(f) \in \mathcal{D}_{i-1}$ となる）ことも，押し出しの定義から $0 \leq \theta_*(f) \leq \#H_{i-1}$ となることからいえる。

特に，$H_m = 1$ で $f \in \mathbb{Z}^{G/H_m}$ が $0 \leq f \leq 1$（i.e., f は G のある部分集合に関する特性函数）であるときは，(v, k, λ)-等分布函数であることと (v, k, λ)-difference set であることが同値であったので $\mathcal{D}_m$ は (v, k, λ)-difference set の特性函数の全体であることがわかる。

3.2　先行研究とアルゴリズムの関係

このアルゴリズムは [1, Lemma 4.1.] の一般化にあたる結果である。[1] は補題 8 の結果について，(X_1, I_1, R_1) と (X_2, I_2, R_2) が共に thin relation paritition（i.e., 有限群）で，かつ f は $0 \leq f \leq 1$（i.e., 特性函数）の場合に示した。この結果を用いて $\lambda < 20$ の場合の difference set の分類などが行われている [6]。また，特性函数の条件を外した（i.e., multi set の）場合にも同様に成り立つことが知られ，それらを利用したアルゴリズムが GAP[2] に「DifSets」というライブラリとして実装されている。実際ライブラリを活用して $v \leq 100$ の場合の difference set の分類などが行われている [7]。

本講演で示すアルゴリズムはこれらの結果の一般化である。先行研究では有限群での範囲でしか等分布函数（先行研究では，difference sum や intersection number，difference list などと呼ばれる）を計算できなかった。しかし，我々のこの一般化によって有限群よりも広い範囲で計算が可能になったことが主結果証明の決め手となっている。

3.3　所与の群による判定について

3.3.1　G_1 の判定

$G_1 := \left\langle x, y, z \mid y^3, x^5, z^8, xy(yx)^{-1}, zx(xz)^{-1}, zyz^{-1}y \right\rangle$ について，以下の部分群列 $H_0 > H_1 > \ldots > H_4$ を取る:

$$H_0 = G_1, \quad H_1 := \langle x, z \rangle, \quad H_2 := \langle z \rangle, \quad H_3 := \left\langle z^2 \right\rangle, \quad H_4 := 1.$$

この中で，H_1 と H_2 は正規部分群ではない。また，$\#H_1 := 40$，$\#H_2 := 8$，$\#H_3 := 4$ である。

このとき，前述のアルゴリズムを計算機を用いて計算すると，以下のことがわかる:

命題 9. アルゴリズムと同じ記号を使う。各 $\mathcal{D}_i$ の濃度は以下のとおり:

$$\#\mathcal{D}_0 = 1, \quad \#\mathcal{D}_1 = 3, \quad \#\mathcal{D}_2 = 45, \quad \#\mathcal{D}_3 = 0, \quad \#\mathcal{D}_4 = 0.$$

i.e., $\mathcal{D}_3 = \emptyset$ であり，アルゴリズムの実行結果は False になる。

3.3.2 G_3 の判定

$G_1 := \left\langle x, y, z \mid y^3, x^5, z^8, zyz^{-1}y, zxz^{-1}x, yx(xy)^{-1} \right\rangle$ について，以下の部分群列 $H_0 > H_1 > \ldots > H_4$ を取る:

$$H_0 = G_1, \quad H_1 := \langle x, z \rangle, \quad H_2 := \langle z \rangle, \quad H_3 := \left\langle z^2 \right\rangle, \quad H_4 := 1.$$

この中で，H_1 と H_2 は正規部分群ではない。また，$\#H_1 := 40$，$\#H_2 := 8$，$\#H_3 := 4$ である。

このとき，前述のアルゴリズムを計算機を用いて計算すると，以下のことがわかる:

命題 10. アルゴリズムと同じ記号を使う。各 $\mathcal{D}_i$ の濃度は以下のとおり:

$$\#\mathcal{D}_0 = 1, \quad \#\mathcal{D}_1 = 3, \quad \#\mathcal{D}_2 = 45, \quad \#\mathcal{D}_3 = 0, \quad \#\mathcal{D}_4 = 0.$$

i.e., $\mathcal{D}_2 = \emptyset$ であり，アルゴリズムの実行結果は False になる。

4 補題 8 の証明

4.1 証明の準備

(X_1, I_1, R_1)，(X_2, I_2, R_2) を unital regular relation paritition として，$k_0, \ldots, k_r$ を (X_1, I_1, R_1) の分岐指数，$l_0, \ldots, l_s$ を (X_2, I_2, R_2) の分岐指数，(θ, τ) を (X_1, I_1, R_1) から (X_2, I_2, R_2) への全射準同型とする。

t を $\mathbb{C}^{X_1}$ から $\mathbb{C}^{X_2}$ への線型写像としたときに，ℓ^2-内積に関する随伴 $t^\dagger : \mathbb{C}^{X_2} \longrightarrow \mathbb{C}^{X_1}$ を以下で定義する:

$$(f_Y | t(f_X))_{X_2} = (t^\dagger(f_Y) | f_X)_{X_1} \quad \text{for any } f_1 \in \mathbb{C}^{X_1},\ f_2 \in \mathbb{C}^{X_2}.$$

簡単な計算で任意の線型写像に対して随伴が存在することがわかる。

また，$\{A_i\}_{i\in I_1}$ を (X_1, I_1, R_1) の隣接行列全体 $\{B_i\}_{i'\in I_2}$ を (X_2, I_2, R_2) の隣接行列全体とする。このとき，以下が成り立つ:

命題 11. 任意の $\beta \in I_2$ に対して，$\theta^\dagger B_\beta \theta = \sum_{\alpha\in\tau^{-1}(\beta)} A_\alpha$ が成り立つ。

証明) $x \in X$ の特性函数を $\delta_x \in \mathbb{Z}^X$ とする。任意の $x_1, x_2 \in X$ に対して一致することを示す。左辺を実際に計算すると，以下が成り立つ:

$$\begin{aligned}((\theta^\dagger B_\beta\theta)\delta_{x_1}|\delta_{x_2})_{X_1} &= (B_\beta\theta(\delta_{x_1})|\theta(\delta_{x_2}))_{X_2} = (B_\beta\delta_{t(x_1)}|\delta_{\theta(x_2)})_{X_2}\\ &= \sum_{y\in X_2}(B_\beta\delta_{\theta(x_1)})(y)\overline{\delta_{\theta(x_2)}(y)} = \sum_{R_2(y_1,y_2)=\beta}\delta_{\theta(x_1)}(y_1)\delta_{\theta(x_2)}(y_2)\\ &= \begin{cases} 1 & R_1(\theta(x_1),\theta(x_2))\in\tau^{-1}(\beta)\\ 0 & \text{otherwise}\end{cases}.\end{aligned}$$

また，(t, τ) が準同型であることから右辺について以下がわかる:

$$\left(\sum_{i\in\tau^{-1}(i')} A_i\delta_{x_1}, \delta_{x_2}\right)_{X_1} = \begin{cases} 1 & R_1(\theta(x_1),\theta(x_2))\in\tau^{-1}(\beta)\\ 0 & \text{otherwise}\end{cases}$$

よって両辺が等しいことが示された。 (証明了)

次に，以下の命題を用意する:

命題 12. 任意の $y \in Y$ に対して，$\#t^{-1}(y) = \#X/\#Y$。

証明) (θ, τ) が unital relation partition 間の準同型であることから以下が成り立つ:

$$\theta(x_1) = \theta(x_2) \Longleftrightarrow (\theta(x_1),\theta(x_2)) \in S_0 \Longleftrightarrow (x_1, x_2) \in \sqcup_{\alpha\in\tau^{-1}(i_0^2)} R^{-1}(\alpha) \quad (x_1, x_2 \in X_1).$$

上から，任意の $y \in X_2$ に対して $x \in \theta^{-1}(y)$ をひとつ固定すると，以下が成り立つ:

$$\begin{aligned}\theta^{-1}(y) &= \{z \in X \mid \theta(z) = y\} = \{z \in X \mid (x, z) \in \sqcup_{\alpha\in\tau^{-1}(i_0^2)} R_1^{-1}(\alpha)\}\\ &= \bigsqcup_{\alpha\in\tau^{-1}(i_0^2)} \{z \in X \mid (x, z) \in R_1^{-1}(\alpha)\}\end{aligned}$$

(X_1, I_1, R_1) が regular であることから，右辺の濃度は $x \in X_1$ の取り方によらない。よって，任意の $y \in X_2$ で $t^{-1}(y)$ が定数であることが示される。

$\#t^{-1}(y) = \#X/\#Y$ は，$\sqcup_{y\in X_2} t^{-1}(y) = \#X$ からすぐに確認できる。 (証明了)

上の命題から直ちに以下が示される:

命題 13. 任意の $\beta \in \{0, \ldots, s\}$ に対して，$l_\beta(\#X/\#Y) = \sum_{\alpha \in \tau^{-1}(\beta)} k_\alpha$。

証明) (θ, τ) が準同型より以下が成り立つ:

$$(t \times t)^{-1}(R_2^{-1}(\beta)) = \bigsqcup_{\alpha \in \tau^{-1}(i_0^2)} R_1^{-1}(\alpha) \quad \text{for any } \beta \in \{0, \ldots, s\}.$$

両辺の濃度を実際に計算すると，前述の命題から以下が言えて成り立つ:

$$\#(t \times t)^{-1}(R_2^{-1}(\beta)) = \sum_{x \in X_1} \left(\sum_{R_2(\theta(x), y) = \beta} \#\theta^{-1}(y) \right) = \#X_1 l_\beta(\#X_1/\#X_2),$$
$$\# \bigsqcup_{i \in \tau^{-1}(i')} R_i = \#X_1 \sum_{\alpha \in \tau^{-1}(\beta)} k_\alpha.$$

(証明了)

4.2 補題 8 の証明

任意の $(\#X_1, k, \lambda)$-等分布函数 f に対して，$\theta_*(f)$ が $(\#X_2, k, \lambda \#X_1/\#X_2)$-等分布函数であることを示す。

任意の $i' \in \{1, \ldots s\}$ をとる。命題 11 より

$$(B_\beta \theta(f) | \theta(f))_{X_2} = ((\theta^\dagger B_\beta \theta) f | f)_{X_1} = \sum_{\alpha \in \tau^{-1}(\beta)} (A_\alpha f | f)_{X_1}$$

となる。f は等分布函数なので，$(A_\alpha f | f)_{X_1} = \lambda k_i$ より，

$$\sum_{\alpha \in \tau^{-1}(\beta)} (A_\alpha f | f)_{X_1} = \lambda \sum_{\alpha \in \tau^{-1}(\beta)} k_\alpha$$

となり，命題 13 と合わせると

$$(B_\beta \theta(f) | \theta(f))_{X_2} = \lambda (\#X/\#Y) l_\beta$$

より，f は $(\#X_2, k, \lambda \#X_1/\#X_2)$-等分布函数である。

参考文献

[1] Bruck, R. Hubert, *Difference sets in a finite group*, 1995, Trans. Amer. Math. Soc.

[2] *GAP - Groups, Algorithms, Programming -a System for Computational Discrete Algebra*, `https://www.gap-system.org/`, 2021/10/15 閲覧.

[3] Hiroki Kajiura, Makoto, Matsumoto, Takayuki Okuda, *A generalization of Bruck's condition pre-difference sets and equi distributed functions in association schemes*, 2020, preprint.

[4] J. H. van Lint, R. M. Wilson, *A Course in Combinatorics (2nd)*, 2001, Cambridge University Press,

[5] Paul E. Becker, *Investigation of Solvable (120, 35, 10) Difference Sets*, 2004, Wiley InterScience.

[6] Robert E. Kibler, *A summary of noncyclic difference sets, $k < 20$*, J. Combinatorial Theory Ser, 1978.

[7] Dylan Peifer, *DifSets, an algorithm for enumerating all difference sets in a group*, Version 2.3.1, 2019, `https://dylanpeifer.github.io/difsets.`, 2021/10/15 閲覧.