

ある association scheme 的の視点による difference set の一般化について

広島大学大学院 理学研究科 数学専攻 梶浦大起 (Hiroki Kajiura)*

Hiroki Kajiura
Department of Mathematics
Graduate School of Science
Hiroshima University

1 導入

本稿の目的は、筆者が導入した「difference set」に関する association scheme 的な視点による一般化（本稿では、「association scheme 上の difference set」と呼ぶことにする）について、ふたつの結果を紹介することである。

結果 1 **Schurian** association scheme について、association scheme 上の difference set と block design の関係

結果 2 **可換** association scheme について、「ある重み付き関数空間上の積分を近似する部分集合」と association scheme 上の difference set の関係

注意 このふたつの結果は斜体で示しているように association scheme に課す条件が全く異なっている。前者は可移な群作用から作られる association scheme であること、後者は association scheme に付随する Bose-Mesner 代数が可換であることを指している。 (注意了)

本稿では、まず最初によく知られている有限群上の difference set の古典的な結

* Email: hikajiura@hiroshima-u.ac.jp

果や association scheme の基本的な知識についてまとめ、その後「association scheme 上の difference set」の定義を示してから結果を紹介する。

また、本稿では特に断りがない限り以下のような記号を用いる：

G : 有限群 (e を単位元とする), 特に断 りがなければ X に推移的に作用 しているものとしても扱う,	$\mathfrak{X} := (X, I, R)$: association scheme,
X : 有限集合,	$X^{(k)} := \{B \subset X \mid \#B = k\}$,
I : 基点 i_0 付有限集合,	$Y \subset X, GY := \{g \cdot Y \mid g \in G\}$,
$R: X \times X \longrightarrow I$,	$\Lambda_T(\mathcal{B}) := \{B \in \mathcal{B} \mid T \subset B\}$,
	k_i : $i \in I$ の分岐指数,

2 準備

2.1 古典的 difference set に関する予備知識

本稿では、これまで一般的によく知られていた difference set を古典的 difference set と呼ぶことにする。最初に、古典的 difference set に対して定義や基本的な例、重要な性質について述べる。

最初に古典的 difference set の定義について述べる。

定義 1 (古典的 difference set). G の空でない真部分集合 Y が difference set である $:\iff \exists l \in \mathbb{N}$ s.t. $\forall a \in G \setminus \{e\}, l = \#\{(x, y) \in Y \times Y \mid x^{-1}y = a\}$ となること。

例 2. $G := \mathbb{Z}/7\mathbb{Z}$ として, $Y := \{0, 1, 3\} \subset G$ とすると Y は difference set である。(例了)

(古典的な) difference set は、古くは Bose がアーベル群を用いて「対称釣合型不完備配置」(以下対称 BIBD, 後に定義を述べる)を構成するためのテクニックとして示したもの(詳しくは [2]などを参照)が知られており, Bruck が「有限群 G が推移的に作用する l -平面^{*1}は G の(古典的な) difference set から構成できる」と

^{*1} l -平面の定義は有限集合 X の k 点部分集合族の部分集合であり, 2つの異なる元(これを線と呼ぶ)の選び方によらず交点の数が一定であることを満たす [5]。ここでは詳しくは述べないが, λ -平面は対称 BIBD となることが知られている。

言う主張によって一般化を行った ([5] を参照)。本節の残りでは、 λ -平面と言う用語を用いず直接的に (古典的な) difference set と block design の関係を述べる。

まず最初に block design の定義を述べる。

定義 3 (t -design). 空でない $\mathcal{B} \subset X^{(k)}$ が t -design である

$:\iff \exists \lambda \in \mathbb{N} \text{ s.t. } \forall T \subset X^{(t)}, \# \Lambda_T(\mathcal{B}) = \lambda \text{ となること。}$

ただし, $T, M \subset X$ に対して, $\Lambda_T(M) = \{B \in \mathcal{B} \mid T \subset B\}$ である。

例 4. $X := \mathbb{Z}/7\mathbb{Z}$ とする。このとき, 以下の部分集合族は 2-design

$$\mathcal{B} := \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{0, 4, 5\}, \{1, 5, 6\}, \{0, 2, 6\}\}.$$

(例了)

特に, $\mathcal{B}$ が非自明 (i.e., k が 1 でも $\#X - 1$ でもない場合) かつ $t = 2$ の場合を釣合型不完備配置 (以下, BIBD), 更に $\#\mathcal{B} = \#X$ の場合を対称^{*2} design と呼ぶ。

そして, (古典的な) difference set と BIBD の間には次のような有名な関係が知られている [5]:

事実 5. 有限群 G の部分集合 D に対して次は同値である:

#1 D が (古典的な) difference set である,

#2 $\mathcal{B} := \{Dg \mid g \in G\}$ が対称 BIBD である。

ただし, $Dg := \{dg \in G \mid d \in D\}$ とする。

この結果は, 対称 BIBD を構成するためには, difference set を構成すれば良いことがわかる非常に重要な結果であり, ここから様々な difference set の構成法などが研究されている。

^{*2} Fisher の不等式という古くから知られている有名な不等式によって, $t = 2$ の場合は $\#\mathcal{B} \geq \#X$ が知られている。よって, 対称な 2-design は Fisher の不等式の下界を達成する「良い」design であると言える。

2.2 Association scheme に関する予備知識

本稿では, association scheme の定義を紹介し, かつその具体例や本論文で必要な性質などをいくつか紹介する。より興味がある場合などは [1] などを参照して欲しい。

最初に association scheme の歴史的経緯を簡単に述べる。association scheme は元々, BIBD (前節参照) などの一般化として「部分的釣合型不完備配置」(以下 PBIBD) を研究するために土台として [3] によってコンセプトが示され [4] によって association scheme と名付けられた^{*3}。

これから association scheme の定義と基本的な例を述べる:

定義 6 (association scheme). $\mathfrak{X} := (X, I, R)$ が association scheme である $:\Longleftrightarrow$

- #1 $R^{-1}(i_0) = \{(x, x) \in X \times X \mid x \in X\}$,
- #2 $\forall i \in I, \exists i^* \in I \text{ s.t. } R^{-1}(i^*) = \{(y, x) \in X \times X \mid R(x, y) = i\}$,
- #3 $\forall i, j, k \in I, \exists p_{i,j}^k \in \mathbb{Z} \text{ s.t. } \forall (x, y) \in R^{-1}(i), p_{i,j}^k = \#(S_i(x) \cap S_j^*(y))$.

ここで, $S_i(x) = \{z \in X \mid R(x, z) = i\}$ とする。また, $k_i := \#S_i(x)$ を i の分岐指数と呼ぶ (これは x のとり方によらない)。

例 7.

- #1 $X := G, I := G, i_0 := e$ として R を次のように定めた association scheme は G から誘導される thin scheme $\mathfrak{T}_G$ と呼ぶ:

$$R(x, y) := x^{-1}y.$$

- #2 V を v 点集合とする。 $X := V^{(d)}, I = \{0, \dots, d\}, i_0 := 0$ として R を次のように定めた association scheme は Johnson scheme $J(v, d)$ と呼ぶ:

$$R(x, y) := d - \#(x \cap y).$$

(例了)

^{*3} ここで定義されているものは, 現在では対称 association scheme と呼ばれる特殊な場合である。

2.3 Schurian scheme

特に, association scheme の重要なクラスとして, 有限群 G が X に推移的に作用している場合は広く知られている。本稿においても結果 1 の中心的題材であるので定義を紹介する:

定義 8 (Schurian scheme). G が X に推移的に作用としてとする。このとき, $I := G \backslash X \times X = \{G(x, y) \mid x, y \in X\}$, $i_0 := G(x, x)$ として R を次のように定めた association scheme を Schurian scheme と呼ぶ:

$$R(x, y) := G(x, y) = \{(g \cdot x, g \cdot y) \in X \times X \mid g \in G\}.$$

例 9.

#1 thin scheme $\mathfrak{T}_G$ は, $X = G$ に G を次のように作用させる Schurian scheme と同型である:

$$g \cdot x := gx \quad (g \in G, x \in X).$$

#2 Johnson scheme $J(v, d)$ は, $X = V^{(m)}$ に $G := \mathfrak{S}_V$ を次のように作用させる Schurian scheme と同型である:

$$g \cdot x := x^g = \{g(a) \mid a \in x\} \quad (g \in \mathfrak{S}_V, x \in X).$$

(例了)

2.4 可換 association scheme

この節では, もうひとつ重要なクラスである可換 association scheme について述べる。その前に, 準備として以下を述べる:

定義 10 (Bose-Mesner 代数). $\mathfrak{X} := (X, I, R)$ を association scheme とする。このとき, $\mathfrak{X}$ に付随する Bose-Mesner 代数 $\mathcal{A}$ とは, 以下で定義される $\mathbb{C}^{X \times X}$ の部分線型空間である:

$$\mathcal{A} := \bigoplus_{i \in I} \mathbb{C} A_i \subset \mathbb{C}^{X \times X}.$$

ただし, $A_i(x, y) := \begin{cases} 1 & R(x, y) = i \\ 0 & R(x, y) \neq i \end{cases}$ と定義される行列である。

命題 11. Bose-Mesner 代数 $\mathcal{A}$ は,

#1 行列積とアダマール積で閉じる。行列積とアダマール積はそれぞれ以下で定義される:

$$(AB)(x, y) := \sum_{z \in X} A(x, z)B(z, y), \quad (A \circ B)(x, y) := A(x, y)B(x, y).$$

#2 $\mathcal{A}$ は複素共役と転置で閉じている。

定義 12 (可換 association scheme). Bose-Mesner 代数 $\mathcal{A}$ が可換であるとき, $\mathfrak{A}$ を可換 association scheme と呼ぶ。

特に $\mathcal{A}$ は自然に $\mathbb{C}^X$ に作用している。また, $\mathcal{A}$ が可換な場合は, $\mathbb{C}^X$ は $\mathcal{A}$ に関して同時固有空間分解をもっている。このときの分解を添字集合 J を使って

$$\mathbb{C}^X = \bigoplus_{j \in J} H_j$$

と書ける。ただし, $j_0 \in J$ で $H_{j_0} = \{\text{定数関数}\}$ とする。特に ℓ^2 -内積 $(f, g) = \sum_{z \in X} f(z)\overline{g(z)}$ を考えればこれは直交分解である。

いま, E_j を $\mathbb{C}^X$ から H_j への直交射影とする。このとき, 次が言える:

命題 13. 以下が成り立つ:

$$\mathcal{A} = \bigoplus_{j \in J} \mathbb{C}E_j$$

特に, $\#I = \#J$ である。

注意) $\{A_i\}_{i \in I}$ はアダマール積に関する原始冪等元全体, $\{E_j\}_{j \in J}$ は行列積に関する原始冪等元全体と一致する。 (注意了)

3 Association scheme 上の difference set

本稿では, difference set の association scheme 的な視点によるひとつの一般化を「association scheme 上の difference set」と呼ぶ。この節では, association scheme 上の difference set の定義とその性質について幾つか述べる:

定義 14 (Association scheme 上の difference set). 真部分集合 $Y \subset X$ が $\mathfrak{A}$ 上の

difference set である

$$:\Leftrightarrow \exists l \in \mathbb{Q} \text{ s.t. } \forall i \in I \setminus \{i_0\}, \#((Y \times Y) \cap R_i)/k_i = l \text{ となること。}$$

注意) 例 7#1 で定義された thin scheme において, 古典的な difference set であることと, association scheme 上の difference set であることは同値である。(注意了)

例 15.

#1 例 7#1 で定義された有限群 G の thin scheme $\mathfrak{T}_G$ について, 古典的な G 上の difference set であることと, $\mathfrak{T}_G$ 上の difference set であることが同値である。

#2 $V = \{0, \dots, 4\}$ とする。例 7#2 で定義された $J(5, 2)$ について, 以下は $J(5, 2)$ 上の difference set:

$$\{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 0\}\}.$$

より一般に, v が 6 以上の正の整数として, $V = \{0, \dots, v-1\}$ としたときに以下の N 角形は $J(2N-3, 2)$ 上の difference set である:

$$\{\{0, 1\}, \{1, 2\}, \dots, \{N-1, 0\}\}$$

(例了)

また, 古典的な difference set と同様に以下が成り立つ:

命題 16. $\mathfrak{X} = (X, I, R)$ が association scheme, $Y \subset X$ を $\mathfrak{X}$ 上の difference set とする。このとき以下が成り立つ:

#1 1 点集合と $\#X - 1$ 点集合は常に $\mathfrak{X}$ 上の difference set。

#2 Y の補集合も $\mathfrak{X}$ 上の difference set。

$$\#3 \frac{\#((Y \times Y) \cap R_i)}{k_i} = \frac{\#Y(\#Y - 1)}{\#X - 1}.$$

注意) 古典的な場合と異なり, association scheme 上の difference set について, $\#((Y \times Y) \cap R_i)/k_i$ は必ずしも自然数になるとは限らない。例 15#2 の $J(5, 2)$ 上の difference set は実際 $\#Y(\#Y - 1)/(\#X - 1) = 3/2$ となり自然数ではない。ただし, i_0 以外の i について, k_i たちが互いに素であれば常に自然数になる。(注意了)

4 結果 1; Schurian scheme 上の difference set と block design

本節では Schurian scheme と block design との関係に関する定理を述べ証明する。証明の後に、具体例を書き紹介する。

定理 17. $\mathfrak{X} = (X, I, R)$ を Schurian scheme とする。真部分集合 $Y \subset X$ について、以下は同値:

- #1 Y は $\mathfrak{X}$ 上の difference set である (i.e., 任意の $i \in I \setminus \{i_0\}$ に対して $\#((Y \times Y) \cap R_i)/k_i$ が一定),
- #2 $GY := \{g \cdot Y \mid g \in G\}$ は BIBD である (i.e., 任意の $T \in X^{(2)}$ に対して, $\#\Lambda_T(GY)$ が一定)。

定理の証明は, $\#\text{Stab}_G(a)$ が a の取り方に依らないことに注意すると, 次の補題を示すことで完了する:

補題 18. 任意の $i \in I \setminus \{i_0\}$ と $T \in X^{(2)}$ に対して以下が成り立つ:

$$\#\Lambda_T(GY) = \frac{\#((Y \times Y) \cap R_i)}{k_i} \frac{\#\text{Stab}_G(a)}{\#\text{Stab}_G(Y)}$$

補題証明の概略を述べる。 $a, b \in X$ を固定し, $i := R(a, b)$ として次の写像を定める:

$$\phi_Y : G \ni g \mapsto g \cdot Y \in X^{(m)}, \quad \varphi_i : G \ni g \mapsto (g \cdot a, g \cdot b) \in R^{-1}(i) \subset X \times X.$$

このとき, このふたつの写像はそれぞれ, 各点のファイバーの濃度が一定である。それを使うと次の性質から示せるので, それらを組み合わせることで証明が完了する:

- #1 $\#\Lambda_{\{a,b\}}(GY) = \#\{g \in G \mid (a, b) \in g^{-1} \cdot Y \times g^{-1} \cdot Y\} / \#\text{Stab}_G(Y),$
- #2 $\#\{g \in G \mid (a, b) \in g \cdot Y \times g \cdot Y\} / \#(\text{Stab}_G(a) \cap \text{Stab}_G(b)) = \#((Y \times Y) \cap R_i),$
- #3 $\#\text{Stab}_G(a) / \#(\text{Stab}_G(a) \cap \text{Stab}_G(b)) = \#S_i(a) = k_i.$

注意) 補題からわかる通り, この BIBD が対称になるためには $\#\text{Stab}_G(a) = \#\text{Stab}_G(Y)$ である必要がある。しかしながら, 現在のところ筆者はそうなる

Schurian association scheme の例を発見できていない。(注意了)

例 19. 例 15#2 で定義した, $J(2N-3, 2)$ 上の N 角形 $Y := \{\{0, 1\}, \dots, \{N-1, 0\}\}$ について考える。

$$\# \text{Stab}_G a = (n-2)!, \quad \# \text{Stab}_G Y = n \times (n-3)!$$

となり, 対称 2-design にはならないことがわかる。(例了)

5 結果 2; 可換 association scheme 上の difference set と 積分誤差評価

この節では, ある種の (Bose-Mesner 代数に基づいて導入した人工的な) 重み付きの変動を持つ関数空間における「積分近似」を考えると「最も良い近似をする部分集合」が difference set であることを示す。この結果は, 古くからよく知られている可換群の difference set と指標の関係に関する Turyn の結果 [7] の一般化となっている。

また, この節の結果はより詳しく [6] に記載されている。

5.1 quasi-Monte Carlo(QMC) 積分

この節では, まず最初にこの結果の動機となる quasi-Monte Carlo(QMC) について述べる。より詳しいことは QMC とは数値積分法の一分野である。非常にラフに概略を述べる。

今, s 次元超立方体 $[0, 1]^s$ 上の関数空間 $\mathcal{H}$ を考える。このとき, 我々は $\mathcal{H}$ 上の関数 f の積分 $\int_{[0, 1]^s} f(x) dx$ を計算したい。このときに, $[0, 1]^s$ の有限部分集合 Y での平均, すなわち $(1/\#Y) \sum_{x \in Y} f(x)$ で近似することを考える。QMC とは, このような問題設定下で, $\mathcal{H}$ 上の関数について積分誤差を小さくする部分集合 Y を構成せよ, というのが主題である。

部分集合 Y を探すにあたって, 以下のような定理が古典的によく知られている:

定理 20 (Koksma-Hlawka の不等式). $\mathcal{H} := \{[0, 1]^s \text{ 上の有界変動関数}\}$ とする。こ

のとき、有限部分集合 $Y \subset [0, 1]^s$ について以下が成り立つ:

$$\left| \int_{[0,1]^s} f(x) dx - \frac{1}{\#Y} \sum_{x \in Y} f(x) \right| \leq V(f) D^*(Y).$$

ここで、 $V(f)$ は「(Hardy and Krause の) 全変動」、 D^* は「star-Discrepancy」である。

この定理を踏まえれば、 $D^*(Y)$ が小さくなるような部分集合 Y が「よく積分を近似する部分集合」と言うことになる。そこで、QMC では、この $D^*(Y)$ を小さくする部分集合を探すことが一種の目標となっている。

また、他の函数空間であったり、そもそも s 次元超立方体以外で QMC の類似を考えると、この Koksma-Hlawka の不等式の類似を考え、同様に研究することが多い。これから述べる内容も、その発想が原点にある。

5.2 可換 association scheme 上のある QMC 類似と difference set

(X, I, R) を可換 association scheme とする。前節の記号を使って述べるのであれば、次のような重み付き変動がある函数空間を考えよう:

函数の変動 本稿において変動 V は以下のように定義される:

$$V(f) := \sum_{j \in J \setminus \{j_0\}} \|E_j f\| \dim H_j.$$

ただし、 $\|f\| := \sum_{x \in X} f(x) \overline{f(x)}$ (すなわち ℓ^2 -ノルム)、 $H_j = E_j \mathbb{C}^X$ である。

函数空間 本稿では $\mathbb{C}^X$ が対象となる函数空間である。 X は有限集合なので、 $\mathbb{C}^X$ と有界変動函数の全体が一致する。

積分 $\int_X f(x) dx = (1/\#X) \sum_{x \in X} f(x)$ とする。

上記の設定では、以下のようにして Koksma-Hlawka 型の不等式の類似が示される:

定理 21 ([6, Theorem 5.1]). $f \in \mathbb{C}^X$ と $Y \subset X$ について, 以下が成り立つ:

$$\left| \frac{1}{\#X} \sum_{x \in X} f(x) - \frac{1}{\#Y} \sum_{x \in Y} f(x) \right| \leq V(f) \partial(Y).$$

ここで, $\partial(Y)$ は以下で定義される:

$$\partial(Y) := \max_{j \in J \setminus \{j_0\}} \sqrt{\frac{1/\dim H_j}{\#Y^2} \sum_{x, y \in Y} E_j(x, y)}.$$

$\partial(Y)$ が前節での star-discrepancy にあたる存在である。そして, 次に $\partial(Y)$ の下界の評価と difference set の関係について述べる:

定理 22 ([6, Theorem 5.15.]). $Y \subset X$ について, 以下が成り立つ:

$$\partial(Y) \geq \sqrt{\frac{1/\#Y - 1/\#X}{\#X - 1}}$$

特に等号が達成することと, Y が $\mathfrak{X}$ 上の difference set であることと同値である。

注意) 例 7#1 の有限群 G に関する thin scheme の場合について述べる。thin scheme が可換 association scheme であることと, G が可換群であることは同値である。そして, 可換群である場合は, E_j たちは G の既約指標に対応する (E_{j_0} は自明表現と対応する)。

この場合に等号が達成する条件を書き下せば, 実際 Turyn の結果 [7] と一致することがわかる。 (注意了)

最後にこれらの結果をまとめると, difference set を「最良の近似を行う部分集合」にするような (人工的ではあるが) Bose-Mesner 代数による変動を定義することができると言える。

参考文献

- [1] 坂内 英一, 坂内 悦子, 伊藤 達郎, 『代数的組合せ論入門』, 共立出版, 2016,
- [2] Bose, R.C., *On the construction of balanced incomplete block designs*, Annals of Eugenics, 1939,

- [3] Bose, R. C., Nair, K. R., *Partially balanced incomplete block designs*, Sankhyā, 1939,
- [4] Bose, R. C., Shimamoto, T., *Classification and analysis of partially balanced incomplete block designs with two associate classes*, Journal of the American Statistical Association, 1952,
- [5] Bruck, R.H., *Difference sets in a finite group*, Transactions of the American Mathematical Society, 1955,
- [6] Kajiura, H., Matsumoto, M., Okuda, T., *Approximation of integration over finite groups, difference sets and association schemes*, 2019, preprint, arXiv:1903.00697
- [7] Turyn, J.R., *Character sums and difference sets*, Pacific journal of mathematics, 1965.