数理解析研究所講究録
第429巻 1981年 9-17

アダマール2デザインの分類

イリノイ大シカゴサークル 伊藤 昇

定義 $P=\{1,\cdots,v\}$，また $B=\{\alpha_1,\cdots,\alpha_v\}$ を P の k-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,k,λ)デザインと呼ばれる：(1) $\forall a\in P$ についてきっかり k 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．$v=4\lambda+3$，$k=2\lambda+1$ のとき $D=D(\lambda)$ はアダマール2デザインと呼ばれる．

定義 対称2デザイン $D_1=(P,B_1)$，$D_2=(P,B_2)$ は B_1 を B_2 にうつす置換を誘導する 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．$d(\lambda)$ で $D(\lambda)$ 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 個のブロックが存在する，$a,b,c\in P$ 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，ブロックを交換して作られるデザイン）の K 関数である．

K 関数の効力についてはつぎのことが云えよう．λ 偶数のときは無力である：$\lambda\equiv 3 \pmod 4$ のときは複雑であり，組織的な研究が待たれる：$\lambda\equiv 1 \pmod 4$ 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 が対称2デザインだから，任意二つのブ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 関数の値がつねに $2\lambda+1$ ならば，D は $GF(2)$

上の射影幾何（ブロックは超平面，$\lambda = 2^n - 1$）と同型である．

証明．双対で見る．2点を含むブロック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}と交わるブロックの個数を数えると，a, bまたはcとだけ交わるのが $\lambda+1$ 個づつ，ラインを含むのが λ 個あるので，任意のブロックと交わる．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．$P = GF(q)$，$q \equiv 3 \pmod 4$，$R = (GF(q)^\times)^2$，$B = \{R + a,\ a \in GF(q)\}$として得られるアダマール2デザイン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ダマール2デザインである．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 χ：$\chi(a)$ は $a = 0$，$a \in R$，$0 \neq a \notin R$ にしたがい0，1，−1である：を使う．この方法は平方剰余型のもっと精密な性質をしらべるのにも有用であると思う．a, b, cを$GF(q)$の異なる3元とする．$4|R+a \cap R+b| = \sum_{x \in R} (1+\chi(x+a))\cdot$

$(1+\chi(x+b))+\varepsilon_2$, $8|R+a\cap R+b\cap R+c| = \sum_{x\in R}(1+\chi(x+a))(1+\chi(x+b))(1+\chi(x+c)) + \varepsilon_3$, ここで ε_2, ε_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 $\left|\sum_{x\in R}\chi(x+a)\chi(x+b)\chi(x+c)\right| \leq 2\sqrt{q}$ [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. $K(\alpha)\geq 3$ となる 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° $\Gamma=\alpha\cap\beta=\alpha\cap\gamma$ (α, β, γ は相異), $\Delta=\delta\cap\varepsilon=\delta\cap\xi$ (δ, ε, ξ は相異) とすると, $\{\alpha,\beta,\gamma\}\cap\{\delta,\varepsilon,\xi\}\neq\emptyset$ である. 否定してみると, $\Delta=(\alpha\cap\Delta-\Gamma\cap\Delta)\oplus(\beta\cap\Delta-\Gamma\cap\Delta)\oplus(\gamma\cap\Delta-\Gamma\cap\Delta)\oplus(\Gamma\cap\Delta)$ で, $|\alpha\cap\Delta|=|\beta\cap\Delta|=|\gamma\cap\Delta|=\frac{\lambda-1}{2}$ が命題1の証でわかっているので, $\lambda=3\left(\frac{\lambda-1}{2}-|\Gamma\cap\Delta|\right)+|\Gamma\cap\Delta|$ から $|\Gamma\cap\Delta|=\frac{\lambda-3}{4}$.

2° $\alpha \cap \beta = \alpha \cap \gamma$, $K(\alpha) > 1$, $K(\beta) > 1$ とする. $\alpha \cap \delta = \alpha \cap \varepsilon$, $\beta \cap \xi = \beta \cap \zeta$, $\{\beta, \gamma\} \cap \{\delta, \varepsilon\} = \emptyset$, $\{\alpha, \gamma\} \cap \{\xi, \zeta\} = \emptyset$ という δ, ε, ξ, ζ が存在する. 1° により $\zeta = \delta$ と仮定出来る. このとき $\gamma \cap \varepsilon = \gamma \cap \xi$ となる. したがって $K(\gamma) > 1$ である. まず 1° とおなじく $\varepsilon \cap \xi = (\alpha \cap \varepsilon \cap \xi - \Gamma \cap \varepsilon \cap \xi) \oplus (\beta \cap \varepsilon \cap \xi - \Gamma \cap \varepsilon \cap \xi) \oplus (\gamma \cap \varepsilon \cap \xi - \Gamma \cap \varepsilon \cap \xi) \oplus \Gamma \cap \varepsilon \cap \xi$, $\Gamma = \alpha \cap \beta$ である. $x = |\gamma \cap \varepsilon \cap \xi|$, $y = |\Gamma \cap \varepsilon \cap \xi|$ とおく. 1° とおなじくすると $x = 2y + 1$ を得る. つぎに $\mathfrak{P} \supset \alpha, \beta, \gamma, \delta, \varepsilon, \xi$ に含除原理 [6, p. 17] を使うと $x = y + \frac{\lambda + 1}{2}$, それで $x = \lambda$, $y = \frac{\lambda - 1}{2}$ を得る.

3° 2° によると相異る 6 ブロックで, $\alpha_1 \cap \alpha_2 = \alpha_1 \cap \alpha_3$, $\alpha_1 \cap \alpha_4 = \alpha_1 \cap \alpha_5$, $\alpha_2 \cap \alpha_4 = \alpha_2 \cap \alpha_6$, $\alpha_3 \cap \alpha_5 = \alpha_3 \cap \alpha_6$ を満足するのが存在する. $K(\alpha_1) \geqq 3$ とすると, さらに $\alpha_1 \cap \alpha_6 = \alpha_1 \cap \alpha_7$, したがって $\alpha_2 \cap \alpha_5 = \alpha_2 \cap \alpha_7$, $\alpha_3 \cap \alpha_4 = \alpha_3 \cap \alpha_7$ も成立つことがわかる. さらに α_i $(1 \leqq i \leqq 7)$ のどの 4 つの共通部分も一致することがわかるので, それを Γ とおく. $\beta \neq \alpha_i$ $(1 \leqq i \leqq 7)$ 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. $x_1+x_2+x_3+x_4=x_1+x_2+x_5+x_6=x_1+x_2+x_7+x_8=\lambda$, $\sum_{i=1}^{8}x_i=2\lambda+1$, $x_1+x_2=\frac{\lambda-1}{2}$ から, $x_2+x_3+x_5+x_7=x_2+x_3+x_6+x_8=x_2+x_4+x_5+x_8=x_2+x_4+x_6+x_7=\lambda$. それで $x_3+x_4=x_5+x_6=x_7+x_8$ となので, これを a とおくと, $x_1+x_2+a=\lambda$, $x_1+x_2+3a=2\lambda+1$, $2a=\lambda+1$. それで $4x_2+6a=4\lambda$, $4x_2=\lambda-3$ となる.

データ. 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方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) $T(\alpha)\in\beta\longleftrightarrow T(\beta)\in\alpha$, $\alpha, \beta\in B$, $\alpha\neq\beta$を満足するときトーナメントと呼ばれる．

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はトーナメントになる．

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

注意．$q\geqq 19$のとき，上のTが唯一のトーナメントのように思はれる．

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ブロックα, β, γで$\alpha\cap\beta=\alpha\cap\gamma$なものがある$(k(\alpha)\geqq 1)$．(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はトーナメントを持たない．

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

属することになる．

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．平方剰余型では $x \to x + a$, $a \in GF(q)$ が自己同型なので，自己同型群は P上可移である．この逆，すなわち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，平方剰余型である？

ともか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，自己同型群とかトーナメントとか位しか，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.