

アダマール 2 元ゲインの分類

イリノイ大学シカゴサークル 伊藤 昇

定義 $P = \{1, \dots, v\}$, また $B = \{\alpha_1, \dots, \alpha_r\}$ を P の r -部分集合の族とする. つぎの 2 条件が満足されるとき $D = (P, B)$ は対称 2- (v, r, λ) ゲインと呼ばれる:
 (1) $\forall a \in P$ についてきっかり r 個の α_i が a を含む.
 (2) $\forall a, b \in P, a \neq b$ についてきっかり λ 個の α_i が a, b を含む. P, B の元をそれぞれ D の点, ブロックと呼ぶ.
 $v = 4\lambda + 3, r = 2\lambda + 1$ のとき $D = D(\lambda)$ はアダマール 2 元ゲインと呼ばれる.

定義 対称 2 元ゲイン $D_1 = (P, B_1), D_2 = (P, B_2)$ は B_1 を B_2 にくつぎ置換を誘導する P 上の置換 σ が存在するとき同型という. $B = B_1 = B_2$ のとき σ は D の自己同型と呼ばれ, その全体が D の自己同型群 $G(D)$ を作る. $d(\lambda)$ は $D(\lambda)$ の同型類の個数を示す.

文献 [1] から $d(5) = 1102$ が示される. その過程で出て来たいくつかの事実, 問題について話したい. 分類のはじ

めの目安はつぎの概念である。

定義 $K(\alpha) = \#\{\beta, \gamma\} ; \beta \neq \gamma ; \alpha \cap \beta = \alpha \cap \gamma,$
 $\alpha, \beta, \gamma \in B$ で定義される B 上の関数を D の K 関数と呼ぶ。
 K 関数が異なる D_1, D_2 は同型でない。 $L(a) = \#\{b, c\} ; b \neq c ; a, b, c$ を含む λ 個の T ロックが存在する
 $a, b, c \in P$ で定義される P 上の関数を D の L 関数と呼ぶ。
 L 関数が異なる D_1, D_2 は同型でない。 L 関数は双対 (点, T ロックを交換して作られる T ギャイン) の K 関数である。

K 関数の効力についてはつぎのことを云えよう。 λ 偶数のときは無効である: $\lambda \equiv 3 \pmod{4}$ のときは複雑であり、組織的研究が待たれる: $\lambda \equiv 1 \pmod{4}$ のときは有効に使用される。

命題 1. λ が偶数ならば K 関数は零関数である。

証明. $\Delta = \alpha \cap \beta = \alpha \cap \gamma$ とすると $P = \alpha \cup \beta \cup \gamma$. それで $\delta \neq \alpha, \beta, \gamma$ について $x = |\Delta \cap \delta|$, $y = |(\alpha - \Delta) \cap \delta|$ とおくと, $x + y = \lambda$ (D の対称 2 ギャインから, 任意二つの T ロックの共通部分は λ -部分集合), $x + 3y = 2\lambda + 1$. したがって $2y = \lambda + 1$, $2x = \lambda - 1$ である。

命題 2. K 関数の値が λ ならば, D は $GF(2)$

上の射影幾何 (グロツフは超平面, $\lambda = 2^n - 1$) と同型である。

証明. 双対で見る. 2 点を含むグロツフ全部の共通部分をその 2 点で決定されるラインと呼ぶ. 仮定は任意のラインが 3 点からできていることを云っている. したがってライン $\{a, b, c\}$ と交わるグロツフの個数を数えると, a, b または c とだけ交わるのが $\lambda + 1$ 個ずつ, ラインを含むのが λ 個あるので, 任意のグロツフと交わる. Dembowski-Wagner の定理 [2, p. 67] によるとそれですみ.

注意. 以上二つの事実は [3] にある. 後者は Norman の定理である.

命題 3. $P = GF(q)$, $q \equiv 3 \pmod{4}$, $R = (GF(q)^{\times})^2$, $B = \{R + a, a \in GF(q)\}$ とし得られるアガマール 2 設計を平方剰余型と云う. 平方剰余型はもっとも興味のあるアガマール 2 設計である. さて平方剰余型では K 関数は零関数である.

証明. [4] による. $GF(q)$ の平方指標 $\chi: \chi(a)$ は $a = 0$, $a \in R$, $0 \neq a \notin R$ にしたがって $0, 1, -1$ である: を使う. この手法は平方剰余型のもっとも精密な性質をしらべるのにも有用であると思ふ. a, b, c を $GF(q)$ の異なる 3 元とする. $4 | R + a \cap R + b | = \sum_{x \in R} (1 + \chi(x+a))$.

$(1 + \chi(x+a)) + \varepsilon_2, 8 | R+a \cap R+b \cap R+c | =$
 $\sum_{x \in R} (1 + \chi(x+a)) (1 + \chi(x+b)) (1 + \chi(x+c))$
 $+ \varepsilon_3$, ここで $\varepsilon_2, \varepsilon_3$ は $x+a, x+b$ または $x+c$ が
 0 になるときの調整項で, a, b または a, b, c に依存す
 る. ここで $\sum_{x \in R} \chi(x+a)\chi(x+b) = -1$ は見易い. 大切な
 のは Weil 評価 $|\sum_{x \in R} \chi(x+a)\chi(x+b)\chi(x+c)| \leq 2\sqrt{q}$
 [5, p.43] である. それで $4 | R+a \cap R+b | \geq q -$
 $5, 8 | R+a \cap R+b \cap R+c | \leq q - 3 + 2\sqrt{q}$ が得られ
 る. $q \geq 17$ のときは前者の方が大きい. $q = 7, 11$ のと
 きは直接確かめる.

命題 4. $\lambda \equiv 1 \pmod{4}$ とする. $K(\alpha) \geq 3$ とする α の
 個数は高々 1 つで, 1 のときは $\forall \beta \neq \alpha$ について $K(\beta) \leq 1$
 . $\lambda = 5$ のときは上の 3 は 2 と出来るが, $\lambda > 5$ のときは未
 知である.

証明. $1^\circ \Gamma = \alpha \cap \beta = \alpha \cap \gamma$ (α, β, γ は相異), Δ
 $= \delta \cap \varepsilon = \delta \cap \xi$ (δ, ε, ξ は相異) とすると, $\{\alpha, \beta$
 $, \gamma\} \cap \{\delta, \varepsilon, \xi\} \neq \emptyset$ である. 否定して仮定すると,
 $\Delta = (\alpha \cap \Delta - \Gamma \cap \Delta) \oplus (\beta \cap \Delta - \Gamma \cap \Delta) \oplus (\gamma \cap \Delta -$
 $\Gamma \cap \Delta) \oplus (\Gamma \cap \Delta)$ で, $|\alpha \cap \Delta| = |\beta \cap \Delta| = |\gamma \cap$
 $\Delta| = \frac{\lambda-1}{2}$ は命題 1 の証で述べられているので, $\lambda = 3$ (
 $\frac{\lambda-1}{2} - |\Gamma \cap \Delta|) + |\Gamma \cap \Delta|$ から $|\Gamma \cap \Delta| = \frac{\lambda-3}{4}$.

$2^\circ \alpha \cap \beta = \alpha \cap \gamma, K(\alpha) > 1, K(\beta) > 1$ とする. $\alpha \cap \delta = \alpha \cap \varepsilon, \beta \cap \xi = \beta \cap \zeta, \{\beta, \gamma\} \cap \{\delta, \varepsilon\} = \emptyset, \{\alpha, \gamma\} \cap \{\xi, \zeta\} = \emptyset$ とし $\delta, \varepsilon, \xi, \zeta$ が存在する. 1° により $\zeta = \delta$ と仮定出来る. このとき $\gamma \cap \varepsilon = \gamma \cap \xi$ とする. したがって $K(\gamma) > 1$ である. まず 1° と仮定して $\varepsilon \cap \xi = (\alpha \cap \varepsilon \cap \xi - \Gamma \cap \varepsilon \cap \xi) \oplus (\beta \cap \varepsilon \cap \xi - \Gamma \cap \varepsilon \cap \xi) \oplus (\gamma \cap \varepsilon \cap \xi - \Gamma \cap \varepsilon \cap \xi) \oplus \Gamma \cap \varepsilon \cap \xi$, $\Gamma = \alpha \cap \beta$ である. $x = |\gamma \cap \varepsilon \cap \xi|, y = |\Gamma \cap \varepsilon \cap \xi|$ とおく. 1° と仮定して $x = 2y + 1$ を得る. \therefore $\alpha, \beta, \gamma, \delta, \varepsilon, \xi$ に含除原理 [6, p. 17] を使えば $x = y + \frac{\lambda+1}{2}$, せめて $x = \lambda, y = \frac{\lambda-1}{2}$ を得る.

$3^\circ 2^\circ$ にあると相異なる 67 "ボックス", $\alpha_1 \cap \alpha_2 = \alpha_1 \cap \alpha_3, \alpha_1 \cap \alpha_4 = \alpha_1 \cap \alpha_5, \alpha_2 \cap \alpha_4 = \alpha_2 \cap \alpha_6, \alpha_3 \cap \alpha_5 = \alpha_3 \cap \alpha_6$ を満足するものが存在する. $K(\alpha_i) \geq 3$ とすると, さしに $\alpha_1 \cap \alpha_6 = \alpha_1 \cap \alpha_7$, したがって $\alpha_2 \cap \alpha_5 = \alpha_2 \cap \alpha_7, \alpha_3 \cap \alpha_4 = \alpha_3 \cap \alpha_7$ も成立することを示される. さしに $\alpha_i (1 \leq i \leq 7)$ のどの 4 つの共通部分も一致することを示されるので, それを Γ とおく. $\beta \neq \alpha_i (1 \leq i \leq 7)$ をとり, $x_1 = |\beta \cap (\alpha_1 \cap \alpha_2 \cap \alpha_3 - \Gamma)|, x_2 = |\beta \cap \Gamma|, x_3 = |\beta \cap (\alpha_1 \cap \alpha_4 \cap \alpha_5 -$

$|\Gamma|$, $x_4 = |\beta \cap (\alpha_1 \cap \alpha_6 \cap \alpha_7 - \Gamma)|$, $x_5 = |\beta \cap (\alpha_2 \cap \alpha_4 \cap \alpha_6 - \Gamma)|$, $x_6 = |\beta \cap (\alpha_2 \cap \alpha_5 \cap \alpha_7 - \Gamma)|$, $x_7 = |\beta \cap (\alpha_3 \cap \alpha_4 \cap \alpha_7 - \Gamma)|$, $x_8 = |\beta \cap (\alpha_3 \cap \alpha_5 \cap \alpha_6 - \Gamma)|$ とおく. $x_1 + x_2 + x_3 + x_4 = x_1 + x_2 + x_5 + x_6 = x_1 + x_2 + x_7 + x_8 = \lambda$, $\sum_{i=1}^8 x_i = 2\lambda + 1$, $x_1 + x_2 = \frac{\lambda-1}{2} \times 5$, $x_2 + x_3 + x_5 + x_7 = x_2 + x_3 + x_6 + x_8 = x_2 + x_4 + x_5 + x_8 = x_2 + x_4 + x_6 + x_7 = \lambda$. ところで $x_3 + x_4 = x_5 + x_6 = x_7 + x_8$ とおくと, $x_1 + x_2 + a = \lambda$, $x_1 + x_2 + 3a = 2\lambda + 1$, $2a = \lambda + 1$. ところで $4x_2 + 6a = 4\lambda$, $4x_2 = \lambda - 3$ とおる.

$\bar{\Gamma} = 7$. 1102個の $2-(23, 11, 5)$ デザインについて, $k = \max_{\alpha \in B} K(\alpha)$ とおく. k の値による細分は次の通りである: $k = 11$ のもの 20, $k = 5$ のもの 108, $k = 3$ のもの 352, $k = 2$ のもの 510, $k = 1$ のもの 108, $k = 0$ のもの 4. 他方, $g = |G(D)|$ とおく. g の値による細分は次の通りである. $g = 660$ のもの 1, $g = 253$ のもの 1, $g = 60$ のもの 2, $g = 55$ のもの 2, $g = 12$ のもの 4, $g = 11$ のもの 1, $g = 6$ のもの 14, $g = 5$ のもの 10, $g = 4$ のもの 17, $g = 3$ のもの 35, $g = 2$ のもの 108, $g = 1$ のもの 907.

注意 このデータだけからみると、自明でない自己同型を持たないものの数が普通であると云えるが、一般の対称2デザインでも本当であるかどうかの追求に値すると思う。

つぎの概念はアダマール2デザインに特有のものである。

定義 $D = (P, B)$ をアダマール2デザインとする。 B から P への双射 T は (1) $T(\alpha) \notin \alpha$, $\alpha \in B$, (2) $T(\alpha) \in \beta \iff T(\beta) \in \alpha$, $\alpha, \beta \in B$, $\alpha \neq \beta$ を満足するとき T - T -メントと呼ばれる。

命題5. 平方剰余型のアダマール2デザインでは、 $T(R+a) = a$ とおくと、 T は T - T -メントになる。

証明. $q \equiv 3 \pmod{4}$ 系なので、 $\chi(-1) = -1$. それから条件(2)が出る。

注意. $q \geq 19$ のとき、上の T が唯一の T - T -メントのよりに思われる。

命題6. アダマール2デザイン $D = (P, B)$ がつぎの2条件を満足するとする: (1) 相異なる3つのブロック α, β, γ で $\alpha \cap \beta = \alpha \cap \gamma$ 系ものがある ($k(\alpha) \geq 1$). (2) 任意3点について、それらを含むブロックが存在する。そのとき D は T - T -メントを持たない。

証明. $P = \alpha \cup \beta \cup \gamma$ 系ので、 $T(\alpha), T(\beta), T(\gamma)$ を含むブロックを δ とすると、 $T(\delta)$ は α, β, γ のどれかに

属することによる。

したがって、

命題7. $GF(2)$ 上の射影幾何は、その次元が4以上ならばトーナメントを持たない。

注意. トーナメントについては、つぎの問題がとくに指適される。平す剰余型では $\alpha \rightarrow \alpha + a$, $a \in GF(q)$ が自己同型なので、自己同型群は P 上可移である。この逆、すまは P 上可移な自己同型群を持つアダマール2デザインがトーナメントを持てば、平す剰余型であるか？

ともなく分類ははじめられたばかりで、たとえば λ 偶数のときは、自己同型群と λ トーナメントとが位しぬ、その規準も知られていない。興味を持って頂ける人の出現を期待したい。

文献

1. Ito-Leon-Longyear, Classification of 3-(24, 12, 5) designs and 24-dimensional Hadamard matrices, JCTA (1981)
2. Dembowski, Finite geometries, Springer 1968.
3. Kimberley, On the construction of certain Hadamard designs, Math. Z. 119 (1971), 41-59.

4. Evans, Note on intersections of translates of powers in finite fields, Hokkaido Math. J. 9 (1980), 135 - 137.

5. Schmidt, Equations over finite fields, Springer 1976.

6. Ryser, Combinatorial mathematics, MAA 1963.