

《科学研究費補助金(総合研究A)研究集会報告集》

代 数 的 組 合 せ 論
報 告 集

1990年7月24日～26日

於 弘 前 大 学

ま え が き

この報告集は、1990年7月24日～26日の3日間、弘前大学理学部に於て行われた研究集会、「代数的組合論」の講演記録である。

集会は多数の参加者を得て、盛会であった。会場の御世話、会の運営には、弘前大学小関道夫教授、大阪教育大学大山豪教授、弘前大学吉荒聡氏にたいへん御世話になった。これら、集会に御協力戴いた方々に深く感謝致します。

なお、研究集会の諸経費、この報告集の作成経費は、文部省科学研究費総合研究A（代表者 名古屋大学北岡良之教授）に依った。

1990年9月

木 村 浩
(愛媛大学)

目 次

1. Characterization of the association schemes of Hermitian forms
over $GF(2^2)$ (A.A.Ivanov-S.V.Shpectorov の仕事の紹介) 1
伊 藤 豊 治 (北大・理)
2. On certain pseudocyclic association schemes 15
生 田 卓 也 (大阪教育大)
伊 藤 達 朗 (大阪教育大)
3. Davenport-Hasse theorem and cyclotomic association schemes 32
坂 内 英 一 (九州大・理)
宗 政 昭 弘 (大阪教育大)
4. An improvement of the Boshier-Nomura bound 44
平 木 彰 (大阪教育大)
5. Applications of intersection diagrams of a distance-regular graph ... 55
鈴 木 寛 (大阪教育大)
6. Bounding the girth of a distance-regular digraph 75
野 村 和 正 (東京医科歯科大)
7. Exact coverings of 2-paths by Hamilton cycles (A solution of
Dudeney's round table problem for even persons) 89
小 林 みどり (静岡県立大)
喜 安 善 市 (半導体研究所)
中 村 義 作 (静岡県立大)
8. A new upper bound on the minimal distance of self-dual codes
(J.H.Conway, N.J.A.Sloan の仕事の紹介) 102
山 野 敏 郎 (愛媛大・理)

9. Hall set を持つ 28 次の Hadamard 行列の分類	120
木 村 浩 (愛媛大・理)	
10. 28 次の Hadamard 行列の木村予想について	129
喜 安 善 市 (半導体研究所)	
木 村 浩 (愛媛大・理)	
11. Translation planes of order q^3 that admit a collineation group of order q^3	145
秋 山 献 之 (福岡大・理)	
末 竹 千 博 (尼崎南高校)	
12. Some recent works on flag-transitive geometries of type $C^k X_m$	160
吉 荒 聡 (弘前大・理)	
13. Note on a p -block of a finite group with abelian defect group	179
渡 辺 アツミ (熊本大・教養)	

Characterization of the association schemes of Hermitian forms over $GF(2^2)$

(A.A. Ivanov - S.V. Shpectorov の仕事の紹介)

北大理

伊藤 豊治

(Toyoharu - Itoh)

(P and Q)-polynomial scheme の分類の programme [1] において重要な step の 1 つ に知られている (P and Q)-polynomial scheme の parameters による characterization problem がある。これは知られている scheme の parameters と一致する parameters をもつ scheme をすべて記述することである。

ここでは、A. A. Ivanov と S. V. Shpectorov による Hermitian forms の association schemes $Her(d, 2)$ の parameters による characterization について紹介します。

§1. まず (P and Q)-polynomial schemes の定義と基本的な性質を見てゆきます。

定義 (symmetric association scheme)

X : 有限集合, $R_i \subseteq X \times X$ $i = 0, 1, \dots, d$

$\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ は symmetric association scheme

with d classes

def \Leftrightarrow i) $R_0 = \{(x, x) \mid x \in X\}$

ii) $R_0 \cup R_1 \cup \dots \cup R_d = X \times X$, $R_i \cap R_j = \emptyset$ ($i \neq j$)

iii) $(x, y) \in R_i \rightarrow (y, x) \in R_i$ $i = 0, 1, \dots, d$.

iv) $0 \leq i, j, k \leq d$ $\forall (x, y) \in R_k$ に $\bar{x} \neq y$ 2

$$\#\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\} = P_{ij}^k$$

は (x, y) のとり方によらず, i, j, k によって決まる。

この P_{ij}^k を \mathfrak{A} の intersection numbers という。

$\mathfrak{A} = (X, \{R_i\}_{0 \leq i \leq d})$: symmetric association scheme

$A_i \in R(X, X)$, $x, y \in X$

$$(A_i)_{x,y} = \begin{cases} 1 & (x, y) \in R_i \\ 0 & \text{otherwise} \end{cases} \quad (i = 0, 1, \dots, d)$$

この行列を \mathfrak{A} の i -th adjacency matrix という。

association scheme の定義 iv) より

$$A_i A_j = \sum_{k=0}^d P_{ij}^k A_k. \quad (0 \leq i, j \leq d).$$

よって A_0, A_1, \dots, A_d によって生成される \mathbb{R} 上の vector space は algebra を成す。この algebra を \mathfrak{A} の Bose-Mesner algebra といひ, $\mathcal{A}(\mathfrak{A})$ で表わす。この B-M algebra $\mathcal{A}(\mathfrak{A})$ は semi simple 故の $d+1$ の primitive idempotents が存在する。それらを E_0, E_1, \dots, E_d (特に $E_0 = \frac{1}{|X|} J$, J : すべて 2 の要素が 1 の行列)

とする。このとき

$$A_i = \sum_{j=0}^d P_{i,j} E_j$$

$$E_i = \frac{1}{|X|} \sum_{j=0}^d q_{i,j} A_j$$

$$= P_{i,j}, q_{i,j} \in \mathbb{R} \quad 0 \leq i, j \leq d$$

と表わせる。また \circ は Hadamard product "o" (行列の要素ごとの積) について閉じているので

$$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^d q_{ij}^k E_k$$

とし、この q_{ij}^k を Krein parameters ($0 \leq i, j, k \leq d$) とする。

$\{P_{ij}^k\}$ ($\{q_{ij}^k\}$, $\{P_{ij}\}$, $\{q_{ij}\}$) を \mathcal{X} の parameters とする。

($\{q_{ij}^k\}$, $\{P_{ij}\}$, $\{q_{ij}\}$ は $\{P_{ij}^k\}$ によって決まることかできる。)

定義 ((P and Q)-polynomial schemes)

$\mathcal{X} = (X, \{P_{ij}\}_{0 \leq i, j \leq d})$ symmetric association scheme

\mathcal{X} : P-polynomial scheme with respect to the ordering P_0, \dots, P_d

$$\stackrel{\text{def}}{\Leftrightarrow} P_i^j = 0 \quad \text{for } |i-j| \geq 2$$

$$P_{ij}^j \neq 0 \quad \text{for } |i-j|=1$$

\mathcal{X} : Q-polynomial scheme with respect to the ordering Q_0, \dots, Q_d

$$\stackrel{\text{def}}{\Leftrightarrow} q_{ij}^i = 0 \quad \text{for } |i-j| \geq 2$$

$$q_{ij}^j \neq 0 \quad \text{for } |i-j|=1$$

$\mathcal{X} : (P \text{ and } Q)\text{-polynomial scheme}$

$\stackrel{\text{def}}{\iff} \mathcal{X}$ は P-polynomial scheme であり, \mathcal{X} が Q-polynomial scheme.

$\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ P-polynomial scheme

$\iff \Gamma = (X, R_i) : \text{distance-regular graph (D.R.G.)}$

$(\alpha, \beta) \in R_i \iff \partial(\alpha, \beta) = i \quad \partial : \Gamma \text{ の キ ョ リ 関 数}$

よ、2 \mathcal{X} を parameters による characterization するとき、 \mathcal{X} による D.R.G. $\Gamma = (X, R_i)$ を parameters (intersection array) による 2 characterized すればよい。

次の記号はよく用いられる。

$\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d}) : \text{P-polynomial scheme}$

$\Gamma = (X, R_i) : \mathcal{X}$ による D.R.G., $\partial : \Gamma$ の キ ョ リ 関 数

とする。

$$b_i = |R_{i+1}^i|, \quad a_i = |R_i^i|, \quad c_i = |R_{i-1}^i|$$

$$k = b_0 = b_i + a_i + c_i \quad 0 \leq i \leq d$$

$$x \in X, \quad \Gamma_i(x) = \{y \in X \mid \partial(x, y) = i\}, \quad y \in \Gamma_i(x)$$

$$B(x, y) = \Gamma_i(x) \cap \Gamma_{i+1}(y), \quad |B(x, y)| = b_i$$

$$A(x, y) = \Gamma_i(x) \cap \Gamma_i(y), \quad |A(x, y)| = a_i$$

$$C(x, y) = \Gamma_i(x) \cap \Gamma_{i-1}(y), \quad |C(x, y)| = c_i$$

• $x, y, z \in X$ $z \in C(y, X)$ のとき.

$$C(x, z) \subseteq C(x, y), \quad B(x, z) \supseteq B(x, y)$$

$$\therefore C_1 \subseteq C_2 \subseteq \dots \subseteq C_d, \quad b_0 \geq b_1 \geq \dots \geq b_{d-1}$$

である。

§2 次に $GF(q^2)$ 上の Hermitian forms の schemes の諸性質を見ます。

定義 (association schemes of Hermitian forms)

V : d -次元 vector space over $GF(q^2)$

$X = \{f: V \text{ 上 の Hermitian form (including the singular)}\}$, $|X| = n$
とす。

V : d^2 -次元 vector space over $GF(q)$

$$x, y \in X \quad (x, y) \in R_i \iff \text{rank}(x - y) = i$$

のとき.

$$\text{Her}(d, q) = (X, \{R_i\}_{0 \leq i \leq d})$$

は $(P \text{ and } Q)$ -polynomial scheme であり, これを Hermitian forms の association scheme とする。

いま $\Gamma = (X, R_i)$ ($\text{Her}(d, q)$ に関する D.R.G.) とする。

このとき, Γ の parameters (intersection numbers) は次のまうになる。

$$b_i = b_i(d, q) = \frac{q^{2d} - q^{2i}}{q + 1}$$

$$C_i = C_i(d, q) = \frac{q^{i-1}(q^i - (-1)^i)}{q + 1}$$

$$A_i = A_i(d, q) = \frac{q^{2i} - q^{i-1}(q^i - (-1)^i) - 1}{q + 1}$$

また次のことが成り立つ。

$$\bullet \text{Aut}(\Gamma) = N \rtimes M \quad \text{但し } N = \langle n_z, | z \in X \rangle \quad n_z: X \rightarrow X; x \mapsto x+z$$

$$M = \Gamma \text{Ld}(q^2)/K \quad K = \{ \alpha \mid \alpha^{q^2+1} = 1, \alpha \in \text{GF}(q^2) \}$$

$$\bullet x, y \in X \quad \partial(x, y) = i$$

$$Y(x, y) = \{ z \in X \mid \text{rad} z \geq \text{rad}(y-z) \}$$

$\Delta(x, y)$: $Y(x, y)$ による 2 誘導される Γ の subgraph

この Δ は $\Delta(x, y)$ は $\text{Herc}(i, q)$ に関する D.R.G. と同形である。

$$\therefore i=d \text{ の } \Delta \cong \Delta(x, y) \cong \Gamma$$

$$i=1 \text{ の } \Delta \cong \Delta(x, y) \text{ は order } q = q_1 + 2 \text{ の clique.}$$

よって $\Gamma(x)$ による 2 誘導された Γ の subgraph

は order $q-1$ の clique の disjoint union である。

• 命題 a.

$$x, y \in X \cdot \partial(x, y) = i, u \in \Gamma(x), v \in \Gamma(y), \partial(x, u) \leq i, \partial(y, u) \leq i$$

$$\rightarrow \partial(u, v) \leq i$$

$$\bullet \partial(x, y) = i, u, v \in \Gamma(x), \partial(u, v) = 1, \partial(y, u) \leq i$$

$$\rightarrow \partial(y, v) \leq i$$

§3 次に $\text{Her}(d, g)$ の parameters から $\Delta(x, y)$ を再構成する。

$\mathfrak{X} = (\tilde{X}, \{\tilde{R}_i\}_{0 \leq i \leq d})$: $\text{Her}(d, g)$ と同じ parameters をもつ association scheme

$\tilde{\Gamma} = (\tilde{X}, \tilde{R}_1)$: \mathfrak{X} に与える D.R.G.

以下次のことを仮定する。

仮定 $x \in \tilde{X}$ に対し $\tilde{\Gamma}(x)$ による $\tilde{\Gamma}$ の subgraph は $e \in X$ についで $\Gamma(e)$ による Γ の subgraph と同形である。すなわち $\tilde{\Gamma}(x)$ による $\tilde{\Gamma}$ の subgraph は size g の cliques の disjoint union である。
($g=2, 3$ のときは、この仮定は成り立つ。)

次のことを用いる..

$$x \in \tilde{X} \quad e_x = (0 \cdots \overset{x}{1} \cdots 0)$$

V : $e_x (x \in \tilde{X})$ による \mathbb{R} 上の vector space

$V_i = E_i V$ (projection) ($\text{Her}(d, g)$ は self dual 故に $\dim V_i = k$)

の場合、

$$*: \tilde{X} \rightarrow V_i; x \mapsto x^* = \sqrt{n} E_i e_x \quad : 1 \text{ 対 } 1 \text{ 写像}$$

とする。このとき $x, y \in \tilde{X}$

$$\langle x^*, y^* \rangle = g_1(i) \quad \text{if } \partial(x, y) = i$$

補題1.

$x \in \tilde{X}$ $\tilde{\Pi}(x) = \{y_1, \dots, y_k\}$ とする。このとき、 $\{y_1^*, \dots, y_k^*\}$ は linear independent である。

(これは行列 $M = \|\langle y_i^*, y_j^* \rangle\|_{k \times k}$ が nonsingular であることによる。)

いま $\dim V_1 = k$ なのだから、補題1より y_1^*, \dots, y_k^* は V_1 の basis としてとれます。よって $\{y_1^*, \dots, y_k^*\}$ を固定することとし、 $\forall z \in \tilde{X}$ に対して $\partial(z, y_i)$ をすべて知ることで z^* は再構成できる。

次の P. Tewilliger [3] の任意の (P and Q)-polynomial scheme に対しての結果により \tilde{X} について命題 Q が成り立つ。

$\tilde{Y} = (Y, \{S_i\}_{0 \leq i \leq d})$: (P and Q)-polynomial scheme

$C = \{x_1, x_2, x_3, x_4\}$: Y の ordered 4-elements subset.

この C に対して $\{(\tau, j) \mid 1 \leq i, j \leq 4, i \neq j\}$ 上の map T を

$$T(\tau, j) = \partial(x_i, x_j)$$

で定義する。この C の type をこの map T によって定める。

このとき

$$m_T = \#\{C \in \binom{Y}{4} \mid C \text{ は type } T\}$$

$$m_i = \#\{C \in \binom{Y}{4} \mid \partial(x_2, x_m) = i \quad x_2 \neq x_m \in C\}$$

とする。

$$0 \leq i \leq d.$$

定理2 (P. Terwilliger [3])

n_T の値は \mathcal{G} の parameters $\lambda, n_1, \dots, n_d, \lambda = \min\{\lfloor \frac{d}{2} \rfloor, T(i,j) \mid 1 \leq i, j \leq d, i \neq j\}$ の値によつて決まる。

仮定より \mathcal{G} の n_i の値は $\text{Her}(d, \mathcal{G})$ の n_i の値と一致する。また定理2より、もし $\#\{(i,j) \mid T(i,j) = 1\} \geq 1$ ならば n_T は $\text{Her}(d, \mathcal{G})$ と \mathcal{G} について一致する。よつて命題Aは \mathcal{G} についても成り立つ。

次に \mathbb{R}^d の $\Delta(\alpha, \gamma)$ を \mathcal{G} について定義する。

$$x, y \in \tilde{X} \quad \text{s.t.} \quad \partial(\alpha, \gamma) = i \quad 1 \leq i \leq d-1$$

$$Z = Z(\alpha, \gamma) = \langle x^*, z^* \mid z \in C(\alpha, \gamma) \cup A(\alpha, \gamma) \rangle \leq V_i \text{ subspace.}$$

$$\tilde{Y} = \tilde{Y}(\alpha, \gamma) = \{z \in \tilde{X} \mid z^* \in Z\}$$

このとき

$$\Delta = \Delta(\alpha, \gamma) : \tilde{Y} \text{ によつて誘導された } \tilde{\Gamma} \text{ の subgraph}$$

(この subgraph Δ の rank を $\partial(\alpha, \gamma)$ によつて与える)

とするとき Δ について次のことが成り立つ。

補題3

$$i) \omega \in \tilde{Y}(\alpha, \gamma) \rightarrow \partial(\alpha, \omega) \leq i, B(\alpha, \gamma) \subseteq B(\alpha, \omega)$$

$$ii) \omega \in \tilde{Y}(\alpha, \gamma), z \in C(\omega, x) \cup A(\omega, x) \rightarrow z \in \tilde{Y}(\alpha, \gamma)$$

$$iii) z \in \tilde{Y}(\alpha, \gamma) \rightarrow \exists \omega \in \tilde{Y}(\alpha, \gamma) \text{ s.t. } \partial(\alpha, \omega) = i \quad \text{と } \exists \text{ に } \Delta = \Delta(\alpha, \omega)$$

以上より

補題4

$\Delta(\alpha, \gamma)$ は $\text{Her}(d, \mathbb{R})$ から得られる D.R.G. と同じ parameters をもつ D.R.G. である。

補題5

$x \in \tilde{X}$, $\{\Delta(\alpha, \gamma) \mid 1 \leq \partial(\alpha, \gamma) \leq d-1, \gamma \in \tilde{X}\}$ は $\text{PG}(d-1, \mathbb{R}^2)$ の構造をもつ。

仮定から初めて適当な \mathcal{G} に対して $\tilde{\Gamma}$ の構造についていくつかの微妙な情報から再構成した。しかしここでは唯一 $\mathcal{G} = 2$ のときのみ完全な characterization を行うことができません。

§4 次に $\text{Her}(d, 2)$ の characterization を行います。

次のことを使います。

補題6

$\Gamma = (X, R_1) : \text{Her}(d, 2)$ に関する graph

$$x \in X, \Sigma(x) = \{\gamma \in X \mid \partial(x, \gamma) \leq d-1\}$$

このとき $\{\alpha^* \in V_1 \mid \alpha \in \Sigma(x)\}$ は $\text{Her}(d, 2)$ を構成する vectors の complete set から一意的に振張られる。

Her(d, 2) の characterization を d について帰納法により行
います。

$d=2$ のとき Γ は Clebsch graph です。これは J.J.
Seidel [2] によつて 2-regularity が示されている。

$d=3$ のとき Γ の intersection array は

$$1^{21} \text{---} 21^{20} \text{---} 210^{16} \text{---} 1280^9$$

$$(\beta_{1(0)}, \beta_{1(1)}, \beta_{1(2)}, \beta_{1(3)}) = (21, -11, 5, -3)$$

この 2-characterization は $\{x^* \mid x \in X\} \subseteq V_1$, s.t. $\langle x^*, y^* \rangle = \beta_{1(i)}$
if $\partial(x, y) = i$ の direct construction により行います。この
vectors の set の選ぶ方の可能性はいくつがある。

$V_1 = \mathbb{R}^{21}$, $e_i^*, -e_i^*$ - V_1 の natural basis.

$$x \in X, \Gamma_1(x) = \{y_1, \dots, y_{21}\}$$

このとき次のように仮定できる。

$$x^* = -\sum_{i=1}^{21} e_i^*, \quad y_i^* = -\frac{1}{3}x^* + 4e_i^* \quad 1 \leq i \leq 21$$

よつて $z \in \Gamma_2(x)$, $w \in \Gamma_3(x)$ とすると

$$\langle z^*, e_i^* \rangle = \begin{cases} -\frac{7}{3} & \text{if } \partial(z, y_i) = 1 \\ \frac{5}{3} & \text{if } \partial(z, y_i) = 2 \\ -\frac{1}{3} & \text{if } \partial(z, y_i) = 3 \end{cases}$$

$$\langle w^*, e_i^* \rangle = \begin{cases} 1 & \text{if } \partial(w, y_i) = 2 \\ -1 & \text{if } \partial(w, y_i) = 3 \end{cases}$$

とある。

補題5より $x \in X$ $L = \{\Delta(x, y) \mid y \in X, \delta(x, y) = 2\}$ のとき $(\Gamma(x), L)$ は order 4 の projective plane である。そしてそのような planes は同形である。この事実と補題6より $\Sigma(x)$ によって誘導された subgraph は Γ 上で再構成できる。それは $\Gamma_3(x)$ からの vector の再構成で十分です。

$$w \in \Gamma_3(x), \{z_1, \dots, z_{12}\} = \Gamma_1(w) \cap \Gamma_2(x) \quad \text{とす。}$$

このとき $\Delta(x, z_1), \dots, \Delta(x, z_{12})$ はすべて異なる。

$$\text{そして命題Aより } \Gamma_2(z_i) \cap \Gamma_1(x) \subseteq \Gamma_3(w) \cap \Gamma_1(x)$$

$$\text{よって } P_w = \Gamma_1(x) \cap \Gamma_3(w) \quad B = \{\Delta(x, z_i) \mid 1 \leq i \leq 12\} \quad \text{とすると}$$

(P_w, B) は order 3 の affine plane となります。

$$\text{そして } w_1, w_2 \in \Gamma_3(x) \quad (w_1 \neq w_2)$$

$$\rightarrow \Gamma_1(x) \cap \Gamma_3(w_1) \neq \Gamma_1(x) \cap \Gamma_3(w_2)$$

$$\text{さらに } \delta(w_1, w_2) = 1 \iff |\Gamma_1(x) \cap \Gamma_3(w_1) \cap \Gamma_3(w_2)| = 1$$

また $PG(2,4)$ はちょうど 280 の order 3 の affine planes を含んでいます。よって $\Gamma_3(x)$ によって誘導された subgraph は order 4 の projective plane 上の order 3 の affine plane のすべしこの埋込みの D.R.G. となります。このことにより $Her(3,2)$ は parameters によって characterization された。

次に $d \geq 4$ とします。また $d' \leq d$ とし $Her(d', 2)$ はそれらの parameters によって characterization されると仮定します。

$x \in X$, $\Pi(x) = \{y_1, \dots, y_n\}$. 補題1より y_1^*, \dots, y_n^* は V の basis としてとれる。また $\Pi(x)$ 上の projective space $\text{PG}(d-1, 2^2)$ の構造も一意的に決まる。ここで y_1^*, \dots, y_n^* と $\Pi(x)$ 上の $\text{PG}(d-1, 2^2)$ の構造の選び方により $\{x^* \mid x \in X\}$ の完全な集合が決まることを見る。

実際、補題6と帰納法の仮定より、 $\{x^* \mid x \in \Sigma(x)\}$ は再構成できる。また $y_i \in \Pi(x)$ に対し $d \geq 4$ なの $\Pi_2(y_i) \subseteq \Sigma(x)$ より Δ を y_i を含む rank 2 の subgraph とすると $\Delta \subseteq \Sigma(x)$ $\text{PG}(d-1, 2^2)$ の構造はすでに $\Pi(y_i)$ 上で定義されているので、 $\{x^* \mid x \in \Sigma(y_i)\}$ は再構成できる。ここで $\forall y_i \in \Pi(x)$ に対しこの構成を行うことにより、 $\forall z \in X$ に対し z^* をみつけることができる。よって $\text{Her}(d, 2)$ は parameters によって characterization されたこととなります。

よって

$\mathcal{X} = (X, \{R_i\}_{i=1}^d)$ が $\text{Her}(d, 2)$ と同じ parameters をもつ $(\text{Pund}(Q))$ -polynomial scheme ならば、 \mathcal{X} は $\text{Her}(d, 2)$ と同形である。

文 献

O. A. A. Ivanov and S. V. Shpectorov , Characterization of the association schemes of Hermitian forms over $GF(2^2)$, Geometriae Dedicata 30 (1989) 23 - 33 .

1. E. Bannai and T. Ito , Algebraic Combinatorics I : Association schemes , Benjamin, 1984 .

2. J. J. Seidel , Strongly Regular Graphs with $(-1, 1, 0)$ Adjacency Matrix having Eigenvalue 3 , Linear Algebra Appl., 1 (1968) 281-298

3. P. Terwilliger , Counting 4-Vertex Configurations in $(\text{Pand}Q)$ -polynomial Association Schemes , Algebras, Groups and Geometries 2, (1985) 541-554 .

On certain pseudocyclic association schemes

大阪教育大学

生田卓也

伊藤達郎

1. Introduction

$\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を位数 n の有限集合 X 上の d -class commutative association scheme とする。association scheme の表記法や一般論については [2] を参照する。

$P = (p_i(j))$, $Q = (q_i(j))$ をそれぞれ $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の 1st eigenmatrix, 2nd eigenmatrix とする。重複度 $m_i = q_i(0)$ ($1 \leq i \leq d$) が互いに一致するとき、 \mathcal{X} は pseudocyclic と呼ばれる。 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ が pseudocyclic ならば、valency $k_i = p_i(0)$ ($1 \leq i \leq d$) は互いに一致する ([2 Theorem 4.3], [4 Proposition 2.2.7] 参照)。

P_0 を P の右下サイズ $d \times d$ の submatrix とし、以後

P_0 を P の 主要部 と呼ぶ。

$$P = \begin{pmatrix} 1 & k_1 & \cdots & k_d \\ 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{pmatrix}$$

P の行は association scheme の adjacency algebra の primitive idempotents で index されており、 P の列は relation の集合 $\{R_i\}_{0 \leq i \leq d}$ で index されている。 P_0 は行と列の置換を除いて決まる。

G を位数 d の有限群、 $A: G \rightarrow GL(d, \mathbb{C})$ を G の右正則表現、すなわち、 G の元 a, b, x に対し、 $(A(x))_{a,b} = \delta_{ax,b}$ である。ただし $\delta_{ax,b}$ はクロネッカーのデルタである。pseudocyclic な association scheme は、 P_0 の行と列の適当な入れ換えにより、 $P_0 = \sum_{a \in G} \eta_a A(a)$ と表わせれるとき、 G -type と呼ばれる。別の言葉で言えば、 P_0 の (a,b) 成分は、 $c = a^{-1}b$ であるときはいつでも η_c である。特にすべての η_a は代数的整数である。巡回群 G に対し、 \mathcal{A} が G -type なら、 \mathcal{A} は cyclic と呼ばれる。cyclotomic association scheme は cyclic association scheme の典型的な例であり、cyclotomic association scheme に対しは、 η_a たちは、

Gaussian periods である ([3], [10]).

$\{\Lambda_j\}_{0 \leq j \leq d}$ を $\Lambda_0 = \{0\}$ である $\{0, 1, \dots, d\}$ の分割とする。
 $R_{\Lambda_j} = \bigcup_{i \in \Lambda_j} R_i$ とする。 $\tilde{\mathcal{X}} = (X, \{R_{\Lambda_j}\}_{0 \leq j \leq d})$ が association scheme になるとき、 $\tilde{\mathcal{X}}$ は $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の fusion scheme と呼ばれる。 $\Lambda_0 = \{0\}$ である任意の分割 $\{\Lambda_j\}_{0 \leq j \leq d}$ に対して、 $\tilde{\mathcal{X}} = (X, \{R_{\Lambda_j}\}_{0 \leq j \leq d})$ が \mathcal{X} の fusion scheme であるとき、 \mathcal{X} を amorphic とよぶ。

与えられた分割 $\{\Lambda_j\}_{0 \leq j \leq d}$ に対して、fusion scheme が
生じるための P の言葉で表わされた簡単な判定基準
がある (Bannai [1], Muzichuk [11] による)。それは、 P の
任意の (Δ_i, Λ_j) block が constant row sum を持つ
ような $\Lambda_0 = \{0\}$ である $\{0, 1, \dots, d\}$ の分割 $\{\Delta_i\}_{0 \leq i \leq d}$
が存在することである。constant row sum は、fusion
scheme の 1st eigenmatrix の (i, j) 成分になる。

文献 [1], [5], [11] などでは "subscheme" という
用語は、"fusion scheme" という用語のかわりに使わ
れている。"subscheme" は、sub-association scheme
([2]) と混乱する恐れがあるので、[7] にちなんで
"fusion scheme" という用語を使うことにする。

A. V. Ivanov [9] より、amorphic association scheme

は Latin square type が negative Latin square type ([4, p.68]) かのどちらかである。この事実から、次の結果を得る。この結果の証明は易しいが、どこにも公表されてないようであるから、定理としてここで述べる価値はあると思う。

Theorem 1. d -class pseudocyclic association scheme が amorphic であるための必要十分条件は、1st eigenmatrix の主要部が 行と列の置換を除いて J と I の線形結合で表わされることである。ただし J はサイズ d の all 1 matrix で I はサイズ d の単位行列である。

d -class の amorphic pseudocyclic association scheme は、位数 d の任意の有限群 G に対して G -type である。Baumert, Mills, Ward [3] は amorphic である cyclotomic association scheme を分類した。

$\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を G -type association scheme とし、 H を G の部分群とする。 $P_0 = \sum_{a \in G} \eta_a A(a)$ であるように集合 $\{1, 2, \dots, d\}$ を G を同一視する。そのとき、Proposition 1 で見るとおり、 G の各部分群に対して fusion scheme が得られる。この事実から、基本アベル 2-群 type の association

scheme は たくさん fusion scheme を持つことがわかる。
 実際 次のことが示される。

Main Theorem G が 基本アベル 2-群 なら、任意の
 G -type association scheme は amorphic である。

2. Some General Results

Proposition 1. $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を G -type association
 scheme. H を G の部分群 とする。

(i) H による 右コセット分解 は、 \mathcal{X} の fusion scheme を
 引き起こす。

(ii) H が 正規部分群 なら、(i) で得られた fusion
 scheme は G/H -type である。

(iii) G の分割 $\{\Lambda_j\}_{1 \leq j \leq d'}$ が fusion scheme を引き
 起こす なら、 G の任意の元 g に対し $\{g\Lambda_j\}_{1 \leq j \leq d'}$
 も fusion scheme を引き起こす。

Proof. (i) Muzichuk - Bannai の判定基準を分割

$\{\Lambda_j\}_{1 \leq j \leq d'} = H \backslash G$ と $\{\Delta_i\}_{1 \leq i \leq d'} = H \backslash G$ に適用する。

$P_0 = \sum_{g \in G} \eta_g A(g)$ とする。このとき、

$$\sum_{x \in H\alpha} (P_0)_{g,x} = \sum_{x \in H\alpha} \sum_{g \in G} \eta_g \delta_{g\alpha, x}$$

$$= \sum_{x \in Ha} \eta_{g^{-1}x}$$

$$= \sum_{y \in g^{-1}Ha} \eta_y$$

だから、 $Hg_1 = Hg_2$ であるときは 1 つでも

$$\sum_{x \in Ha} (P_0)_{g_1, x} = \sum_{x \in Ha} (P_0)_{g_2, x}$$

である。

(ii) H が G の正規部分群 とする。このとき fusion scheme の 1st eigenmatrix の (Hg, Ha) 成分は $\sum_{x \in Hg^{-1}a} \eta_x$ である。

これは 行列

$$\sum_{Hg \in G/H} \left(\sum_{x \in Hg} \eta_x \right) \tilde{A}(Hg)$$

の (Hg, Ha) で成分である。ただし \tilde{A} は G/H の正則表現である。だからこの fusion scheme は G/H -type である。

(iii) P の任意の (Δ_i, Λ_j) block が constant row sum であるような分割 $\{\Delta_i\}_{1 \leq i \leq d'}$ が存在する。このとき

$\{g\Lambda_j\}_{1 \leq j \leq d'}$ と $\{g\Delta_i\}_{1 \leq i \leq d'}$ は G の分割であり、 P の任意の $(g\Delta_i, g\Lambda_j)$ block は constant row sum を

持つ。□

G を アーベル群。 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を G -type の association scheme とする。 \hat{G} で G の指標群を表わす

ことにする。 $a \in G, \chi \in \hat{G}$ に対し、 T を (a, χ) 成分が $\frac{1}{\sqrt{|G|}} \chi(a)$ であるサイズ $|G|$ の正方行列とする。このとき、指標の直交関係より、 T はユニタリ行列で、 G の右正則表現 A は次のように対角化される。

$$T^{-1} A(a) T = \text{diag}(\chi(a))_{\chi \in \hat{G}}$$

$P_0 = \sum_{a \in G} \eta_a A(a)$ であるから

$$T^{-1} P_0 T = \text{diag}\left(\sum_{a \in G} \eta_a \chi(a)\right)_{\chi \in \hat{G}} \quad (1)$$

を得る。

$1 \leq i \leq d$ に対し、 $k_i = k_i = m_i$ での 2nd eigen matrix Q の主要部は $\overline{P_0^t}$ ([2 Theorem 3.5 (i)]) であるから、直交関係 $PQ = nI$ は、次の式と同値である。

$$\sum_{a \in G} \eta_a = -1 \quad (2)$$

$$P_0 \cdot \overline{P_0^t} = nI - kJ \quad (3)$$

ただし、 $n = 1 + kd = |X|$ ($d = |G|$)、 I はサイズ d の単位行列、 J はサイズ d の all 1 matrix である。単位指標に対応する T の列は成分がすべて $\frac{1}{\sqrt{d}}$ であり、これは固有値 d に属する J の固有ベクトルである。 T のその他の列は J の kernel に属している。従って、(1) から (3) を用いると、単位指標 1_G に対しては

$$\left| \sum_{a \in G} \eta_a \right|^2 = n - \text{ord} = 1$$

であり、 $\chi \neq 1_G$ に対しては、

$$\sum_{a \in G} \eta_a \chi(a) = \varepsilon(\chi) \sqrt{n} \quad (4)$$

ただし、 $\varepsilon(\chi)$ は絶対値 1 の複素数である。

(2) と (4) を η_a について指標の直交関係を用いて解くと、次の式を得る。

$$\eta_a = \frac{1}{|G|} \left(-1 + \sqrt{n} \sum_{\chi \neq 1_G} \varepsilon(\chi) \chi(a) \right) \quad (5)$$

G と \hat{G} を同一視することにより、 G の元を \hat{G} 上の関数と見なせる。このように、 ε は $\hat{G} - \{1_G\}$ 上の関数であるが、(4) より次のように表わせる。

$$\varepsilon = \frac{1}{\sqrt{n}} \sum_{a \in G} \eta_a a$$

指標の直交関係を用いると、 $\hat{G} - \{1_G\}$ 上の関数として

$$1 = - \sum_{a \neq 1} a$$

であり、 ε は次のように書くことができる。

$$\varepsilon = \frac{1}{\sqrt{n}} \sum_{a \neq 1} (\eta_a - \eta_1) a \quad (6)$$

明らかに、 G の任意の元 a に対して、

$$P_0 A(y) = \sum_{x \in G} \eta_{xy}^{-1} A(x) \quad (7)$$

が成り立つ。また $T(\alpha)$ を G の自己同型写像 α に対して $(T(\alpha))_{g,h} = \delta_{g, \alpha(h)}$ と定義すると、

$$T(\alpha) P_0 T(\alpha)^{-1} = \sum_{x \in G} \eta_{x\alpha} A(x) \quad (8)$$

が成り立つ。

3. Main Theorem の証明

はじめに nonsymmetric な場合を除いておく。

Proposition 2. 位数 4 以上の基本アベル 2-群 G に対し

2. G -type の nonsymmetric association scheme は存在しない。

Proof. G の位数についての帰納法で証明する。 G が位数 4 のとき、すなわち $G = \{(0,0), (1,0), (0,1), (1,1)\}$ とする。 $(\eta_{0,0}, \eta_{1,0}, \eta_{0,1}, \eta_{1,1})$ を P_0 の第 1 行とする。 P_0 の成分の 1 つは実数でないとする。(7) より $\eta_{0,0}$ が実数でないとしてよい。また (8) より $\eta_{0,0} = \overline{\eta_{0,1}}$ を仮定してよい。 $H = \{(0,0), (1,0)\}$ に対応する fusion scheme は Proposition 1 より \mathbb{Z}_2 -type である。すると、この fusion scheme は nonsymmetric であり、

1st eigenmatrix の主要部は.

$$\begin{pmatrix} \eta_{00} + \eta_{10} & \eta_{01} + \eta_{11} \\ \eta_{01} + \eta_{11} & \eta_{00} + \eta_{10} \end{pmatrix}$$

である.

第1列の成分は互いに複素共役であるから, $\eta_{10} = \overline{\eta_{11}}$ を得る.

(b)より $\sqrt{n} \varepsilon = \alpha(1,0) + \beta(0,1) + \gamma(1,1)$. ただし $\alpha = \eta_{10} - \eta_{00}$, $\beta = \eta_{01} - \eta_{00}$, $\gamma = \eta_{11} - \eta_{00}$ と表わされる. ここで, $\alpha - \beta = \overline{\gamma}$ に注意しておく. G の適当な指標により ε を評価すると次の式を得る.

$$n = |\alpha - \beta - \gamma|^2$$

と.

$$n = |-\alpha + \beta - \gamma|^2$$

である. 従って $(\alpha - \beta)\overline{\gamma}$ の実部は零であり,

$$n = |\alpha - \beta|^2 + |\gamma|^2$$

を得る. $\alpha - \beta = \overline{\gamma}$ より, n は even であるが, 一方,

$n = 1 + 4k$ と表わされるから, これは矛盾である.

次に, $G \cong \mathbb{Z}_2^m$, $m \geq 3$ とする. 位数2の任意の部分群に対して, fusion scheme が対応している. この fusion scheme の少なくとも一つが nonsymmetric である

ことを主張するわけであるが、そうでないと仮定する。

すると、 G の異なる 2 元 a, b に対して、 $\eta_a + \eta_b$ は実数である。

G の任意の元 a に対して、

$$\eta_a = \frac{(\eta_a + \eta_b) - (\eta_b + \eta_c) + (\eta_c + \eta_a)}{2}$$

と表わされるから、実数である。これは矛盾である。それ故、

\mathbb{Z}_2^{m-1} -type の nonsymmetric な fusion scheme が存在するが、

帰納法の仮定より矛盾する。

Proposition 2. より G の任意の元 a に対して、 η_a は実数である。以後、 G は位数 4 以上の基本アハル 2-群

とする。 \hat{G} の指標の値は ± 1 である。さらに、(4) の

左辺は実数であるから、 $\chi \neq 1_G$ に対して $\varepsilon(\chi) = \pm 1$ を得る。

(5) より G の任意の 2 元 a, b に対して次を得る。

$$\sqrt{n}(\eta_a - \eta_b) = \frac{n}{|G|} \sum_{\chi \neq 1_G} \varepsilon(\chi) (\chi(a) - \chi(b))$$

左辺は代数的整数であり、右辺は有理数であるから、

両辺は有理整数である。 $n \equiv 1 \pmod{|G|}$ である

から

$$|G| \mid \sum_{\chi \neq 1_G} \varepsilon(\chi) (\chi(a) - \chi(b))$$

でなければならぬ。また $\left| \sum_{x \in 1_G} \varepsilon(x) \chi(a) \right| \leq |G| - 1$ から

$$\sum_{x \in 1_G} \varepsilon(x) (\chi(a) - \chi(b)) \in \{0, |G|, -|G|\}$$

である。 $\varepsilon(1_G) = 1$, $b = 1$ とすると、上の式は次のように書き換えられる。 G の任意の元 a に対して、

$$(\varepsilon, a)_{\hat{G}} \in \left\{ (\varepsilon, 1)_{\hat{G}}, (\varepsilon, 1)_{\hat{G}} + 1, (\varepsilon, 1)_{\hat{G}} - 1 \right\}$$

ただし、 $(\varepsilon, a)_{\hat{G}} = \frac{1}{|G|} \sum_{x \in \hat{G}} \varepsilon(x) \overline{\chi(a)}$ である。

ここで、我々は ε が $-\varepsilon$ が $\hat{G} - \{1_G\}$ 上で \hat{G} の既約指標に一致することを示したいわけであるが、元々の我々の証明は幾分複雑である。そこで、鈴木寛氏による以下の Lemma を用いることにする。

Lemma (Suzuki) G を有限アベル群、 ε を G 上の複素数値関数とする。 次の (i), (ii) を仮定する。

- (i) G の任意の単位元以外の元 a に対して、 $|\varepsilon(a)| = 1$
- (ii) G の任意の既約指標 χ に対して、

$$(\varepsilon, \chi)_{\hat{G}} \in \{\alpha, \alpha + 1, \alpha - 1\}$$

である \mathbb{C} のある元 α が存在する。

このとき、 ε は G のある既約指標 ψ に対して、

$G - \{1_G\}$ 上 $\varepsilon = \psi$ か、 $G - \{1_G\}$ 上 $\varepsilon = -\psi$ かの
どちらかである。

Proof. ρ を G の右正則表現の指標とする。すなわち

$$\rho(a) = \begin{cases} |G| & (a=1) \\ 0 & (\text{それ以外}) \end{cases}$$

$\varepsilon^* = \varepsilon - \alpha\rho$ とおくと $(\varepsilon^*, \chi)_{\hat{G}} \in \{0, \pm 1\}$ なる $G - \{1\}$ 上

$\varepsilon^* = \varepsilon$ となる。

$$\Phi = \{ \chi \in \hat{G} ; (\varepsilon^*, \chi) = 1 \}$$

$$\bar{\Phi} = \{ \chi \in \hat{G} ; (\varepsilon^*, \chi) = -1 \}$$

とおく。このとき

$$\varepsilon^* = \sum_{\chi \in \Phi} \chi - \sum_{\chi \in \bar{\Phi}} \chi,$$

であり

$$(\varepsilon^*, \varepsilon^*)_G = |\Phi| + |\bar{\Phi}|$$

である。

一方

$$(\varepsilon^*, \varepsilon^*) = \frac{1}{|G|} \left(|\varepsilon^*(1)|^2 + \sum_{a \neq 1} |\varepsilon(a)|^2 \right)$$

$$= \frac{1}{|G|} \left\{ (|\Phi| - |\bar{\Phi}|)^2 + |G| - 1 \right\}.$$

$r = |\Phi|$, $s = |\bar{\Phi}|$, $d = |G|$ ($d \geq r+s$) とおくと、次の
式を得る。

$$r+s = \frac{1}{d} \{ (r-s)^2 + d - 1 \}.$$

すなわち

$$d(r+s-1) = (r-s+1)(r-s-1).$$

$r \geq s$ なら $S=0$ であり、 $r=1$ か $r=d-1$ である。 $r < s$ なら $r=0$ で $S=1$ か $S=d-1$ である。従って、 G のある既約指標 ψ に対し、 $G-\{1\}$ 上 $\varepsilon^* = \pm \psi$ である。□

鈴木氏の Lemma を群 \hat{G} に適応すると、 ε か $-\varepsilon$ が $\hat{G}-\{1_G\}$ 上で \hat{G} の既約指標に一致することを言っている。従って、 G の元 a に対して

$$\eta_a = \frac{1}{|G|} \left\{ -1 \pm \sqrt{n} \sum_{\chi \neq 1_G} \chi(a, a) \right\}$$

となる G のある元 a_0 が存在する。これ故 η_a ($a \in G$) は、唯2つの異なる値しかとらず、Theorem 1 より、この association scheme は amorphic である。これこそ Main Theorem の証明ができた。

4. Remark

$p \geq 2$ に対し G が基本アベル p -群 なら、 G -type の association scheme が amorphic になるかどうかということに興味がある。

上述の証明では P_0 の次の性質のみを使っている

(i) $\eta_a (a \in G)$ が代数的整数である。

(ii) 直交関係 (2), (4) が P_0 に対して成り立っている。

ところが $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ の場合には P_0 のこれらの性質は association scheme が amorphic であることを示すには十分でない。実際、直交関係 (2), (4) を満足し、すべての成分が整数であるような $\mathbb{Z}_3 \times \mathbb{Z}_3$ type の P_0 が存在する。

ところが intersection number p_{ij}^k の integrality より我々が見つけたような P_0 は association scheme からは作れない。

References

- [1] E. Bannai, Subschemes of some association schemes, to appear in J. Algebra.
- [2] E. Bannai and T. Ito, Algebraic Combinatorics I Association schemes, Benjamin/Cummings 1984.
- [3] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy, J. Number Theory 14 (1982), 67-82.

- [4] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer, Berlin-Heidelberg 1989.
- [5] I. A. Faradžev, A. A. Ivanov and M. H. Klin, Galois correspondence between permutation groups and cellular rings (association schemes), to appear in Graphs and combinatorics.
- [6] Ja. Ju. Gelfand and M. H. Klin, Amorphic cellular rings I, Investigation in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system sciences 1985, 32-38 (in Russian).
- [7] J. Hemmeter and A. Wolder, Fusion Schemes and partially balanced incomplete block designs, to appear in Ars Combinatoria.
- [8] T. Ikuta, T. Ito and A. Munemasa, On certain pseudocyclic association schemes, preprint.

[9] A.V. Ivanov, Amorphous cellular rings II, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system studies, 1985, 104-111 (in Russian).

[10] J.H. van Lint and A. Schijver, Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields, *Combinatorica* 1 (1981), 63-73.

[11] M.E. Muzichuk, Ph.D. thesis, unpublished.

Davenport-Hasse theorem and cyclotomic association schemes

E. Bannai

Department of Mathematics
Kyushu University

A. Munemasa

Department of Mathematics
Osaka Kyoiku University

July 24, 1990

1 Cyclotomic association schemes

In this section, we define cyclotomic association scheme (or cyclotomic scheme) of class e on $GF(q)$. We shall establish the relationship with its character table and Gauss sums.

Definition. Let q be a prime power and e be a divisor of $q - 1$. Fix a generator α of the multiplicative group of $GF(q)$. Then $\langle \alpha^e \rangle$ is a subgroup of index e and its cosets are $\langle \alpha^e \rangle \alpha^i$, $i = 0, \dots, e - 1$. Define

$$R_0 = \{(x, x) | x \in GF(q)\}$$

$$R_i = \{(x, y) | x, y \in GF(q), x - y \in \langle \alpha^e \rangle \alpha^{i-1}\}, (1 \leq i \leq e)$$

$$\mathcal{R} = \{R_i | 0 \leq i \leq e\}$$

Then $(GF(q), \mathcal{R})$ forms an association scheme and is called the cyclotomic scheme of class e on $GF(q)$. The character table of the cyclotomic scheme is the first eigenmatrix of the association scheme. We will not give a formal

definition here, instead, we show how to construct the character table of cyclotomic scheme from the character table of elementary abelian group. For a discussion of association scheme in general and the definition of the character table, see [2].

Consider the character table T of the additive group of $F = GF(q)$:

$$T = (\chi(a))_{\chi \in \hat{F}, a \in F}$$

The rows of T are indexed by the set of additive characters, the columns of T are indexed by F . The coset decomposition by the subgroup $\langle \alpha^e \rangle$ is a partition of $F - \{0\}$. Consider the q by $e + 1$ matrix T' whose rows are

$$(1, \sum_{\beta \in \langle \alpha^e \rangle} \chi(\beta), \sum_{\beta \in \langle \alpha^e \rangle \alpha} \chi(\beta), \dots, \sum_{\beta \in \langle \alpha^e \rangle \alpha^{e-1}} \chi(\beta))$$

where χ runs through \hat{F} . Then T' has exactly $e + 1$ distinct rows. The character table P of the cyclotomic scheme is the $e + 1$ by $e + 1$ submatrix of T' consisting of $e + 1$ distinct rows. The rows of P can be rearranged in such a way that

$$P = \begin{pmatrix} 1 & f & \dots & f \\ 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{pmatrix}$$

with $q = 1 + ef$, $P_0 = \sum_{i=0}^{e-1} \eta_i C^i$, where C is the e by e matrix:

$$C = \begin{pmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{pmatrix}$$

The matrix P_0 is called the principal part of the character table. The number η_i 's are called Gaussian periods, given by

$$\eta_i = \sum_{\beta \in \langle \alpha^e \rangle \alpha^{i-1}} \chi(\beta)$$

for a fixed nontrivial additive character χ . Let T be a nonsingular matrix such that

$$T^{-1}CT = \begin{pmatrix} 1 & & & & \\ & \xi & & & \\ & & \xi^2 & & \\ & & & \ddots & \\ & & & & \xi^{e-1} \end{pmatrix}$$

where ξ is a primitive e -th root of unity. Then we have

$$\begin{aligned} T^{-1}P_0T &= \sum_{i=0}^{e-1} \eta_i T^{-1}C^i T \\ &= \text{diag} \left(\sum_{i=0}^{e-1} \eta_i, \sum_{i=0}^{e-1} \eta_i \xi^i, \dots, \sum_{i=0}^{e-1} \eta_i \xi^{(e-1)i} \right) \\ &= \text{diag} (G(\psi^0, \chi), G(\psi, \chi), \dots, G(\psi^{e-1}, \chi)) \end{aligned}$$

where ψ is the multiplicative character of F defined by $\psi(\alpha^j) = \xi^j, j = 0, 1, \dots$. Therefore, the eigenvalues of P_0 are Gauss sums.

Theorem 1 (Davenport-Hasse [6]) *Let $K = GF(q^s)$ be an extension of $F = GF(q)$, χ an additive character of F , ψ a multiplicative character of F . Let*

$$\tilde{\psi} = \psi \circ N_{K/F}$$

$$\tilde{\chi} = \chi \circ \text{Tr}_{K/F}$$

Then we have

$$G(\tilde{\psi}, \tilde{\chi}) = (-1)^{s-1} G(\psi, \chi)^s$$

Suppose that \tilde{P}_0 is the principal part of the first eigenmatrix of the cyclotomic scheme of class e on $GF(q^s)$. Then, by a suitable rearrangement of rows and columns, the following matrix equation holds

$$\tilde{P}_0 = (-1)^{s-1} P_0^s$$

This is simply a direct consequence of Davenport-Hasse theorem.

Example. Let $q = r^2$ be a square and take $e = r + 1$. Then $\langle \alpha^e \rangle$ is the multiplicative group of $GF(r)$. One can readily see that $P_0 = rI - J$. The

spectrum of P_0 is $(-1)^1(r)^r$. Notice that this fact is essentially equivalent to Theorem 2. One can apply Davenport-Hasse theorem to conclude that the principal part of the first eigenmatrix of the cyclotomic association schemes of class $r + 1$ on $GF(r^{2s})$ is given by

$$-(-r)^s I + \frac{(-r)^m - 1}{r + 1} J$$

Theorem 2 *Let $q = r^2$ be a square, ψ a multiplicative character of order $r + 1$ of $GF(q)$. Then there exists an additive character χ such that $G(\psi^i, \chi) = q$ for $1 \leq i \leq r$.*

This theorem is a direct consequence of Stickelberger's theorem [11].

Definition. Let (X, \mathcal{R}) be an e -class commutative association scheme. The association scheme is called pseudocyclic if the multiplicities m_1, m_2, \dots, m_d coincide each other. Notice that if $(X, \{R_i\}_{0 \leq i \leq d})$ is pseudocyclic, then the valencies $k_i = p_i(0)$ ($1 \leq i \leq d$) coincide each other. More precisely,

Proposition 3 *Let $(X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme of class d over a finite set X of cardinality $v = 1 + kd$, with $k = k_i$ for $1 \leq i \leq d$. Let*

$$\mathcal{B} = \{R_i(x) \mid x \in X, 1 \leq i \leq d\}$$

The following are equivalent.

- (i) $(X, \{R_i\}_{0 \leq i \leq d})$ is pseudocyclic.
- (ii) $\sum_{i=1}^d p_{ii}^1 = k - 1$.
- (iii) \mathcal{B} is a 2 - $(v, k, k - 1)$ -design.

Proof. See [[4], Proposition 2.2.7] \square

A pseudocyclic association scheme has the first eigenmatrix of the form

$$\begin{pmatrix} 1 & f & \cdots & f \\ 1 & & & \\ \vdots & & P_0 & \\ 1 & & & \end{pmatrix}$$

with $|X| = 1 + ef$.

2 Amorphic association schemes

In this section, we state a theorem of A. V. Ivanov on amorphic association schemes, and present the classification of amorphic cyclotomic scheme due to Baumert, Mills and Ward [3]. Throughout this section, we let p be a prime, ζ a primitive p -th root of unity. We denote the all one matrix by the same notation J regardless the size, since no confusion is likely.

First let us define amorphic association schemes. Let $\{\Lambda_j\}_{0 \leq j \leq d'}$ be a partition of $\{0, 1, \dots, d\}$ with $\Lambda_0 = \{0\}$. Let $R_{\Lambda_j} = \bigcup_{i \in \Lambda_j} R_i$. If $(X, \{R_{\Lambda_j}\}_{0 \leq j \leq d'})$ becomes an association scheme, then it is said to be a *fusion* scheme of $(X, \{R_i\}_{0 \leq i \leq d})$. $(X, \{R_i\}_{0 \leq i \leq d})$ is called *amorphic* if $(X, \{R_{\Lambda_j}\}_{0 \leq j \leq d'})$ is a fusion scheme of $(X, \{R_i\}_{0 \leq i \leq d})$ for any partition $\{\Lambda_j\}_{0 \leq j \leq d'}$ with $\Lambda_0 = \{0\}$.

There is a simple criterion in terms of the first eigenmatrix P for a given partition $\{\Lambda_j\}_{0 \leq j \leq d'}$ to give rise to a fusion scheme (due to Bannai [1], Muzichuk [10]): there exists a partition $\{\Delta_i\}_{0 \leq i \leq d'}$ of $\{0, 1, \dots, d\}$ with $\Delta_0 = \{0\}$ such that each (Δ_i, Λ_j) block of P has a constant row sum. The constant row sum turns out to be the (i, j) entry of the first eigenmatrix of the fusion scheme. Examples of amorphic association schemes are derived from affine planes. The isomorphism classes of affine planes of order q is in one-to-one correspondence with the isomorphism classes of association schemes having the same parameters as the cyclotomic scheme of class $q+1$ on $GF(q^2)$.

Theorem 4 (A. V. Ivanov [9]) *Let (X, \mathcal{R}) be an amorphic association scheme of class d , $d \geq 3$, on n vertices. Then n is a square, say $n = m^2$. If we write $k_i = p_{ii}^0$, $\lambda_i = p_{ii}^1$, $\mu_i = p_{ii}^j$, ($j \neq i, 0$), then either*

(i) *there exist integers g_i , ($1 \leq i \leq d$) such that*

$$\begin{aligned} k_i &= g_i(m-1) \\ \lambda_i &= (g_i-1)(g_i-2) + m-2 \\ \mu_i &= g_i(g_i-1) \end{aligned}$$

or

(ii) *there exist integers g_i , ($1 \leq i \leq d$) such that*

$$k_i = g_i(m+1)$$

$$\begin{aligned}\lambda_i &= (g_i + 1)(g_i + 2) - m - 2 \\ \mu_i &= g_i(g_i + 1)\end{aligned}$$

Definition. An amorphic association scheme satisfying (i) (resp. (ii)) in Theorem 4 is said to be of Latin square type (resp. negative Latin square type).

The following lemma is immediate from Theorem 4.

Lemma 5 *A pseudocyclic association scheme of class d is amorphic if and only if the principal part of the first eigenmatrix is a linear combination of J and I , where J is the all one matrix of size d and I is the identity matrix of size d .*

Therefore the cyclotomic scheme of class $r + 1$ on $GF(r^{2s})$ is amorphic, in view of example in the previous section. Since any fusion scheme of amorphic association scheme is also amorphic, the cyclotomic scheme of class e on $GF(r^{2s})$ is amorphic, if e divides $r + 1$. These are the only amorphic cyclotomic schemes, as we will see in Theorem 7. It should be noted that the first eigenmatrix of an amorphic pseudocyclic association scheme is uniquely determined by the number of classes and the number of vertices. Let us describe the parameters of pseudocyclic amorphic association schemes of class at least 3. Let the number of vertices be m^2 , $m^2 - 1 = ef$, where e is the number of classes. We have $f = g(m - 1)$ for some integer g , if the association scheme is of Latin square type, $f = g(n + 1)$ for some integer g , if it is of negative Latin square type. In what follows, the upper sign of the double sign corresponds to the case of Latin square type, the lower corresponds to the case of negative Latin square type. We will express the parameters and the eigenvalues in terms of e and g .

$$m^2 - 1 = ef = eg(m \mp 1)$$

$$m = eg \mp 1$$

$$f = g(eg \mp 2)$$

Suppose that the first eigenmatrix is of the form

$$\begin{pmatrix} 1 & f & \cdots & f \\ 1 & a & & b \\ \vdots & & \ddots & \\ 1 & b & & a \end{pmatrix}$$

By the orthogonality relation, we have

$$1 + a + (e - 1)b = 0$$

$$f + a^2 + (e - 1)b^2 = ef + 1$$

$$b = \frac{-1 + (eg \mp 1)}{e}, \frac{-1 - (eg \mp 1)}{e}$$

The integrality of b forces that $b = \mp g$. Then $a = -1 \pm (e - 1)g$. The intersection numbers are

$$p_{ii}^i = g^2 - 1 \pm g(e - 3), 1 \leq i \leq e$$

$$p_{ii}^j = g(g \mp 1), 1 \leq i \leq e, 1 \leq j \leq e, i \neq j$$

$$p_{ij}^k = g^2, 1 \leq i \leq e, 1 \leq j \leq e, 1 \leq k \leq e, i \neq j, j \neq k, k \neq i$$

Now we present a short proof of the classification of amorphic cyclotomic association schemes due to Baumert, Mills and Ward [3]. The following lemma, appeared in [8], plays a key role in our proof.

Lemma 6 (Suzuki) *Let G be a finite abelian group and let ϵ be a complex-valued function on G . Suppose*

- (i) $|\epsilon(a)| = 1$ for any nonidentity element a of G ,
- (ii) there exists some $\alpha \in \mathbb{C}$ such that $(\epsilon, \chi)_G \in \{\alpha, \alpha + 1, \alpha - 1\}$ for any irreducible character χ of G .

Then $\epsilon = \psi$ on $G - \{1_G\}$ or $\epsilon = -\psi$ on $G - \{1_G\}$ for some irreducible character ψ of G .

Theorem 7 *Let p be a prime. A cyclotomic scheme of class e on $GF(p^{2s})$ is amorphic if and only if there exists a divisor r of s such that e divides $p^r + 1$.*

Proof. We may assume $e \geq 3$, since the case $e = 2$ is trivial. Let $p^{2s} - 1 = ef$. If the scheme is of Latin square type, then f is divisible by $p^s - 1$. Thus e divides $p^s + 1$.

We prove the assertion for the case of negative Latin square type by induction. Since f is divisible by $p^s + 1$, we see that e divides $p^s - 1$, that is, there exists a cyclotomic scheme of class e on $K = GF(p^s)$. We aim to

show that this scheme is amorphic. Let P_0 be the principal part of its first eigenmatrix. Let $L = GF(p^{2s})$,

$$\tilde{\psi} = \psi \circ N_{L/K}$$

$$\tilde{\chi} = \chi \circ \text{Tr}_{L/K}$$

By Davenport–Hasse Theorem, we have

$$-(T^{-1}P_0T)^2 = \text{diag}((G(\tilde{\psi}^0, \tilde{\chi}), G(\tilde{\psi}, \tilde{\chi}), \dots, G(\tilde{\psi}^{e-1}, \tilde{\chi}))$$

For an appropriate choice of χ , we have

$$G(\tilde{\psi}^j, \tilde{\chi}) = p^s, \quad j = 1, \dots, e-1.$$

This implies

$$G(\psi^j, \chi) = \epsilon(j)\sqrt{p^s}, \quad j = 1, \dots, e-1,$$

where $\epsilon(j) = \pm 1$. It follows that

$$\eta_a = \frac{1}{|G|} \left(-1 + \sqrt{p^s} \sum_{j=1}^{e-1} \epsilon(j) \overline{\chi(a)} \right)$$

Suppose that s is odd. Then η_a belongs to $\mathbf{Q}(\sqrt{p}, \xi)$, which has an automorphism τ fixing ξ and sending \sqrt{p} to $-\sqrt{p}$. Then $\eta_a + \eta_a^\tau = -2/e$, which is a contradiction since $e \geq 3$. Therefore s is even. Now we see that η_a belongs to $\mathbf{Q}(\xi) \cap \mathbf{Q}(\zeta) = \mathbf{Q}$. Combined with the fact that $p^{2s} \equiv 1 \pmod{e}$, we find $\frac{1}{e} \sum_{j=1}^{e-1} \epsilon(j) \xi^{-ij}$ is an integer, hence it must be 0 or ± 1 . By Lemma 6 we conclude $\epsilon(j) = \xi^{kj}$ for some k . Since $\epsilon(j) = \pm 1$ we see $k = 0$, or $k = e/2$ and e even. Now one can conclude the cyclotomic scheme of class e on $GF(p^s)$ is amorphic. Repeating this procedure, one eventually reaches amorphic association scheme of Latin square type, which was treated earlier. \square

3 Notes

3.1 Davenport–Hasse theorem for association schemes

Davenport–Hasse theorem provides a powerful tool to compute the character table i.e., Gaussian periods of cyclotomic scheme, as shown in section 1.

The fact that a power of the principal part of the character table as a matrix is the principal part of the character table of another association scheme is quite remarkable, and we are interested in the situations where this phenomenon occurs.

Here is an example. Consider cyclotomic scheme of class 3 on $GF(4)$ and $GF(16)$. The principal part of their character tables are

$$P_0 = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

$$\tilde{P}_0 = \begin{pmatrix} -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

Notice that the relation $-P_0^2 = \tilde{P}_0$ holds. Now consider the principal part of the character table of \mathbf{Z}_4 , the cyclic group of order 4:

$$Q_0 = \begin{pmatrix} i & -1 & -i \\ -1 & 1 & -1 \\ -i & -1 & i \end{pmatrix}$$

Then

$$-Q_0^2 = \begin{pmatrix} 1 & 1 & -3 \\ 1 & -3 & 1 \\ -3 & 1 & 1 \end{pmatrix}$$

which is the same as \tilde{P}_0 up to some permutation of rows. This motivated us to search for an association scheme on $\mathbf{Z}_4 \times \mathbf{Z}_4$ having the same parameters as cyclotomic scheme of class 3 on $GF(16)$. Indeed, the following partition of $\mathbf{Z}_4 \times \mathbf{Z}_4$ defines an S-ring (hence an association scheme) with the desired property.

$$\begin{aligned} S_0 &= \{(0,0)\} \\ S_1 &= \{(2,2), (0,1), (0,3), (1,0), (3,0)\} \\ S_2 &= \{(1,1), (3,3), (0,2), (3,2), (1,2)\} \\ S_3 &= \{(2,0), (2,1), (2,3), (1,3), (3,1)\} \end{aligned}$$

This association scheme was already included in the list of A. V. Ivanov [9], however, no interpretation was previously known. This association scheme has only the trivial automorphisms, namely, the translations by the elements of $\mathbf{Z}_4 \times \mathbf{Z}_4$ and the inversion, therefore the scheme is not Schurian. We now give the relationship between this association scheme and the Shrikhande-Bose difference set.

Let $\mathcal{D} = \{D - \{(0,0)\} | \mathbf{Z}_4 \times \mathbf{Z}_4 \supset D : (v, k, \lambda)\text{-difference set}, (0,0) \in D = -D\}$. Then $GL(2, \mathbf{Z}_4)$ acts transitively on \mathcal{D} . For example $S_1 = \{(2,2), (0,1), (0,3), (1,0), (3,0)\} \in \mathcal{D}$. Let

$$D_0 = \{(1,0), (2,0), (3,0), (0,1), (0,2), (0,3)\}$$

D_0 is called the Shrikhande-Bose difference set. $\{(0,0)\} \cup S_0$ is equivalent to D_0 , i.e., there exists $g \in G = (\mathbf{Z}_4 \times \mathbf{Z}_4) \cdot GL(2, \mathbf{Z}_4)$ such that $D_0^g = \{(0,0)\} \cup S_0$. This implies the following characterization of the Shrikhande-Bose difference set.

Proposition 8 *If $D \subset \mathbf{Z}_4 \times \mathbf{Z}_4$ is a difference set satisfying $(0,0) \in D, D = -D$, then D is equivalent to the Shrikhande-Bose difference set.*

Let

$$\Sigma = \{(S_1, S_2, S_3) \in \mathcal{D} \times \mathcal{D} \times \mathcal{D} | S_1, S_2, S_3 \text{ are disjoint}\}$$

Then $GL(2, \mathbf{Z}_4)$ acts transitively on Σ . Moreover, $\langle (0,0), \underline{S_1}, \underline{S_2}, \underline{S_3} \rangle$ is an S-ring on $\mathbf{Z}_4 \times \mathbf{Z}_4$ for any $(S_1, S_2, S_3) \in \Sigma$. Conversely, suppose $\langle (0,0), \underline{S_1}, \underline{S_2}, \underline{S_3} \rangle$ is an S-ring on $\mathbf{Z}_4 \times \mathbf{Z}_4$ which defines an amorphic pseudocyclic association scheme, then $(0,0) \cup S_i$ is a difference set for $i = 1, 2, 3$. Therefore $S_i \in \mathcal{D}$, and so $(S_1, S_2, S_3) \in \Sigma$.

Finally let us mention another design associated to our S-ring. In view of Proposition 3, one obtains (16,5,4)-difference families on $GF(16)$ and on $\mathbf{Z}_4 \times \mathbf{Z}_4$. These two designs have the same inner distribution, but not isomorphic.

3.2 Fusion schemes of non-amorphic cyclic association scheme

There are many non-amorphic cyclotomic schemes which have nontrivial fusion schemes. Cyclotomic schemes are pseudocyclic association schemes,

with the additional property: the principal part of the character table is a circulant matrix. We call pseudocyclic association scheme with this property cyclic. If e is not prime, then there exist a fusion scheme of cyclic association schemes corresponding to subgroups of the cyclic group of order e . (see [8]). We call such fusion scheme trivial.

Theorem 9 *If $e \leq 5$, then the only cyclic association schemes with a non-trivial fusion scheme are amorphic association schemes.*

Fusion schemes of class 2 of cyclotomic schemes have been extensively studied, since such a fusion scheme gives rise to a two weight code [5]. If $e \geq 6$ then there exist non-amorphic cyclic association schemes which have non-trivial fusion scheme. We give a few examples below.

Example. Let $K = GF(49)$, α a generator of K^* ,

$$T : K \rightarrow K; x \mapsto x^9$$

$$S : K \rightarrow K; x \mapsto x\alpha$$

Let $H = \langle S^{12}, S^3T \rangle$. Then one obtains a cyclic association scheme of class 6 on K via the action on the group $K \cdot H$. This association scheme has nontrivial fusion schemes, however, it is not amorphic.

Example. The cyclotomic scheme of class 7 on $GF(64)$ has nontrivial fusion schemes of class 2, however, it is not amorphic. The fusion schemes give rise to (64,28,12)-difference sets.

References

- [1] E. Bannai, Subschemes of some association schemes, to appear in J. algebra.
- [2] E. Bannai and T. Ito, Algebraic Combinatorics I : Association schemes, Benjamin/Cummings 1984.
- [3] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy, J. Number Theory 14 (1982), 67 - 82.

- [4] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer, Berlin-Heidelberg 1989.
- [5] A. R. Calderbank and W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) 97-122.
- [6] H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. Reine. Angew. Math. 172 (1935), 151-182.
- [7] Ja. Ju. Gelfand and M. H. Klin, Amorphic cellular rings I, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system sciences 1985, 32 - 38 (in Russian).
- [8] T. Ikuta, T. Ito and A. Munemasa, On certain pseudocyclic association schemes, submitted.
- [9] A. V. Ivanov, Amorphic cellular rings II, Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Moscow, Institute for system sciences, 1985, 104 - 111 (in Russian).
- [10] M. E. Muzichuk, Ph.D.thesis, unpublished.
- [11] L. Stickelberger, Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. 37 (1890), 321-367

An Improvement of the Boshier - Nomura Bound

大阪教育大学 平木 章

1. Introduction.

Let Γ be connected undirected simple finite graph and let ∂ denote the usual distance on Γ

Let d be the diameter of Γ
i.e. $d = \max \{ \partial(u, v) \mid u, v \in \Gamma \}$

For vertices $u, v \in \Gamma$ and non-negative integers $i, j \leq d$ we set

$$\Gamma_i(u) = \{ x \in \Gamma \mid \partial(u, x) = i \}$$

$$D_j^i(u, v) = \Gamma_i(u) \cap \Gamma_j(v)$$

Γ is distance regular, if it satisfies following properties, that is :

the size of $D_j^i(u, v)$ depends only on the distance between u and v rather than the individual vertices.

In that case we write

$$P_{ij}^{\mathcal{L}} = |D_j^i(u, v)|$$

where $\mathcal{L} = \partial(u, v)$

we set intersection numbers as follows

$$c_i = P_{i-1}^i = P_{i-1}^{i-1}$$

$$a_i = P_1^i = P_i^{i-1}$$

$$b_i = P_{i+1}^i = P_{i+1}^{i-1}$$

And let k be the valency of Γ

$$k = P_{11}^0 = |\Gamma_1(u)| \quad \text{for } \forall u \in \Gamma$$

and let

$$\left\{ \begin{array}{cccccccc} * & c_1 & c_2 & \cdots & c_i & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_i & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_i & \cdots & b & * \end{array} \right\}$$

\hat{i}

be the intersection array of Γ

A detailed description of distance-regular graphs will be found in [1] and [2]

One of the most important thing in the study of distance-regular graph is to determine the properties of the intersection array .

For example . we have following properties of the intersection numbers .

LEMMA 1.

- 1) $c_i + a_i + b_i = k$
for $i = 0, 1, 2, \dots, d$
- 2) $1 = c_1 \leq c_2 \leq \dots \leq c_d \leq k$
- 3) $k = b_0 \geq b_1 \geq \dots \geq b_{d-1} > 0$
- 4) If $i + j \leq d$ then $c_i \leq b_j$

In this note . we shall prove the following result

THEOREM

Let Γ be distance-regular graph with valency $k > 3$ and intersection array

$$\left\{ \begin{array}{cccccccc} * & 1 & \cdots & 1 & 1 & \cdots & 1 & \cdots \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 1 & \cdots \\ k & \underbrace{k-1 \cdots k-1}_r & & \underbrace{k-2 \cdots k-2}_s & & & & \cdots \end{array} \right\}$$

If $r > 0$ then $s < 4$

Moreover

If $r > 0$ $s = 3$ then $C_{r+4} > 1$

Boshier and Nomura proved that $s < 5$ if $r > 0$ for all k (see [3])

So what we have shown is we improved their bound by one .

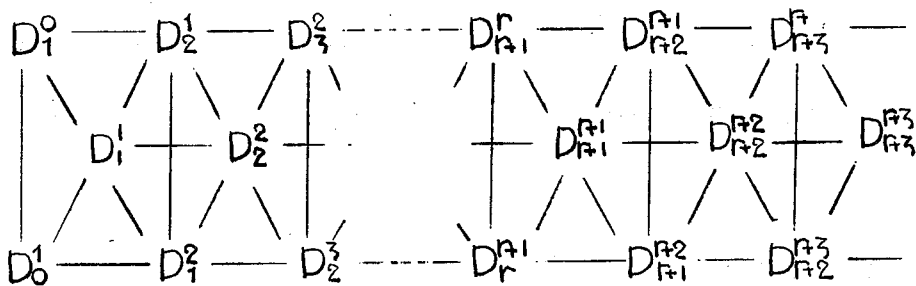
2. Proof of THEOREM

Our proof is based on circuit chasing technique as in Bashier-Nomura's paper [3].

By way of contradiction we assume that

$$r > 0 \text{ and } s \geq 4$$

Let u, v be adjacent vertices and set $D_j^i = D_j^i(u, v)$ then in general the intersection diagram w.r.t. u, v has the shape like this.



where a line between two entries indicates possibility of existence of edges between them.

For a subset A in Γ , the number of edges from a vertex u to A will be denoted by $e(u, A)$.

LEMMA 2

$$D_i^i = \emptyset \quad \text{for } 1 \leq i \leq r$$

Proof

Suppose not. $\exists x \in D_i^i = D_i^i(u, v)$
 then $u \in \Gamma_1(v) \cap \Gamma_i(x)$, $\partial(v, x) = i$
 $\therefore |\Gamma_1(v) \cap \Gamma_i(x)| = \theta_i > 0$

a. contradiction.

□

LEMMA 3

There are no edges between D_{i+1}^i and $D_i^{i+1} \cup D_i^i$ for $1 \leq i < r+1$

Proof

for $x \in D_{i+1}^i$, $e(x, D_i^{i-1}) = c_i$
 and $e(x, D_i^{i-1}) + e(x, D_i^i) + e(x, D_i^{i+1}) = c_{i+1}$
 Since $c_i = c_{i+1}$, $e(x, D_i^i) + e(x, D_i^{i+1}) = 0$ □

LEMMA 3'

There are no edges between D_{i-1}^{i+1} and $D_{i-1}^i \cup D_i^i$ for $1 \leq i < r+4$

LEMMA 4

There are no edges between D_{i+1}^i and $D_{i+1}^{i+1} \cup D_i^{i+1}$ for $1 \leq i < r+4$ $i \neq r$

Proof

$$\text{for } x \in D_{i+1}^i \quad e(x, D_{i+2}^{i+1}) = b_{i+1}$$

$$e(x, D_{i+2}^{i+1}) + e(x, D_{i+1}^{i+1}) + e(x, D_i^{i+1}) = b_i$$

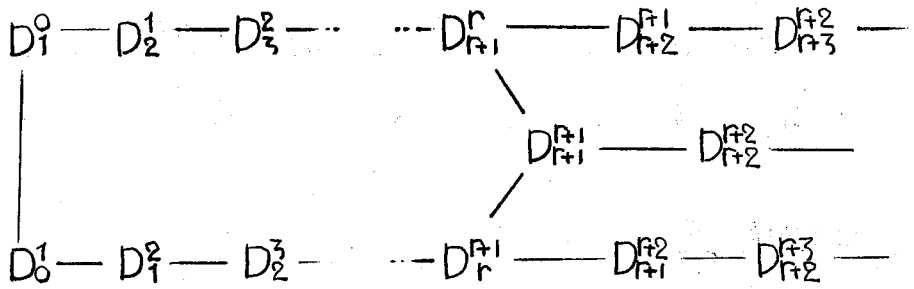
$$\text{Since } b_{i+1} = b_i \quad \therefore e(x, D_{i+1}^{i+1}) + e(x, D_i^{i+1}) = 0$$

□

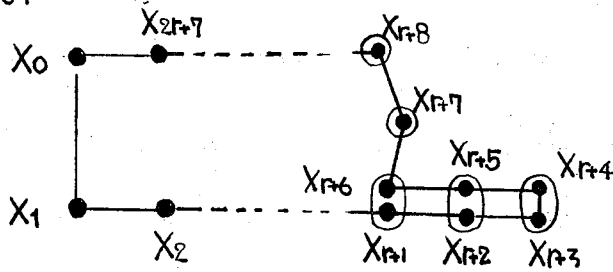
LEMMA 4'

There are no edges between D_i^{i+1} and $D_{i+1}^{i+1} \cup D_{i+1}^i$ for $1 \leq i < r+4$ $i \neq r$

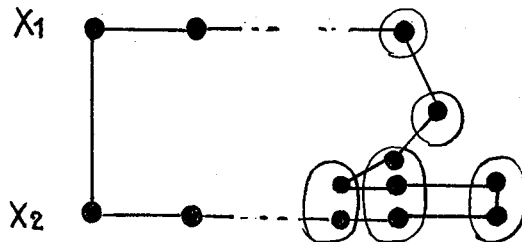
Then, the shape of the diagram becomes one like this .



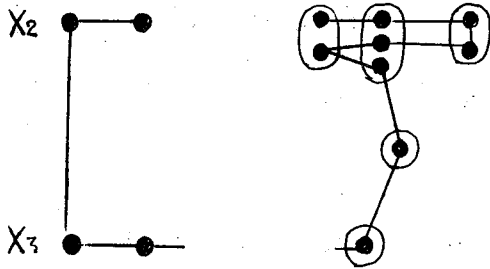
Now we consider a circuit of length $2r+8$ such that



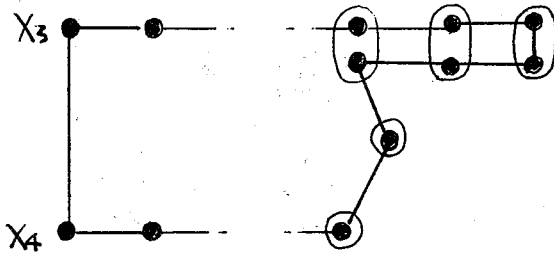
Next we consider the location of vertices of this same circuit on the diagram w.r.t X_1 X_2 . Then we find



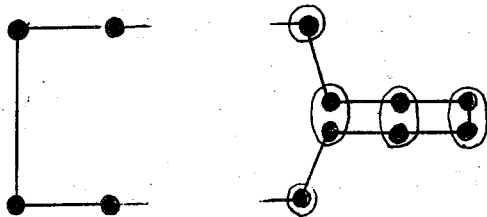
Next with respect to $X_2 X_3$



Next with respect to $X_3 X_4$



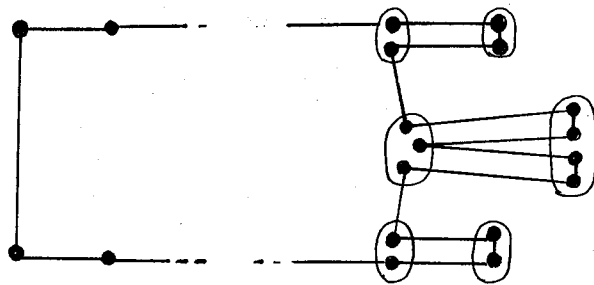
Next. with respect to $X_4 X_5$



Then at fifth try. on the diagram w.r.t
 $X_5 X_6$. we find the same shape as w.r.t
 $X_0 X_1$.

So we can conclude that length of this circuit $2r+8$ is divisible by 5 i.e $2r+8 \equiv 0 \pmod{5}$ $r \equiv 1 \pmod{5}$

Next we consider the different circuit of length $2r+15$. The shape of the circuit on the diagram w.r.t $x_0 x_1$ as follows.



we can do the same business as we have done before. In this case we find the shape of the circuit on the diagram w.r.t $x_0 x_1$ is the same as that w.r.t $x_{15} x_{16}$. It follows that $2r+15 \equiv 0 \pmod{15}$ i.e $r \equiv 0 \pmod{15}$, contradicting $r \equiv 1 \pmod{5}$

REFERENCES

1. E. Bannai and T. Ito
"Algebraic Combinatorics I" Benjamin(1984)
2. A. E. Brouwer, A.M. Cohen, A. Neumaier
"Distance-Regular Graphs" Springer (1989)
3. A. Boshier and K. Nomura
A Remark on the intersection arrays of
distance-regular graphs,
J. Combin. Th. (B). 44 (1988) 147-153

Applications of Intersection Diagrams of a Distance Regular Graph

大阪教育大学 数理科学 鈴木 寛

1. Distance Regular Graph.

Γ : connected undirected simple finite graph.

($\Gamma = (V, E)$, vertex set V , edge set E の組であるが。ここで $V = \Gamma$ とし、 Γ と vertex set を

同一視する。) (simple: loop, multiple bond free)

同-視する。) (simple: loop, multiple bond free)

$d(\alpha, \beta)$: distance (the length of a shortest path)
of α and β . $\alpha, \beta \in \Gamma$.

$d = \max \{ d(\alpha, \beta) \mid \alpha, \beta \in \Gamma \}$: diameter

$\Gamma_i(\alpha) = \{ \beta \in \Gamma \mid d(\alpha, \beta) = i \}$. $\Gamma_0(\alpha) = \Gamma(\alpha)$.

DEFINITION. Γ : distance regular graph (D.R.G.)

$$\Leftrightarrow p_{ij}^l = |\Gamma_i(\alpha) \cap \Gamma_j(\beta)|$$

depends only on $l = d(\alpha, \beta)$. $\alpha, \beta \in \Gamma$.

以下、 Γ を DRG とする。次の定数が定まる。

$$k_i = |\Gamma_i(\alpha)| = |\Gamma_i(\alpha) \cap \Gamma_i(\alpha)| = p_{ii}^{\circ} : i\text{-th valency}$$

$$k = k_1 : \text{valency.}$$

$$c_i = p_{i, i-1}^{\wedge} \quad 1 \leq i \leq d, \quad c_0 = 0$$

$$a_i = p_{ii}^{\wedge} \quad 0 \leq i \leq d$$

$$b_i = p_{i, i+1}^{\wedge} \quad 0 \leq i \leq d-1, \quad b_d = 0, \quad (b_0 = k).$$

c_i, a_i, b_i をならべたものを Γ の intersection array という。 c_0, b_d のところは * とすることが多い。

$$L(\Gamma) = \left\{ \begin{array}{ccccccc} * & c_1 & \cdots & c_i & \cdots & c_d & \\ 0 & a_1 & \cdots & a_i & \cdots & a_d & \\ b_0 & b_1 & \cdots & b_i & \cdots & * & \end{array} \right\}$$

DRG 研究の主要目標は、

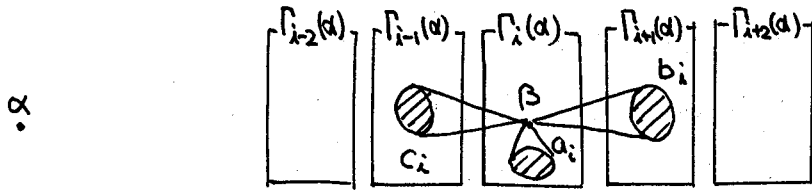
1. DRG の intersection array となりうる array の決定。 または、 intersection array の 性質をみる こと。

2. $L(\Gamma)$ による Γ の 特徴付け。

parameter による characterization とよばれる。

この二つだということもできる。

Let $\alpha, \beta \in \Gamma$ with $d(\alpha, \beta) = i$.



β から出ている edge で $\Gamma_{i-1}(\alpha)$, $\Gamma_i(\alpha)$, $\Gamma_{i+1}(\alpha)$ に行っているものの数がそれぞれ c_i, a_i, b_i 本である。 $\Gamma_j(\alpha)$ の定義と 三角不等式 (距離 $d(\alpha, \beta)$ に関する) より、 β からは これ以外に edge が出ていることから、 i.e.,

$$\Gamma(\beta) \subset \Gamma_{i-1}(\alpha) \cup \Gamma_i(\alpha) \cup \Gamma_{i+1}(\alpha).$$

次が成立することがわかる。

$$k = c_i + a_i + b_i \quad 0 \leq i \leq d.$$

すなわち、 intersection array の row sum は一定で $k = b_0$ である。

2. Intersection Diagram of Rank r

Γ : DRG. $\alpha, \beta \in \Gamma$ $d(\alpha, \beta) = r$

$D_j^i = D_j^i(\alpha, \beta) = \Gamma_i(\alpha) \cap \Gamma_j(\beta)$ と置くと、 ($|D_j^i| = p_{ij}^r$)

(1) $D_j^i = \emptyset$ if $i+j < r$ or $|i-j| > r$.

(2) No edge between D_j^i and D_t^s if $|i-s| > 1$ or $|j-t| > 1$

これらはいずれも 三角不等式

$$d(\alpha, \delta) \leq d(\alpha, r) + d(r, \delta)$$

から、簡単にみちみかれる。

Intersection Diagram とは、 $\{D_j^i\}$ と、それらを結ぶ line とでつくられた図形で、

$$D_j^i \text{ --- } D_t^s \quad \text{possibility of edges}$$

$$D_j^i \text{ --- } D_t^s \quad |r(\alpha) \cap D_t^s| = p \quad \forall r \in D_j^i$$

をいみする。p. という様な数は一定とは限らず。又、様な考察ののち、 D_j^i, D_t^s 間に edge が無いことがわかると、その line を消していく。以下の例参照。

また D_j^i の下に \boxed{m} とあるときは $|D_j^i| = m$ をいみするものとし、 $D_j^i \text{ --- } D_j^i$ は $D_j^i \text{ --- } D_j^i$ をいみする。

EXAMPLE 0. $d(\alpha, \beta) = r = 0$ i.e., $\alpha = \beta$

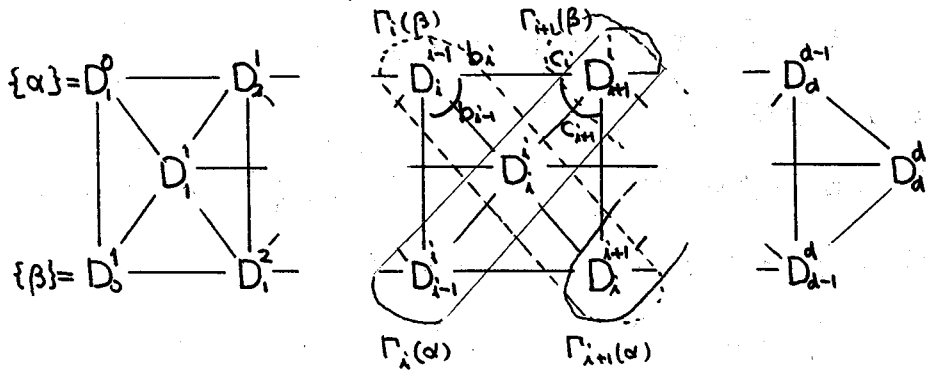
$$\{\alpha\} = D_0^0 \xrightarrow{b_0} D_1^1 \xrightarrow{c_1} \dots \xrightarrow{c_i} D_i^i \xrightarrow{b_i} D_{i+1}^{i+1} \xrightarrow{c_{i+1}} \dots \xrightarrow{c_d} D_d^d$$

$\boxed{1} \quad \boxed{1} \quad \quad \quad \boxed{1} \quad \quad \quad \boxed{1} \quad \quad \quad \boxed{1}$

$\#\{(r, \delta) \in D_i^i \times D_{i+1}^{i+1} \mid d(\alpha, \beta) = 1\}$ を二通りに数えることにより 次を得る。

$$r_i b_i = r_{i+1} c_{i+1}, \quad 1 = c_1 \leq c_i, \quad b_j \leq d \quad j \leq d-1$$

EXAMPLE 1. $d(\alpha, \beta) = r = 1$



$e(A, B) = \#\{(r, \delta) \in A \times B \mid d(r, \delta) = 1\}$ とすると.

($e(\{r\}, B) = e(r, B)$ とお書くと)

$r \in D_{i-1}^{i-1}$ としたとき. $r \in \Gamma_{i-1}(\alpha) \cap \Gamma_i(\beta)$ を用いて

$$b_i = e(r, D_{i+1}^i) \leq e(r, D_{i+1}^i) + e(r, D_i^i) + e(r, D_{i-1}^i) = b_{i-1}$$

従って $b_i \leq b_{i-1}$ がえらぬ 等号成立の時は.

$$e(r, D_i^i) = e(r, D_{i-1}^i) = 0 \quad \text{を得る.}$$

同様に. $c_i \leq c_{i+1}$ と. 等号成立の条件

$$e(D_{i+1}^i, D_i^i) = e(D_{i+1}^i, D_i^{i+1}) = 0 \quad \text{を得る.}$$

従って.

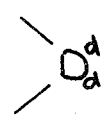
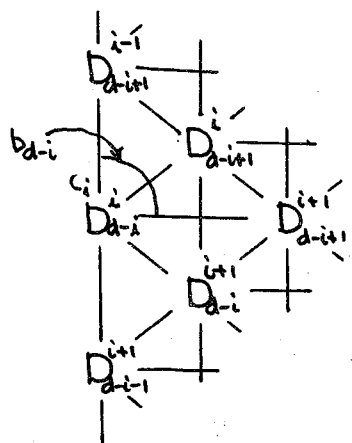
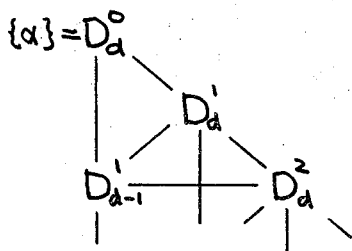
$$k = \frac{b_0}{c_1} \geq \frac{b_1}{c_2} \geq \dots \geq \frac{b_{d-1}}{c_d} > 0 \quad k_{i+1} = \frac{b_i}{c_{i+1}} k_i$$

よ) $\exists 0 \leq s \leq t \leq d$ s.t.

$$k = k_1 < k_2 < \dots < k_s = k_{s+1} = \dots = k_t > k_{t+1} > \dots > k_d$$

k_i の unimodal property を得る.

EXAMPLE d $d(\alpha, \beta) = r = d$ diameter



$\{\beta\} = D_0^d$

$r \in D_{d-i}^i$ とすると.

$$c_i = e(r, D_{d-i+1}^{i-1}) \leq e(r, D_{d-i+1}^{i-1}) + e(r, D_{d-i+1}^i) + e(r, D_{d-i+1}^{i+1}) = b_{d-i}$$

かつ、 $c_i = b_{d-i}$ のときは $e(D_{d-i}^i, D_{d-i+1}^i \cup D_{d-i+1}^{i+1}) = 0$.

さらに、 b_i の単調減少性より、 $c_i \leq b_{d-i} \leq b_{d-i-1} \leq \dots \leq b_1$

すなわち、 $c_i \leq b_j$ if $i+j \leq d$ を得る。

さらに、 $i+j \leq d$, $i \leq j$ とすると。

$$r_j = \frac{b_{j-1} \cdots b_i}{c_j \cdots c_{i+1}} \quad r_i = \frac{\underbrace{b_{j-1} \cdots b_i}_{\substack{v_i \\ 1}}}{\underbrace{c_{i+1} \cdots c_j}_{\substack{v_i \\ 1}}} \quad r_i \geq r_j$$

より、次の結果を得る。

$$r_i \leq r_j \quad \text{if} \quad i+j \leq d, \quad i \leq j \quad \text{---} \quad (1)$$

$$r_i = r_j \quad \text{ならば} \quad b_i = c_j, \quad b_{i+1} = c_{j-1}, \quad \dots, \quad b_{j-1} = c_{i+1}.$$

以上の要点をまとめると。

Basic Properties of Parameters.

(1). $c_i + a_i + b_i = k$, $0 \leq i \leq d$.

(2). $1 = c_1 \leq c_2 \leq \dots \leq c_d$

(3). $k = b_0 \geq b_1 \geq \dots \geq b_{d-1} \geq 1$

(4). $r_i b_i = r_{i+1} c_{i+1}$

(5). r_i has unimodal property. i.e., $\exists 0 \leq l \leq m \leq d$ s.t.

$$1 = r_0 < r_1 < \dots < r_l = r_{l+1} = \dots = r_m > \dots > r_d$$

(6). $b_i \geq c_j$ if $i+j \leq d$.

(7). $r_i \leq r_j$ if $i+j \leq d$, $i \leq j$.

(8). If $r_i = r_j$ with $i+j \leq d$, $i < j$,

then $b_i = c_j$, $b_{i+1} = c_{j-1}$, \dots , $b_{j-1} = c_{i+1}$.

3. $k_i = k_j$

この節では 前節末の (8) の精密化の定理を紹介する。

THEOREM 1. Γ : DRG. d : diameter

Suppose $k_e = k_f \neq k_{f+1}$ with $0 \leq e < f$, $e+f \leq d$.

Then $e+f=d$ and one of the following holds.

(i) $k_i = k_{d-i}$ $0 \leq i \leq d$, i.e., antipodal 2-cover.

(ii) $k_e = k_{e+1} = \dots = k_{d-e}$, $a_d \neq 0$ and

$$b_e = \dots = b_{d-e-1} = b_{d-e} = c_{e+1} = \dots = c_{d-e}$$

For any vertex u in Γ , $\Gamma_d(u)$ is a clique

of size a_{d+1} . Moreover if $d \geq 3e$, then

$$e=1 \text{ and } k=2.$$

これより次の系を得る。この系は [BCN, p168]

での予想の一つを解決している。

COR. Γ : DRG. d : diameter. Suppose $k_e = k_f$

with $0 \leq e < f$, $e+f \leq d$. Then one of the following holds.

(i) $k_i = k_{d-i}$ $0 \leq i \leq d$ and $e+f=d$

(ii) $k_e = k_{e+1} = \dots = k_f$.

もう一歩進んで次は興味深い問題である。

問題. Γ : DRG d : diameter, $k > 2$ valency.

$k_e = k_f$, $0 \leq e < f$, $e+f \leq d$ ならば 常に.

$k_i = k_{d-i}$, $0 \leq i \leq d$ and $e+f = d$. すなわち

antipodal 2-cover である. COR の (ii) は あらうか? ?

DRG Γ の height h

$h(\Gamma) = \max \{ m \mid p_{\alpha m}^d \neq 0 \}$ と定義すると.

antipodal 2-cover. すなわち (i) が成立するのは.

$h(\Gamma) = 0$ と同値であり. THM 1 の (ii) にあらか

ねる $Q_d \neq 0$ かつ $\Gamma_d(u)$: clique という条件は

$h(\Gamma) = 1$ と同値である. $h(\Gamma) = 1$ である DRG

は [BCN] では generalized odd graph とよばれる

ている.

THEOREM 1 の証明は多少複雑になるので. ここでは

$e=2$, $f=4$ とし. COR の証明を与える。

COR の証明 ($e=2$, $f=4$).

$k_2 = k_4$ とする.

① $k_4 > k_5$, $c_5 > b_4$ と仮定してよい。

(\because) (5) (前節末 Basic Properties. 以下番号のみで引用)
より. $k_2 = k_4$ から $k_2 \geq k_5$ を得る. $k_4 = k_5$ とする
と. 同様に $k_2 = k_3 = k_4 = k_5$ を得. (ii) を得るので
 $k_4 > k_5$ としてよい. (4) より $c_5 > b_4$ を得る.

② $d = 6$.

(\because) 仮定から $d \geq 2+4 = 6$. $d \geq 7$ とすると
(7) より $k_2 \leq k_5$ となり ① に矛盾.

③ $k \geq c_6 \geq c_5 \geq c_4 \geq c_3 \geq c_2 \geq c_1 = 1$

$$\begin{array}{ccccccccc} & \wedge & & \wedge & & \parallel & & \parallel & & \wedge & & \wedge \\ k = b_0 & > & b_1 & \geq & b_2 & \geq & b_3 & \geq & b_4 & \geq & b_5 & > & 0 \end{array}$$

(\because) (2), (3), (6), (8) より 明らか.

④ $e(D_4^2, D_5^3 \cup D_4^3) = e(D_3^3, D_4^3 \cup D_4^4 \cup D_3^4)$
 $= e(D_2^4, D_3^4 \cup D_3^5) = 0$ τ 次元の diagram を得る.

(\because) 前節 EXAMPLE d 参照. ($c_4 = b_2, c_3 = b_3$)

⑤ $D_4^3 = D_3^4 = \phi$ としてよい。

(\because) ③ より $c_4 \geq b_3$. $r \in D_4^3$ とすると.

$$c_4 = e(r, D_3^4) \leq e(r, D_3^4) + e(r, D_4^4) + e(r, D_5^4) = b_3$$

よって $b_3 = c_4$. (4) より $k_3 = k_4$. (5) より

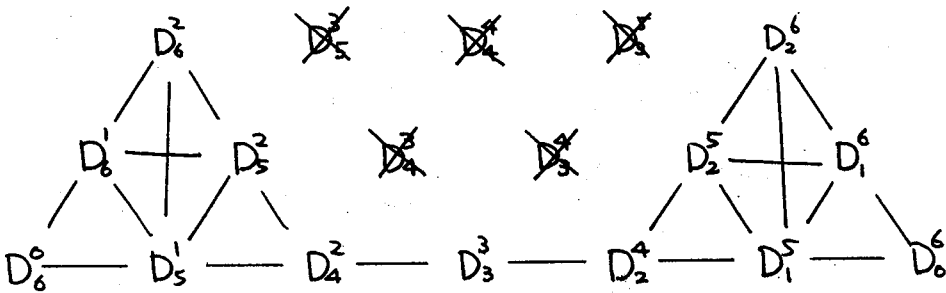
$k_2 = k_3 = k_4$ よって (ii) を得る。

⑦ $h(\Gamma) \leq 2$. としつゝ 11.

(\because) $D_6^3 \neq \emptyset$ とすると. $r \in D_6^3$ とし.

$$c_6 = e(r, D_5^2) \leq e(r, D_5^2) + e(r, D_6^2) = c_3$$

ゆゑより $b_3 = c_4$, $k_3 = k_4$ を得. (ii) を得る.



⑧ $h(\Gamma) = 0$.

(\because) D_6^2 又は $D_5^2 \neq \emptyset$ とすると. $b_2 = 0$ となり

矛盾. 同様に $D_6^1 = \emptyset$.

$h(\Gamma) = 0$ とすると. diagram から明らかなように $b_i = c_{6-i}$ を得る. よて $k_i = k_{6-i}$.

ここでは $k_i = k_{d-i}$ $0 \leq i \leq d$ を antipodal 2-cover の定義としたが. $k_d = 1$ のみから. antipodal 2-cover が言えることは. diagram 又は (8) から簡単にわかる. antipodal graph は imprimitive である. (より小さな graph の場合)

4. $b_e = 1$.

この節では、性質 (3) において、どれぐらい前のオまで b_i が 1 となりうるか、という問題を考える。

この問題については 次の結果が知られている。

Godsil diameter bound. [G] [BCN]

If $b_e = 1$, then $d < 3e$.

さらに $d = 3e - 1$ の時は Lambeck が Γ は 12 面体であることを示している。すなわち

$$L(\Gamma) = \begin{Bmatrix} * & 1 & 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 1 & 1 & * \end{Bmatrix}$$

これは antipodal 2-cover である。

$h(\Gamma)$ は、前節で定義した height とし、さらに

$$e(\Gamma) = \min \{ m \mid b_m = 1 \}$$

$$r(\Gamma) = \max \{ m \mid a_0 = a_1 = \dots = a_m = 0 \}$$

$$s(\Gamma) = \max \{ m \mid c_m = 1 \}$$

とする。これらは、 n と場合により少しずつ異なるものの DRG の研究において非常に重要な数である。

THEOREM 2. Γ : DRG. d : diameter, k : valency

Suppose $k > 2$, $k_d \neq 1$ (i.e., Γ is not an antipodal

2-cover) $b_e = 1$ with $d \geq 2e + 1$. Then

$$(1) \quad d \leq \frac{5}{2}e - 4$$

(2) If $k \geq 5$

$$d < 2e + \frac{\log(k-1)}{\log(k-1) + \log(k-3)} \left(\frac{1}{2}e + 2 \right) - 4$$

$$\leq \frac{1}{2} \left(4 + \frac{\log(k-1)}{\log(k-1) + \log(k-3)} \right) e - \frac{8}{3}$$

$$\leq \frac{7}{3}e - \frac{8}{3}.$$

(2) において k が十分大きいと、 d は大体

$2.25e$ 程度でおさえられることを意味している。

しかしそれでもまだ Best possible ではなく、 $2e$ 程度

でおさえられるのではないうだろうか。

問題. Γ : DRG. d : diameter, k : valency.

$k_d \neq 1$, $k > 2$, $b_e = 1 \Rightarrow d < 2e$?

$b_e = 1$, $d \geq 2e$ とすると 性質 (6) より $c_e = 1$.

従って intersection array は $e=e(\Gamma)$, $r=r(\Gamma)$
 $s=s(\Gamma)$ を用いると次の様になる。

$$L(\Gamma) = \begin{pmatrix} * & 1 & \cdots & 1 & \cdots & 1 & 1 & \cdots & 1 & c_{s+1} & c_d \\ 0 & 0 & & 0 & \cdots & a_{e-1} & k-2 & & k-2 & & a_d \\ k & k-1 & & \underbrace{k-1}_{r=2} & \cdots & b_{e-1} & 1 & & 1 & 1 & \cdots & 1 & * \\ & & & & & \underbrace{1}_{1} & \underbrace{b_e}_{s-e+2} & & \underbrace{b_s}_{s-e+2} & & & & \end{pmatrix}$$

ここでさらに $k > 2$, $k_d \neq 1$, $d \geq 2e+1$ を仮定し
 $h=h(\Gamma)$ とおくと 次の不等式がえられる。

- (0) $r \leq e-1$, $0 < r$
- (I) $d-e + [(h+1)/2] \leq s$ [] は かな記号
- (II) $s-e+3 \leq r$, if $r \geq 5$
 $s-e+2 \leq r$, if $r \geq 3$
 $s-e \leq r$
- (III) $h \geq 2d-4e+3$
- (IV) $h \geq r+1$
- (V) $(k-3)^{r+1} < (k-1)^{2e-s}$

(II) の 2番目 3番目は A.V. Ivanov の結果. (I) は
 K. Nomura の結果で. (0)~(IV) を用いると THM 2

の (1) がえられ、(V) をあわせて用いると (1) の改良である (2) が得られる。

(0) の前半は明らか。

(I) は rank d の diagram による前節の議論を用いて証明される。

(II) は、 $(c_1, a_1, b_1) = \dots = (c_r, a_r, b_r)$,

$(c_u, a_u, b_u) = \dots = (c_{u+m-1}, a_{u+m-1}, b_{u+m-1}) \neq (c_{u+m}, a_{u+m}, b_{u+m})$

で $c_u = 1$, $r < u$ $b_u \neq b_{u-1}$ なる時の r による m の bound である。あとの \Rightarrow は rank 1 の diagram の応用。最初のものは rank 2 の diagram の応用である。

(III), (IV) は rank d の diagram 上で様な path を用いて示す。

(V) は、 $\alpha, \beta \in \Gamma$ $d(\alpha, \beta) = 2e$ とした時、

D_e^e が a_e -regular であることを用いて示される。

Intersection array において、 $(c_i, a_i, b_i) = (c, a, c)$

となる i の個数は、 $10R \cdot 2^R$ で押えられる。とい

う Bannai-Ito の結果があるか? $c=1$ のとき

特に $R \geq 4$ ならば、この数は 1? ではないだろうか。
(R は absolute const.)

5. Θ -polynomial DRG. \sim Concluding Remark \sim

$$R_i = \{(\alpha, \beta) \in \Gamma \times \Gamma \mid d(\alpha, \beta) = i\} \quad 0 \leq i \leq d.$$

とすると、 $(\Gamma, \{R_i\}_{0 \leq i \leq d})$ は P-polynomial association scheme という特別の symmetric association scheme になっている。又逆に、P-polynomial symmetric association scheme から DRG がえられる。

association scheme におけるこの dual な性質をみたすものとして Θ -polynomial association scheme があるが、DRG からつくった association scheme が Θ -polynomial となるとき、この DRG を Θ -polynomial DRG (簡単のため以後 Θ -DRG と称) という、知られている primitive な DRG で、diameter d が大きいもの (私の知る範囲では $d \geq 8$) はすべて Θ -DRG である。これに反し、 d が小さいもの (例えば $d \leq 4$) では、 Θ -DRG ではないものの方が多いくらいである。

Θ -DRG については、D. Leonard の定理があり、free parameter は 5 つで、これすべての c_i, a_i, b_i 達が書け、known な series の parameter に近いことが示されている。

従って DRG の研究は大きく 2 つに分けられる。

①-DRG の分類. すなわち, Leonard の定理にあらわれる parameter から, known (classical) DRG を特徴付けること. この問題. まだ先は大分遠いように思われるが, A.A. Ivanov, P. Terwilliger らによつてかなりの進展がみられる。

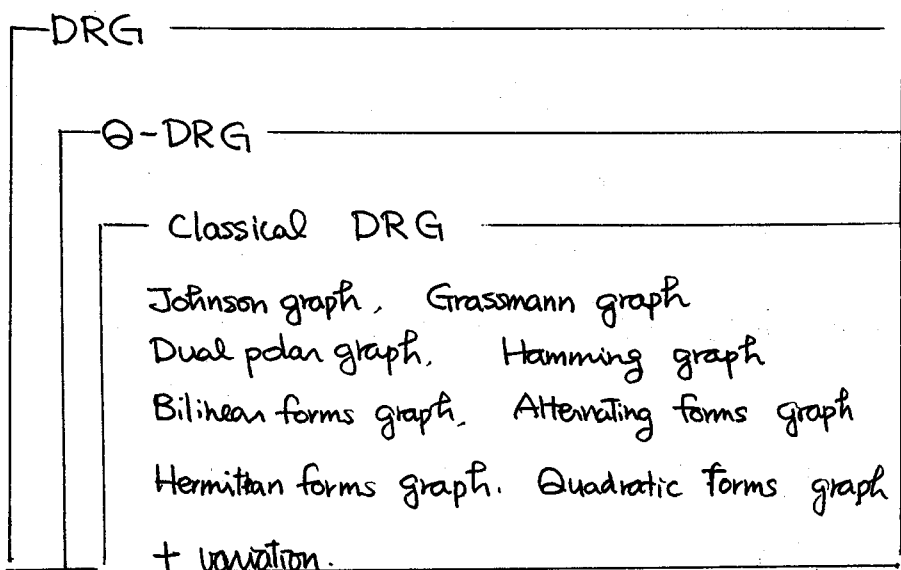
DRG と ①-DRG の Gap の研究. Bannai-Ito の予想の中に diameter が十分大な primitive DRG は ①-DRG ではないだろうか. というのがあるが, 今のところ, known DRG の list が, これそうら付けてはいるものの, 何の進展も得られていない。

①-DRG において 3 節の問題は, 私は check してはいるがおそらく正しいであろうし, ①-DRG においてはおそらく $be=1 \Rightarrow e \geq d-2$ くらいが成立しているであろう. 従つて, もし d が十分大なら ①-DRG という予想が正しいとすると, ここで紹介した Thm 1, 2 は甚だ 有名な定理ということになる. 現在の到達地点がここであるとするならば, この予想に関する研究はまだまだ先が長いことを意味しているとはいえないのではないか。

最後に. Brgs-Smith graph の intersection array を
記して結びとする.

$$c(\Gamma) = \begin{Bmatrix} * & 1 & 1 & 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 3 & 2 & 2 & 2 & 1 & 1 & 1 & * \end{Bmatrix}$$

- DRG τ \ominus -DRG τ の例. 知られていゝるもので
diameter 最大.
- $b_4=1$ $d=7$.
- Boshui-Nomura-Hiraki bound の限界を示す例
- $k=3$ τ primitive な diameter 最大の例
primitive τ 知られていゝる他のものは $d \leq 2k$ をみたす.
- $L_2(17) / \Sigma_4$ から得られる graph.



REFERENCES

BASES REFERENCES

[B-I] E. Bannai, T. Ito "Algebraic Combinatorics I" Benjamin 1984

[B-I Suppl.] —, — Current researches on algebraic combinatorics,
Graphs and Combin. 2 (1986), 287-308

[B] N.L. Biggs "Algebraic Graph Theory", Cambridge U.P. 1974

[BCN] A.E. Brouwer, A.M. Cohen and A. Neumaier, "Distance
Regular Graphs", Springer 1989

Section 3.

H. Suzuki, On a distance regular graph with $k_i = k_j$
preprint.

Section 4.

H. Suzuki, On a distance regular graph with $b_e = 1$
preprint.

[G] C.D. Godsil, Bounding the diameter of distance regular
graphs, Combinatorica 8 (1988)

[N] K. Nomura, Some inequalities in distance-regular
graphs. preprint.

東京医科歯科大学 野村 和正

1. 有向距離正則グラフの研究経過

距離正則グラフの理論における最大の問題の1つに、

「与えられた次数 $k > 2$ をもつ距離正則グラフは高々有限個か？」
というのがある。これは次数 k のある関数 $f(k)$ で直径 $d(G)$ を押さ
えるということと同値であるが、この問題に向かって多くの研究がな
されている。坂内 - 伊藤 [4], [5], [6], [7], A. A. Ivanov [11],
Terwilliger [15], [16], Biggs - Boshier - ShaweTaylor (次数 3 の
分類), Gardinar, Godsil 等多くの研究者がこの問題に取り組んでい
て、相当な進展を見せているが、一般に直径が押さえられているのは、
いまのところ次数が 3, 4 のときだけで、次数 5 の場合ですら、出来
ていない。

ここでは、距離正則グラフの non-symmetric version である有向
距離正則グラフについて同じ問題を考え、その肯定的な結論を得る。
有向距離正則グラフは Damerell [9], Lam [12] において導入された。
自明なものとしては、有向サイクルがあるが、これは除外しておく。坂
内 - Cameron - Kahn [1] により、「群の作用があるとき、内周が奇数
(≥ 5) のものはない」ことが示された。当時知られているものは
(サイクル以外は) すべて内周 3 であったが、榎本 - Mena [10] によ
り内周 4 の例 (64 点) が構成され、さらに Liebler - Mena [13] によ
り無限系列へと一般化された。この例に関しては、山田美枝子女史に

より詳しく研究されている。宗政氏は内周 5 の場合を研究し Q -polynomial なものは存在しないことを示した。内周 5 については、計算機による固有値の計算により $k \leq 20000$ のものは存在しないことがいえる。従って、内周 5 のものは存在しないのではないかと予想されるが、内周 6 については何ともいえない。

ここでは、特定の内周を扱うのをやめて、距離正則グラフの一般論を展開し、基本的なパラメータの間に成り立つ関係式を求める。

与えられた次数をもつ有向距離正則グラフの分類をする問題は、かねてから興味があったが、最近、伊藤達郎氏により $k \leq 7$ の場合の非存在が示され、それが、今回の研究の契機となった。

2. 有向距離正則グラフの定義

空でない集合 V と, $V \times V$ の部分集合 E の組を 有向グラフ という. ここでは V は有限集合とし, E は次の条件をみたしているとする.

$$(i) (x, x) \in E, \quad (ii) (x, y) \in E \text{ ならば } (y, x) \in E$$

V の元を 点, E の元を 辺 と呼ぶ. G の点の列

$$x_0, x_1, \dots, x_r$$

で, $(x_{i-1}, x_i) \in E$ ($1 \leq i \leq r$) をみたすものを, x_0 から x_r への長さ r の 道 という. とくに, $r > 0$ で $x_0 = x_r$ のときは, サイクル という. G の任意の2点 u, v に対して u から v への道があるとき, G は 連結 であるという. ここでは2点以上からなる連結グラフのみを扱う. G の2点 u, v に対して, u から v への道のうちで長さが最小のものを考え, その道の長さを u から v までの 距離 といい, $\partial(u, v)$ とかく. $\partial(u, u) = 0$ であることに注意.

$$d(G) = \max \{ \partial(u, v) \mid u, v \in V \}$$

を G の 直径 という. G は連結であるから, G にサイクルがある. G に含まれるすべてのサイクルのうちで長さが最小のものを考え, その長さを G の 内周 という.

G の2点 u, v と非負整数 j, l に対して

$$p_{j,l}(u, v) := \# \{ x \in V \mid \partial(u, x) = j, \partial(x, v) = l \}$$

によって定義される数 $p_{j,l}(u, v)$ が u から v への距離のみによって決まるとき, G は 距離正則 であるという. 正確にいうと,

$\partial(u, v) = \partial(u', v')$ をみたす点 u, v, u', v' に対して必ず

$$p_{jl}(u, v) = p_{jl}(u', v') \quad (\text{すべての } j, l \text{ について})$$

が成立していること. このとき $p_{jl}^i := p_{jl}(u, v)$ (ここで $i = \partial(u, v)$)

とかき, これを G の 交差数 という.

3. 得られた結果

G を有向距離正則グラフとし、 G の直径を d 、内周を g とする。
Damerell [] による次の定理が基本的である。

- 定理. (1) $(0 < \partial(u, v) < g)$ ならば $\partial(u, v) + \partial(v, u) = g$.
(2) $d = g$ (long type) または $d = g - 1$ (short type).
(3) long type のものはすべて short type のものから構成できる.

従って、有向距離正則グラフの分類問題を考えるときは、short type のものだけを扱えばよいことになる。以下、 $d = g - 1, k > 1$ を仮定する。ここで k は G の次数 (1点から出る辺の本数) である。また、次のパラメータを用いる。

$\lambda = u$ から v への長さ 2 の道の個数 ($\partial(u, v) = 1$ のとき)

$\mu = u$ から v への長さ 2 の道の個数 ($\partial(u, v) = 2$ のとき)

これらのパラメータは交差数を用いて次の様に表せるので、点のとりかたによらずに決まる。

$$k = p_{1g-1}^0, \quad \lambda = p_{11}^1, \quad \mu = p_{11}^2$$

最近、伊藤達郎氏により、「 $k \leq 7$ ならば $g = 3$ 」が示され、さらに彼は一般に $g \leq k$ が成り立つであろうと予想した。次の結果はこの予想に対する肯定的な答を与える。さらに、 k, λ, μ のうちのいずれか 1つを固定すると、そのような有向距離正則グラフ (short type) は高々有限個しかないことがわかる。

定理 1. $g \leq \mu + 2$.

定理 2. $2(g-3)(g-4) \leq (\lambda+1)(\lambda+1-\mu)$.

定理 2 から次の系が得られる.

系. $\mu \leq \lambda+1$. $g > 4$ のときは $\mu \leq \lambda$.

$g=3$ のときは, いつでも $\mu = \lambda+1$ が成立している. $g=4$ のときについては, 榎本-Mena の論文で詳しく調べられていて, それをよく読むと $\mu \leq \lambda$ が成立していることがわかる. 従って, 上の系における仮定は $g \geq 4$ としてよいことになる.

4. 基本的事項

この節では有向距離正則グラフに関する基本的な事柄をまとめておく。点 x から距離 i にある点全体の集合を $\Gamma_i(x)$ とかき、その点数を k_i とおく。次の補題は交差数の一般的な性質を与える。

補題 1. $0 < i, j, l < g$ をみたす i, j, l に対して

$$(1) p_{j l}^i = p_{l j}^i,$$

$$(2) p_{j l}^i = p_{g-j g-l}^{g-i},$$

$$(3) p_{i 1}^i = p_{i g-1}^i.$$

ここで、基本的なパラメータである a_i, b_i, c_i を次のように定義する。

$$a_i = p_{i 1}^i, \quad c_i = p_{i-1 1}^i, \quad (0 < i < g),$$

$$b_i = p_{i+1 g-1}^i \quad (0 < i < g-1), \quad b_{g-1} = 1.$$

いま $\vartheta(u, x) = i$ なる点 u, x を考えると、 x から $\Gamma_{i-1}(u)$ へ向かって c_i 本の辺が出ている。同様に x から $\Gamma_i(u)$ へは a_i 本、 $\Gamma_{i+1}(u)$ へは b_i 本の辺が出ている。 $a_1 = \lambda, b_1 = k - \lambda, c_1 = 1$ であることに注意。これらのパラメータには次の性質がある。

補題 2. $0 < i < g$ のとき、

$$(1) b_i = c_{g-i},$$

$$(2) 1 = c_1 \leq c_2 \leq \dots \leq c_{g-1},$$

$$(3) b_1 \geq b_2 \geq \dots \geq b_{g-1} = 1.$$

次の補題は $k_i = |\Gamma_i(u)|$ の性質を述べたものである。

補題 3. For any i with $0 < i < g$.

(1) $k_{i-1} b_{i-1} = k_i c_i$,

(2) $k_i = k_{g-i}$,

(3) $1 = k_0 \leq k_1 \leq k_2 \leq \dots \leq k_m$, where $m = \left\lfloor \frac{g}{2} \right\rfloor$.

(4) $k_2 = k(k - \lambda) / \mu$.

5. 証明

定理は次の様に定義されるパラメータ f_i, h_i を詳しく調べることに
により得られる. G の点 u をとる. $\Gamma_i(u)$ から $\Gamma_1(u)$ の点 x に向
かって出ている辺の本数を f_i , $\Gamma_i(u)$ の点 y から $\Gamma_1(u)$ に向かっ
て出ている辺の本数を h_i とする.

$$f_i = p_{i1}^{-1}, \quad h_i = p_{1g-i}$$

と表せるので, f_i, h_i は点 u, x, y の取り方によらずに決まる. 次の
補題は前節の補題と定義から容易に得られる.

補題 4.

- (1) $kf_i = k_i h_i \quad (0 \leq i < g),$
- (2) $f_i = f_{g-i}, \quad h_i = h_{g-i} \quad (0 < i < g),$
- (3) $f_0 = 1, \quad f_1 = f_{g-1} = \lambda, \quad h_0 = k, \quad h_1 = h_{g-1} = \lambda,$
- (4) $\sum_{i=0}^{g-1} f_i = k.$

補題 5.

- (1) $\sum_{i=2}^{g-2} f_i = k - 2\lambda - 1,$
- (2) $\sum_{i=2}^{g-2} h_i \leq \frac{(k - 2\lambda - 1)\mu}{k - \lambda}.$
- (3) $\sum_{i=2}^{g-2} f_i h_i = (\mu - 1)k - \lambda(\lambda + \mu),$

(証明) (1) 補題 4 の (3), (4) から出る.

(2) 次の関係 $k_2 \leq k_i, \quad k_2 \mu = k(k - \lambda)$ および $k_i h_i = k f_i$ から

$h_i \leq f_i \mu / (k - \lambda)$ ($2 \leq i \leq g - 2$) がわかる. これと (1) から (2) が出る.

(3) $\Gamma_{g-1}(u)$ から $\Gamma_1(u)$ への長さ 2 の道 (x, y, z) の本数を 2 通りの方法で数える. まず $\Gamma_i(u)$ の点 y をとる. すると $\Gamma_1(u)$ の点 z で y からの距離が 1 のものが h_i 点あり, また $\Gamma_{g-1}(u)$ の点 x で $\partial(x, y) = 1$ となるものが $p_{g-1}^i = p_{1, g-1}^i = h_i$ 点ある. 従って, 道 (x, y, z) の個数は $\sum_{i=0}^{g-1} k_i h_i^2$.

次に, $\Gamma_{g-1}(u)$ の点 x を最初にとる. ここで $\Gamma_1(u)$ の点は x から距離 1 または 2 であることに注意せよ. x からの距離が 1 であるような $\Gamma_1(u)$ の点は ちょうど λ 個あることが容易にわかる. 従って, x からの距離が 2 であるような $\Gamma_1(u)$ の点は $k - \lambda$ 個ある. いま $\Gamma_1(u)$ の点 z をとると, $\partial(x, z) = 1$ のときは $\partial(x, y) = \partial(y, z) = 1$ となる点 y は λ 個あり, $\partial(x, z) = 2$ のときは同様の点 y は μ 個ある. 従って x から $\Gamma_1(u)$ への長さ 2 の道は $\lambda^2 + (k - \lambda)\mu$ 個ある. 従って

$$\sum_{i=0}^{g-1} k_i h_i^2 = k(k - \lambda)\mu + k\lambda^2$$

を得る. これと 補題 4 の (1), (3) を用いて (3) を得る.

V の部分集合 X の各点 x が

$$|X \cap \Gamma_1(x)| = |X \cap \Gamma_{g-1}(x)| = r$$

をみたすとき, X は r -正則な部分集合であるということにする.

補題 6. X を V の r -正則な部分集合 ($r > 0$) とし, u を X の点とする. このとき, 各 i ($0 \leq i < g$) に対して, X は $\Gamma_i(u)$ と交わ

る.

(証明) u を通る X のサイクル $C: u = x_0, x_1, \dots, x_{m-1}, x_m = u$ があることは明か. x_{m-1} は $\Gamma_{g-1}(u)$ に入る. すなわち $C \cap \Gamma_{g-1}(u) \neq \emptyset$. このことから容易に $C \cap \Gamma_i(u)$ ($0 \leq i \leq g-1$) がわかる.

補題 7. $\mu > 1, \lambda > 0$.

(証明) 補題 5 の (3) において $\mu = 1$ とおいてみると, $\lambda = 0, f_i = 0$ でなければならないが, すると補題 5 の (1) から $k-1=0$ となり, $k > 1$ の仮定に反する. 従って $\mu > 1$. 次に $\lambda = 0$ とすると, 補題 5 の (2) から $\sum_{i=2}^{g-2} h_i \leq \mu - 1$. これは補題 5 の (1), (3) に反する.

補題 8. $f_i > 0, h_i > 0$ ($0 \leq i \leq g-1$).

(証明) V の点 u と $\Gamma_1(u)$ の点 x をとり, $X = \Gamma_{g-1}(x)$ に対して補題 6 を適用する. X は λ -正則であり, 補題 7 より $\lambda > 0$ であるから X は各 $\Gamma_i(u)$ と交わる. 従って $f_i = |X \cap \Gamma_i(u)| > 0$. これから $h_i > 0$ は明か.

補題 9. $k < k_i$ ($2 \leq i \leq g-2$).

(証明) ある i ($2 \leq i \leq g-2$) について $k \geq k_i$ となったとする.
 すると 補題 3 (3) より $k = k_2$ となり, さらに 補題 3 (4) より
 $k - \lambda = \mu$, $k = \lambda + \mu$ が出る. 一方, 補題 8 より $f_2 > 0$ であるか
 ら, $\Gamma_2(u)$ から $\Gamma_1(u)$ へ向かう辺 (x, y) がある. いま,
 $A = \Gamma_1(u) \cap \Gamma_1(y)$, $B = \Gamma_1(u) \cap \Gamma_{g-1}(x)$ とおくと, いまの場合は
 $g > 3$ であるから $\{y\} \cap A \cap B = \emptyset$ となり, $k \geq 1 + \lambda + \mu$ が出る.
 これは上で得た $k = \lambda + \mu$ に反する.

補題 10. $f_i \geq 2$ ($2 \leq i \leq g-2$).

(証明) 補題 9 と 補題 4 (1) から出る.

(定理 1 の証明) 補題 5 (2) より $\sum_{i=2}^{g-1} h_i \leq \mu - 1$ を得るが, する
 と補題 8 から $g-3 \leq \mu - 1$.

(定理 2 の証明) 補題 5 (2) より $\sum_{i=2}^{g-1} h_i \leq \mu - 1$. 補題 5 (1),

(3) および 補題 8, 補題 10 から

$$\begin{aligned} (\mu - 1)k - \lambda(\lambda + \mu) &= \sum_{i=2}^{g-2} f_i h_i \leq \left(\sum_{i=2}^{g-2} f_i \right) \left(\sum_{i=2}^{g-2} h_i \right) - 2(g-3)(g-4) \\ &\leq (k - 2\lambda - 1)(\mu - 1) - 2(g-3)(g-4). \end{aligned}$$

この式を変形することにより $(\lambda - \mu + 1)(\lambda + 1) \geq 2(g-3)(g-4)$.

参照文献

1. E. BANNAI, P. J. CAMERON AND J. KAHN, Nonexistence of certain distance-transitive digraphs, *J. Combin. Theory Ser. B* 31 (1981) 105-110.
2. E. BANNAI AND T. ITO, "Algebraic Combinatorics I," Benjamin, 1984.
3. E. BANNAI AND T. ITO, Current research on algebraic combinatorics, *Graphs and Combinatorics* 4 (1986) 287-308.
4. E. BANNAI AND T. ITO, On distance-regular graphs with fixed valency, *Graphs and Combinatorics* 3 (1987) 95-109.
5. E. BANNAI AND T. ITO, On distance-regular graphs with fixed valency II, *Graphs and Combinatorics* 4 (1988) 219-228.
6. E. BANNAI AND T. ITO, On distance-regular graphs with fixed valency III, *J. Algebra* 107 (1987) 43-52.
7. E. BANNAI AND T. ITO, On distance-regular graphs with fixed valency IV, submitted.
8. E. BANNAI AND T. ITO, On distance-regular graphs with fixed valency V, submitted.
9. R. M. DAMERELL, Distance-regular and distance-transitive digraphs, *J. Combin. Theory Ser. B* 31 (1981) 46-53.
10. H. ENOMOTO AND R. A. MENA, Distance-regular digraphs of Girth 4, *J. Combin. Theory Ser. B* 43 (1987) 293-302.
11. A. A. IVANOV, Bounding the diameter of a distance-regular graph, *Sov. Math. Dokl* 28 (1983) 149-152.

12. C. W. H. LAM, Distance-transitive digraphs, *Discrete Math.* 29 (1980), 265-274.
13. R. A. LIEBLER AND R. A. MENA, Certain distance-regular digraphs and related rings of characteristic 4, *J. Combin. Theory Ser. A* 47 (1988).
14. A. MUNEMASA, On non-symmetric P- and Q-polynomial association schemes, to appear in *J. Combin. Theory Ser. B*.
15. P. TERWILLIGER, The diameter of bipartite distance-regular graphs, *J. Combin. Theory Ser. B* 32 (1982) 182-188.
16. P. TERWILLIGER, Distance-regular graphs with girth 3 or 4, *J. Combin. Theory Ser. B* 39 (1985) 265-281.
17. M. YAMADA, Distance-regular digraphs of girth 4 over an extension ring of $\mathbb{Z}/4\mathbb{Z}$, to appear in *Graphs and Combinatorics*.

Exact coverings of 2-paths by Hamilton cycles

— A solution of Dudeney's round table problem for even persons

静岡県立大学 小林みどり
半導体研究所 喜安 善市
静岡県立大学 中村 義作

1. Introduction

1905年に Dudeney は 次の円卓問題を提出した [2, problem 273]:

“ n 人の人を $\frac{(n-1)(n-2)}{2}$ 回円卓に座らせ、どの人も同じ 2 人を 2 回以上両隣りに持つことのないようにせよ。つまり、どの人も、任意の 2 人の間に 1 回、しかもただ 1 回座るようにせよ。”

この問題は、完全グラフ K_n において、任意の 2-path (長さ 2 の path) をちょうど 1 回ずつ含むような Hamilton cycle の集合を求めると同値である。そのような性質を持つ Hamilton cycle の集合を、Dudeney set と呼ぶこととする。

K_n の 1-factorization は、それらに含まれる任意の 2 つの 1-factor の和が Hamilton cycle となるとき、perfect と呼ばれる。 K_n に perfect 1-factorization が存在すれば、Dudeney set $\mathcal{D} = \{FUF'\}$ $F, F' \in \mathcal{F}$ が得られる。

K_n の Dudeney set は、 $n = p+1, 2p$ (p は素数), $n = p^e+1$
 (p は素数, e は自然数), $n = p+2$ (p は素数, 2 が p の原始根),
 $n = pq+1$ (p, q は相異なる奇素数), $n = p^e q^f + 1$ (p, q は相
 異なる奇素数, $p \geq 5, q \geq 11; e, f$ は自然数) のとき構成され
 ている [1, 3, 4, 6, 10, 11]. $n = p^e+1$ (p は奇素数, e は 2 以上の自然
 数) のときは、異なる 2 つの方法で Dudeney set が構成され
 ている [4, 11]. さらに、 K_{n+1} の Dudeney set が存在すれば、
 K_{2n} の Dudeney set が存在することも知られている [3].

一方、 n が偶数のとき、 K_n の任意の 2-path をちょうど 2 回お
 っ持つような Hamilton cycle の family は既に構成されてい
 る [7].

ここでは、 n が任意の偶数のとき、 K_n の Dudeney set を構
 成する。即ち、

Theorem 1.1 n が偶数のとき、 K_n の枝全体は、任意の 2-path
 をちょうど 1 回含むような Hamilton cycle の集合により覆われる。

2. 記号と準備

n を任意の偶数 > 0 とする. $n=2a$ ときは, ϕ が K_2 の

Dudeney set であるから, $n \geq 4$ としおく. $n=m+1$,

$r = \frac{m-1}{2}$ とおく. $K_n = (V_n, E_n)$ を n 個の頂点を持つ完全

グラフ, $V_n = \{\infty\} \cup Z_m = \{\infty\} \cup \{0, 1, 2, \dots, m-1\}$ を頂点集合

(ここで Z_m は $\text{mod } m$ の剰余類群), E_n を枝集合とする.

任意の整数 i ($0 \leq i \leq m-1$) について, 1-factor F_i を定義

する: $F_i = \{\{\infty, i\}\} \cup \{\{a, b\} \in E_n \mid a, b \neq \infty, a+b \equiv 2i \pmod{m}\}$.

$\sigma = (\infty)(0\ 1\ 2 \dots m-1)$ を V_n の置換とし, $\Sigma = \langle \sigma \rangle$ とおく. K_n の

cycle の集合 \mathcal{C} に対して, $\Sigma \mathcal{C} = \{\sigma^t C \mid 0 \leq t \leq m-1, C \in \mathcal{C}\}$ と

決めおこす.

K_n の次の性質を (A_n) とおく:

(A_n) (1)(2) の性質を満たす K_n の 1-factor G_1, G_2, \dots, G_r が存在する.

(1) $F_0 \cup G_i$ ($1 \leq i \leq r$) は Hamilton cycle であり, $\Sigma \{F_0 \cup G_i \mid 1 \leq i \leq r\}$

は Dudeney set である.

(2) $(\bigcup_{i=1}^r G_i) \cap (\bigcup_{i=1}^r (-G_i)) = \emptyset$.

p が素数 $a \geq 7$. K_{p+1} は性質 (A_{p+1}) を満たしている. 以下,

[4] 例) K_{p^2+1} (p は奇素数, e は自然数) も性質 (A_{p^2+1}) を

満たしている.

3. K_n の Dudeney set を構成する 1-factor の定義.

n を任意の偶数 ≥ 4 とし、§3 と同じく、 $n = m+1$, $r = \frac{m-1}{2}$ とおく。 m が素数中では"、 K_n には Dudeney set が存在する"、 m は素数中で"と仮定する。すると、 $m = m_1 m_2$, $(m_1, m_2) = 1$, $m_1, m_2 \neq 1$ とかける。一般性を失うことなく、 $m_1 < m_2$ とする。 $l = 1, 2$ に対し、 $n_l = m_l + 1$, $r_l = \frac{m_l - 1}{2}$ とおき、完全グラフ $K_{n_l} = (V_{n_l}, E_{n_l})$, $V_{n_l} = \{\infty_l\} \cup \mathbb{Z}_{m_l} = \{\infty_l\} \cup \{0, 1, 2, \dots, m_l - 1\}$ を考へる。

$(m_1, m_2) = 1$ であるから、 \mathbb{Z}_m は $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ に同型である。

$$V_n = \{\infty\} \cup \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \mid a_1 \in \mathbb{Z}_{m_1}, a_2 \in \mathbb{Z}_{m_2} \right\}$$

と表すことができる。 $l = 1, 2$ に対し、 K_{n_l} の $F_0 \in F_0^{(l)}$ とおき、 K_n の $F_0 \in F_0^{(l)}$ とかく：

$$F_0^{(l)} = \left\{ \left\{ \infty, \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right\} \in E_n \mid a_2 + b_2 \equiv 0 \pmod{m_l} \ (l=1, 2) \right\}.$$

$l = 1, 2$ に対し、 K_{n_l} は性質 (A_{n_l}) を満たすことと仮定する： $G_1^{(l)}$, $G_2^{(l)}$, \dots , $G_{r_l}^{(l)}$ は次の (1)(2) を満たす K_{n_l} の 1-factor とする。

(1) $F_0^{(l)} \cup G_i^{(l)}$ ($1 \leq i \leq r_l$) は、 K_{n_l} の Hamilton cycle τ , $\Sigma^{(l)} \setminus F_0 \cup G_i^{(l)} \mid 1 \leq i \leq r_l$ は、 K_{n_l} の Dudeney set である。

$$(2) (U G_i^{(l)}) \cap (U (-G_i^{(l)})) = \emptyset.$$

3つのindex set を定義する: $I = \{i \mid 1 \leq i \leq n\}$, $J = \{j \mid 1 \leq j \leq n\}$,
 $J' = J \cup -J$. 且し, K_{n_2} の 1-factor を定義する: $G_j^{(2)} = -G_j^{(2)}$ ($j \in J$),
 且し, $v_i, w_j \in \mathbb{F}$, $(\infty_1, v_i) \in G_i^{(1)}$ ($i \in I$), $(\infty_2, w_j) \in G_j^{(2)}$ ($j \in J$)
 を満たす頂点とする.

以上のものを用いて K_n の 1-factor を定義する:

(1) $i \in I, j \in J'$ に対し

$$G_{(j)}^{(i)} = \left\{ \left\{ \infty, \begin{pmatrix} v_i \\ w_j \end{pmatrix} \right\} \right. \\
\cup \left\{ \left\{ \begin{pmatrix} v_i \\ a \end{pmatrix}, \begin{pmatrix} v_i \\ b \end{pmatrix} \right\} \mid a, b \neq \infty_2, \{a, b\} \in G_j^{(2)} \right\} \\
\cup \left\{ \left\{ \begin{pmatrix} a \\ w_j \end{pmatrix}, \begin{pmatrix} b \\ w_j \end{pmatrix} \right\} \mid a, b \neq \infty_1, \{a, b\} \in G_i^{(1)} \right\} \\
\cup \left\{ \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right\} \mid \{a_1, b_1\} \in G_i^{(1)}, \{a_2, b_2\} \in G_j^{(2)} \right\}.$$

(2) $i \in I$ に対し

$$G_{(i)}^{(i)} = \left\{ \left\{ \infty, \begin{pmatrix} v_i \\ 0 \end{pmatrix} \right\} \right. \\
\cup \left\{ \left\{ \begin{pmatrix} v_i \\ a \end{pmatrix}, \begin{pmatrix} v_i \\ b \end{pmatrix} \right\} \mid a, b \neq \infty_2, \{a, b\} \in F_0^{(2)} \right\} \\
\cup \left\{ \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right\} \mid \{a_1, b_1\} \in G_i^{(1)}, a_2 + b_2 \equiv 0 \pmod{m_2} \right\}.$$

(3) $j \in J$ に対し

$$G_{(j)}^{(j)} = \left\{ \left\{ \infty, \begin{pmatrix} 0 \\ w_j \end{pmatrix} \right\} \right. \\
\cup \left\{ \left\{ \begin{pmatrix} a \\ w_j \end{pmatrix}, \begin{pmatrix} b \\ w_j \end{pmatrix} \right\} \mid a, b \neq \infty_1, \{a, b\} \in F_0^{(1)} \right\} \\
\cup \left\{ \left\{ \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right\} \mid a_1 + b_1 \equiv 0 \pmod{m_1}, \{a_2, b_2\} \in G_j^{(2)} \right\}.$$

K_n は n 頂点の 1-factor を \mathbb{Z} で表すことを考えよう。 $F_0^{(i)} \cup G_i^{(i)}$ ($i \in \mathbb{I}$)

は、 K_n の Hamilton cycle となる。

$$F_0^{(1)} \cup G_i^{(1)} = (\infty_1, x_{1i} = 0, x_{2i}, x_{3i}, \dots, x_{n_1-1,i} = v_i)$$

と表すことが出来る。 となる。

$$\{\infty_1, x_{1i}\} \in F_0^{(1)}, \{x_{1i}, x_{2i}\} \in G_i^{(1)}, \{x_{2i}, x_{3i}\} \in F_0^{(1)}, \dots, \\ \{x_{n_1-2,i}, x_{n_1-1,i}\} \in F_0^{(1)}, \{x_{n_1-1,i}, \infty_1\} \in G_i^{(1)}$$

とすればよい。 $F_0^{(2)} \cup G_j^{(2)}$ ($j \in \mathbb{J}$) についても同様。

$$F_0^{(2)} \cup G_j^{(2)} = (\infty_2, y_{1j} = 0, y_{2j}, y_{3j}, \dots, y_{n_2-1,j} = w_j),$$

$$\{\infty_2, y_{1j}\} \in F_0^{(2)}, \{y_{1j}, y_{2j}\} \in G_j^{(2)}, \{y_{2j}, y_{3j}\} \in F_0^{(2)}, \dots, \\ \{y_{n_2-2,j}, y_{n_2-1,j}\} \in F_0^{(2)}, \{y_{n_2-1,j}, \infty_2\} \in G_j^{(2)}.$$

と表すことが出来る。 となる。 $G_{(j)}$ ($i \in \mathbb{I}, j \in \mathbb{J}$) は、Figure 1 で表す

ことが出来る。 Figure の各 cell は、 K_n の頂点 ($\neq \infty$) を表す。 cell

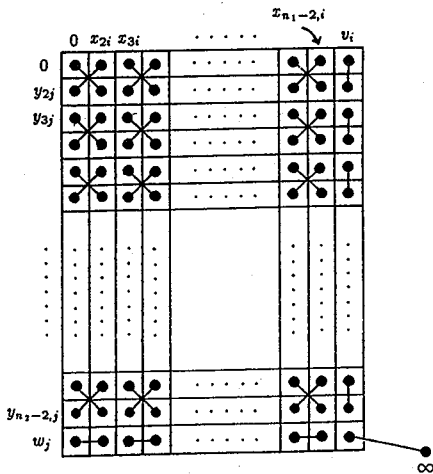


Figure 1 $G_{(i)}$

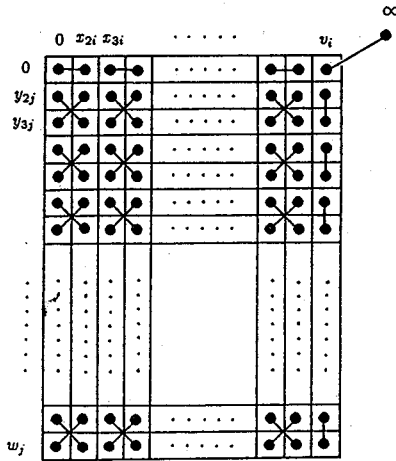


Figure 2 $G_{(i)}$

$\begin{pmatrix} x_{2i} \\ y_{2j} \end{pmatrix}$ は、頂点 $\begin{pmatrix} x_{2i} \\ y_{2j} \end{pmatrix}$ を表している。次に $G_{(i)}^{(1)}$ ($i \in I$) は、Figure 2 で表すことができる、こゝで縦軸は、任意の $G_j^{(2)}$ ($j \in J'$) をとる。最後に $G_{(j)}$ ($j \in J$) は、Figure 3 で表すことができる、こゝで横軸は、任意の $G_{(i)}^{(1)}$ ($i \in I$) をとる。 $F_{(i)}$ ($i \in I$) は、Figure 4 で表すことができる、こゝで、横軸は任意の $G_{(i)}^{(1)}$ ($i \in I$)、縦軸は任意の $G_j^{(2)}$ ($j \in J$) をとる。

次に、これらの種類の 1-factor と $F_{(i)}$ との和の cycle 構造を考へよう。まず、 $F_{(i)} \cup G_{(j)}$ ($i \in I, j \in J'$) は Hamilton cycle である (Figure 5)。次に $F_{(i)} \cup G_{(i)}$ ($i \in I$) は、長さ $\pm m_1 + 1$ の 1 個の cycle と、長さ $\pm 2m_1$ の r_2 個の cycle から成る (Figure 6)。最後に $F_{(i)} \cup G_{(j)}$ ($j \in J$) は、長さ $\pm m_2 + 1$ の 1 個の cycle と長さ $\pm 2m_2$ の r_1 個の cycle から成る (Figure 7)。

$$G = \{ G_{(j)} \mid i \in I, j \in J' \} \cup \{ G_{(i)} \mid i \in I \} \cup \{ G_{(j)} \mid j \in J \} \text{ とおく}$$

とし、 $(\cup_{G \in G} G) \cap (\cup_{G \in G} G) = \emptyset$ が成りたつことは可成り証明できる。すなわち、

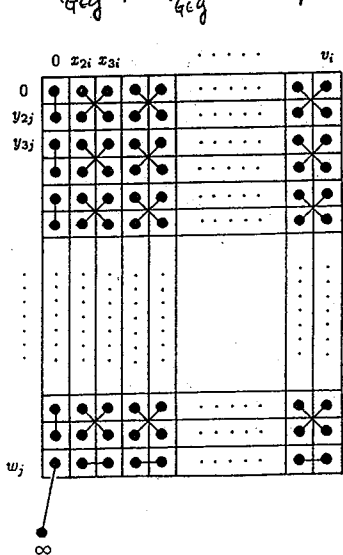


Figure 3 $G_{(j)}^{(1)}$

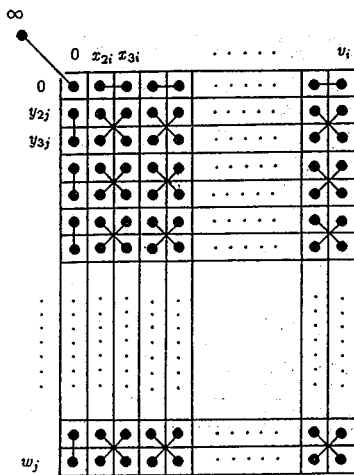


Figure 4 $F_{(i)}$

$\Sigma\{F(i) \cup G \mid G \in \mathcal{G}\}$ は, K_n の任意の 2-path をちょうど 1 回ずつ含む
 ことも証明される. よって $F(i) \cup G$ ($G \in \mathcal{G}$) が Hamilton cycle ならば,
 $\Sigma\{F(i) \cup G \mid G \in \mathcal{G}\}$ は Dudeney set となるが, 先程述べたように,
 $F(i) \cup G(i)$ ($i \in I$) と $F(j) \cup G(j)$ ($j \in J$) は Hamilton cycle とはならず
 11 の 2, Hamilton cycle となるように枝交換を行わなければならない.

4. 枝交換

$G(i) \cup G(j)$ ($i \in I, j \in J$) は, Figure 1 と 2 を重ねてみれば
 わかるように, Hamilton cycle とはならない. その cycle 構造は

$$G(i) \cup G(j) = C_1 \cup C_2 \cup \dots \cup C_{r_1} \cup C_{r_1+1},$$

ところで $\{(0, \begin{pmatrix} x_{2i} \\ 0 \end{pmatrix})\} \in C_1, \{(\begin{pmatrix} x_{3i} \\ 0 \end{pmatrix}, \begin{pmatrix} x_{4i} \\ 0 \end{pmatrix})\} \in C_2, \dots, \{(\begin{pmatrix} x_{n_1-3,i} \\ 0 \end{pmatrix}, \begin{pmatrix} x_{n_1-2,i} \\ 0 \end{pmatrix})\} \in C_{r_1}, \{(\begin{pmatrix} v_i \\ 0 \end{pmatrix}, \infty)\} \in C_{r_1+1}; |V(C_t)| = 2m_2 (1 \leq t \leq r_1), |V(C_{r_1+1})| =$

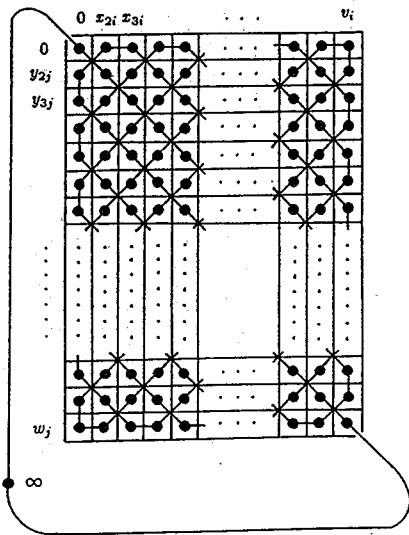


Figure 5 $F(i) \cup G(j)$

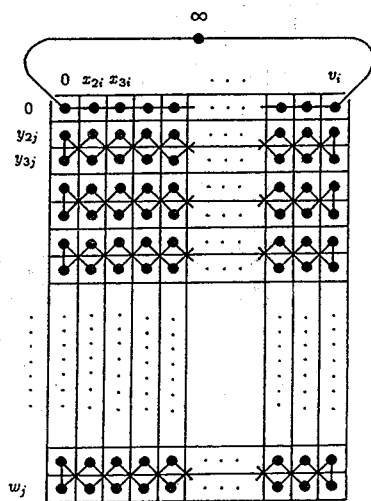


Figure 6 $F(i) \cup G(i)$

$m_2 + 1$ である。 k を任意の整数 ($1 \leq k \leq m_1 - 1$) とし、 k が odd のときは

$$C_k = C_{r_1+1} \cup C_{r_1} \cup C_{r_1-1} \cdots \cup C_{r_1-(k-3)/2}$$

k が even のときは、

$$C_k = C_1 \cup C_2 \cup \cdots \cup C_{k/2}$$

とす。 そして、 $G_{(i)}^{(j)}$ と $G_{(j)}^{(i)}$ を C_k に含まれる枝について、 枝を交換

しよう。 交換してできた新しい 1-factor を

$$G_{(i)}^{(j)}(k) = (G_{(i)}^{(j)} \setminus C_k) \cup (G_{(j)}^{(i)} \cap C_k),$$

$$G_{(j)}^{(i)}(k) = (G_{(j)}^{(i)} \setminus C_k) \cup (G_{(i)}^{(j)} \cap C_k)$$

とす。 (k が odd のときは $G_{(i)}^{(j)}(k)$ は、 Figure 8 に示されている)

そのとき、 次の lemma が成り立つ。

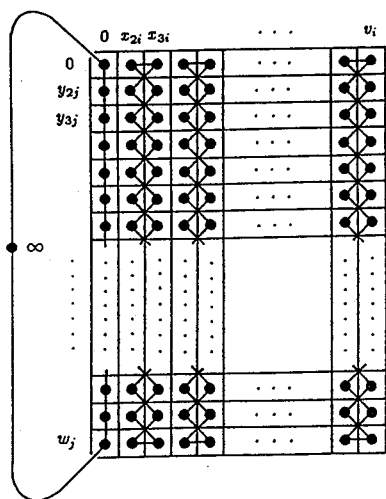


Figure 7 $F_{(i)} \cup G_{(j)}$

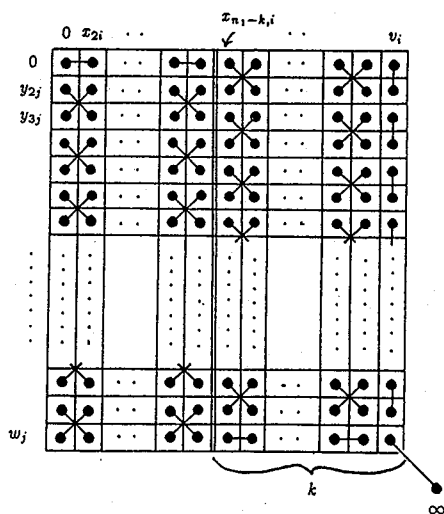


Figure 8 $G_{(i)}^{(j)}(k)$ (k : odd)

Lemma 4.1 $i \in I, j \in J, 1 \leq k \leq m_1 - 1$ とする.

(1) $(k, m_2) = 1$ ならば $F_{(0)} \cup G_{(j)}^{(i)}(k)$ は Hamilton cycle である.

(2) $(m_1 - k, m_2) = 1$ ならば $F_{(0)} \cup G_{(j)}^{*(i)}(k)$ は Hamilton cycle である.

次に $G_{(j)} \cup G_{(i)} (j \in J, i \in I)$ について同様にして cycle 構造は

$$G_{(j)} \cup G_{(i)} = D_1 \cup D_2 \cup \dots \cup D_{r_2} \cup D_{r_2+1},$$

$$= \mathcal{C}_j \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ y_{2j} \end{pmatrix} \right\} \in D_1, \left\{ \begin{pmatrix} 0 \\ y_{3j} \end{pmatrix}, \begin{pmatrix} 0 \\ y_{4j} \end{pmatrix} \right\} \in D_2, \dots, \left\{ \begin{pmatrix} 0 \\ y_{n_2-3,j} \end{pmatrix}, \begin{pmatrix} 0 \\ y_{n_2-2,j} \end{pmatrix} \right\} \in D_{r_2}, \left\{ \begin{pmatrix} 0 \\ w_j \end{pmatrix}, \infty \right\} \in D_{r_2+1}; |V(D_0)| = m_2 + 1, |V(D_t)| = 2m_2 (1 \leq t \leq r_2)$$

である. k' を任意の整数 $(1 \leq k' \leq m_2 - 1)$ とし, k' が odd のときは,

$$D_{k'} = D_{r_1+1} \cup D_{r_2} \cup D_{r_2-1} \dots \cup D_{r_2-(k'-3)/2}$$

k' が even のときは

$$D_{k'} = D_1 \cup D_2 \cup \dots \cup D_{k'/2}$$

とみる. すなわち $G_{(j)}$ と $G_{(i)}$ を $D_{k'}$ に含まれる枝について, 枝を交換しよう. 交換してできた新しい 1-factor を,

$$G_{(j)}^{(i)}(k') = (G_{(j)} \setminus D_{k'}) \cup (G_{(i)} \cap D_{k'}),$$

$$G_{(j)}^{*(i)}(k') = (G_{(j)} \setminus D_{k'}) \cup (G_{(i)} \cap D_{k'})$$

とみる. さて. 同様にして次の lemma が成り立つ.

Lemma 4.2 $j \in J, i \in I, 1 \leq k' \leq m_2 - 1$ とする.

(1) $(k', m_1) = 1$ ならば $F_{(0)} \cup G_{(j)}^{(i)}(k')$ は Hamilton cycle である.

(2) $(m_2 - k', m_1) = 1$ ならば $F_{(0)} \cup G_{(j)}^{*(i)}(k')$ は Hamilton cycle である.

5. Dudeney set of recursive construction

m_1, m_2 は奇数で、 $(m_1, m_2) = 1$, $3 \leq m_1 < m_2$ を満たすとする。

次の m_1, m_2 に関する条件を C_{m_1, m_2} とおく：

- (1) $(r_1, m_2) = (m_1 - r_1, m_2) = 1$ を満たす整数 r_1 ($1 \leq r_1 \leq m_1 - 1$) が存在し、かつ、
 (2) $(r_2, m_1) = (m_2 - r_2, m_1) = 1$ を満たす整数 r_2 ($1 \leq r_2 \leq m_2 - 1$) が存在する。

Theorem 5.1 n を任意の偶数 ≥ 4 とし、 $n = m + 1$ とおく。 m は素数中ではないとし、 $m = m_1 m_2$, $(m_1, m_2) = 1$, $3 \leq m_1 < m_2$ とする。
 $n_1 = m_1 + 1$, $n_2 = m_2 + 1$ とおく。 K_{n_1} , K_{n_2} がそれぞれ性質 (A_{n_1}) , (A_{n_2}) を満たし、 m_1, m_2 が条件 C_{m_1, m_2} を満たすならば、 K_n は性質 (A_n) を満たす。

(証明) r_1, r_2 を、条件 C_{m_1, m_2} の (1), (2) を満たす整数とする。

$G(i)$ ($i \in I$) に関し、 $G(i)$ と $G(i_{r_1})$ を C_{r_1} に含まれる枝 1 について枝交換をし、 $G(j)$ に関し、 $G(j)$ と $G(j)$ を D_{r_2} に含まれる枝 1 について枝交換する。 したがって得られた新しい 1-factor と $F(i)$ との和をとると、Lemma 4.1, 4.2 より、Hamilton cycle となる。 任意の 2-path を T として 1 回ずつ持つこと、 (A_n) の (2) については、§3 で述べたとおり枝交換する前は既に満たされたこと、から、枝交換した後も自動的に満たす。 よって定理が示される。 //

Theorem 5.2 n が任意の偶数 (≥ 4) のとき、 K_n は (A_n) を満たす。

(証明) $n = m + 1$ とおき、 m の素因数分解を $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ とする。 $S=1$ に関する帰納法で証明する。まず $S=1$ のときは、§2 で述べたように成り立つ。次に、 $S \geq 2$ と仮定する。一般性を失なうことなく、 $p_1 < p_2 < \cdots < p_s$ とする。 $m_1 = p_1^{e_1}$, $m_2 = p_2^{e_2} \cdots p_s^{e_s}$ とおくと、 K_{m+1} は (A_{m+1}) を満たし、また帰納法の仮定より、 K_{m_2+1} は (A_{m_2+1}) を満たす (Theorem 5.1 より)。 m_1, m_2 が条件 C_{m_1, m_2} を満たすことを示せばよい。

(1) $k_1 = p_1^{e_1-1}$ とおくと、 $(k_1, m_1) = 1$ は明らか。また p_1 の最小性より、 $(m_1 - k_1, m_2) = 1$ を得る。

(2) $(p_1, p_2 - 1) = 1$ のときは $k_2 = p_2^{e_2-1} p_3^{e_3} \cdots p_s^{e_s}$ とおき、 $(p_1, p_2 - 1) \neq 1$ のときは、 $k_2 = 2 p_2^{e_2-1} p_3^{e_3} \cdots p_s^{e_s}$ とおくと、 $(k_2, m_1) = (m_2 - k_2, m_1) = 1$ を得る //

従って、Theorem 1.1 が示された。

REFERENCES

1. B.A.ANDERSON, Symmetry groups of some perfect 1-factorizations of complete graphs, *Discrete Math* **18** (1977), 227-234.
2. H.E.DUDENEY, "Amusements in Mathematics," Thomas Nelson and Sons, London, 1917, Dover Reprint, New York, 1970.
3. K.HEINRICH, M.KOBAYASHI AND G.NAKAMURA, Dudeney's Round Table Problem, *Annals of Discrete Math.* (to appear).
4. K.HEINRICH, M.KOBAYASHI AND G.NAKAMURA, A Solution of Dudeney's Round Table Problem for $p^e q^f + 1$ (manuscript).
5. K.HEINRICH AND G.NONAY, Exact coverings of 2-path by 4-cycles, *J. Combinatorial Theory A* **45** (1987), 50-61.
6. M.KOBAYASHI, On Perfect One-Factorization of the Complete Graph K_{2p} , *Graphs and Combinatorics* **5** (1989), 243-244.
7. M.KOBAYASHI AND G.NAKAMURA, Exact coverings of 2-paths by Hamilton cycles (in submission).
8. M.KOBAYASHI AND G.NAKAMURA, Resolvable coverings of 2-paths by 4-cycles (in submission).
9. M.KOBAYASHI, KIYASU-Z. AND G.NAKAMURA, A solution of Dudeney's round table problem for even persons (in submission).
10. G.NAKAMURA, Solution of Dudeney's round table problem for the cases of $n = p+1$ and $n = 2p$ (in Japanese), *Sugaku Seminar* **159** (1975), 24-29.
11. G.NAKAMURA, KIYASU-Z. AND N.IKENO, Solution of the round table problem for the case of $p^k + 1$ persons, *Commentarii Mathematici Universitatis Santi Pauli* **29** (1980), 7-20.

A New Upper Bound on the Minimal Distance of Self-Dual Codes (J. H. Conway, N. J. A. Sloane の仕事の紹介)

愛媛大学 山野敏郎

1. Introduction

ここで紹介するのは、Conway, Sloane による “A New Upper Bound on the Minimal Distance of Self-Dual Codes” (1990, preprint) の概略である。このレポートの主たる結果としては、

定理1 \mathcal{C} を長さ n の binary self-dual code、 d を \mathcal{C} の minimal distance とすると、 $n \neq 2, 8, 12, 22, 24, 32, 48, 72$ に関して、 d は

$$d \leq 2 \lfloor (n+6)/10 \rfloor \quad (1)$$

をみたす。

が挙げられる。 \mathcal{C} が、Type II (doubly even self-dual code; すべての code word の weight が 4 で割り切れる self-dual code) のとき、定理1は、 n (必然的に

8の倍数)が8, 24, 32, 48, 72のときに成立しない。また、Type I (doubly evenでない self-dual code)のとき、 n (必然的に偶数)が2, 12, 22, 32で成立しない。これら、成立しない場合の \mathcal{C} の highest minimal distance は、 $n=72$ を除いて、 $2\lceil(n+6)/10\rceil+2$ となる。

これより過去の bound としては、1973年の Mallows Sloane bound;

Type I の場合、任意の n に関して

$$d \leq 2\lceil n/8 \rceil + 2 \quad (2)$$

Type II の場合、任意の n に関して

$$d \leq 4\lceil n/24 \rceil + 4 \quad (3)$$

が一般的であるが、これに比べると(1)は、Type I のときに強いboundとなっている。Type IIの場合は(3)の方が、(1)より強いのか、等しいか、どちらかである。

例1 (1), (2), (3)の bound の比較

n	8	24	40	56	72	88	...	160	240	320	400
(1)	4	8	8	12	?	18	...	32	48	64	80
(2)	4	8	12	16	20	24	...	42	62	82	102
(3)	4	8	8	12	16	16	...	28	44	56	68

実は、このレポートには $n \neq 72$ という条件はない。証明に A. R. Calderbank, "Nonexistence of an extremal binary self-dual [72, 36, 16] code" (preprint) の結果が利用されたためであるが、最近、この論文に誤りがあることを Sloane が発見した。Type II code に関して、定理 1 が、何ら新しい結果を生み出していないのは、この条件があるためである。

定理 1 は、“shadow” と呼ばれる nonlinear code を考えることによって生まれた。Type I code の shadow の性質は、もとの code の weight enumerator にある制限を与え、それによって、 $n \leq 60$ の self-dual code の highest minimal distance が決定される。 $62 \leq n \leq 72$ についてもある程度の予想がつく。

定理 2 $n \leq 60$ の self-dual code の highest minimal distance はすべて知られている。実際の値は表 1 の通り。

表1 self-dual code の highest minimal distance

n	d_1	d_2	codes	n	d_1	d_2	codes
2	2		1code	38	8		≥ 2
4	2		1code	40	8	8	$\geq 2; \geq 100$
6	2		1code	42	8		≥ 9
8	2	4	1code; 1code	44	8		≥ 14
10	2		2codes	46	10		≥ 1
12	4		1code	48	10	12	$\geq 1; \geq 1$
14	4		1code	50	10		≥ 1
16	4	4	1code; 2codes	52	10		≥ 1
18	4		2codes	54	10		≥ 1
20	4		7codes	56	10 or 12	12	?; ≥ 20
22	6		1code	58	10		≥ 2
24	6	8	1code; 1code	60	12		≥ 1
26	6		1code	62	10 or 12		?
28	6		3codes	64	12	12	$\geq 1; \geq 38$
30	6		12codes	66	12		≥ 1
32	8	8	3codes; 5codes	68	12		≥ 1
34	6		≥ 200 codes	70	10 or 12		?
36	8		≥ 2				

$d_1, (d_2)$ は Type I (II) code の highest minimal distance

d_2 は $n \leq 88 (n \neq 72)$ に関しては、これまでにわかっている

$n < 72$ で、定理1が成立していることがこれによって確かめられる。(よって証明は $n \geq 74$ で行う)

また、shadowを導入することで、別の新しい結果も見されている。

Notation

$\mathcal{C} : [n, k]$ code

$d : \mathcal{C}$ の minimal distance

$\mathcal{C}^\perp : \mathcal{C}$ の dual code

$W(x, y) = \sum A_r x^{n-r} y^r : \mathcal{C}$ の weight enumerator

$w(u)$: u の weight

$A(n, k, d)$: 長さ n 、weight が r で距離が少なくとも d 離れている binary vector の最大存在数

2. Shadow の定義とその特性

一般的な shadow の定義としては、 $\mathcal{C} \supset \mathcal{C}^\perp = \mathcal{B}$ のときを考える。 $\mathcal{B}^{(0)} = \{u \in \mathcal{B} \mid w(u) \equiv 0 \pmod{4}\}$ とすると、 \mathcal{C} の shadow \mathcal{S} は次のように定義される；

$$\mathcal{S} = \{u \mid (u, v) = 0 \quad \forall v \in \mathcal{B}^{(0)};$$

$$(u, v) = 1 \quad \forall v \in \mathcal{B} - \mathcal{B}^{(0)}\}$$

これは $\mathcal{S} = \mathcal{B}^{(0)\perp} - \mathcal{C}$ の形に書ける。 $\mathcal{B}^{(0)\perp} = \mathcal{C} \cup (a + \mathcal{C})$ ($a \notin \mathcal{C}$) と書けるので、 \mathcal{S} は nonlinear code である。

ここでは self-dual code を扱うので、 $\mathcal{C}^{(0)} = \mathcal{B}^{(0)}$ 、 $\mathcal{C}^{(2)} = \mathcal{C} - \mathcal{C}^{(0)}$ とし、定義を書き換える；

$$\mathcal{S} = \{u \mid (u, v) = 0 \quad \forall v \in \mathcal{C}^{(0)};$$

$$(u, v) = 1 \quad \forall v \in \mathcal{C}^{(2)}\}$$

\mathcal{C} が Type II のとき ($\mathcal{C}^{(2)} = \emptyset$)、 $\mathcal{S} = \mathcal{C}$ となり、shadow は実質存在しない。定理 1 に貢献するのは、 \mathcal{C}

が Type I のときで、その shadow の性質を示したものが次の定理3である；

定理3 \mathcal{C} を $[n, k, d]$ Type I self-dual code、 \mathcal{P} をその shadow code とする。 $\mathcal{C}^{(0)\perp}$ は、 $\mathcal{C}^{(0)}$ の4つの coset の union で構成される。すなわち、 $\mathcal{C}^{(0)\perp} = \mathcal{C}^{(0)} \cup \mathcal{C}^{(1)} \cup \mathcal{C}^{(2)} \cup \mathcal{C}^{(3)}$ ($\mathcal{C} = \mathcal{C}^{(0)} \cup \mathcal{C}^{(2)}$) と書ける。すると、 \mathcal{P} について次のことがいえる；

$$(i) \quad \mathcal{P} = \mathcal{C}^{(0)\perp} - \mathcal{C} = \mathcal{C}^{(1)} \cup \mathcal{C}^{(3)}$$

$$(ii) \quad u, v \in \mathcal{P} \Rightarrow u + v \in \mathcal{C}; \text{ もっと正確には、}$$

$$u, v \in \mathcal{C}^{(1)} \Rightarrow u + v \in \mathcal{C}^{(0)}; u \in \mathcal{C}^{(1)}, v \in \mathcal{C}^{(3)}$$

$$\Rightarrow u + v \in \mathcal{C}^{(2)}; u, v \in \mathcal{C}^{(3)} \Rightarrow u + v \in \mathcal{C}^{(0)}$$

(iii) $S(x, y) = \sum B_r x^{n-r} y^r$ を \mathcal{P} の weight enumerator とすると、

$$S(x, y) = W\left(\frac{x+y}{\sqrt{2}}, i \frac{x-y}{\sqrt{2}}\right) \quad (4)$$

また、

$$r \equiv n/2 \pmod{4} \text{ でないかぎり、 } B_r = 0 \quad (5)$$

$$B_0 = 0 \quad (6)$$

$$\text{すべての } r \text{ に関して、 } B_r \leq 1 \quad (7)$$

$$B_{d/2} \leq 2n/d \quad (8)$$

$$\text{すべての } r \text{ に関して、} B_r \leq A(n, d, r) \quad (9)$$

すべての $r < (d+4)/2$ に関して、0でない B_r は、最大1つしか存在しない。 (10)

(iv) Gleason の定理により、 $W(x, y)$ は適当な整数 a_j をつかって次のように書ける；

$$W(x, y) = \sum_{j=0}^{n/8} a_j (x^2 + y^2)^{n/2-4j} \{x^2 y^2 (x^2 - y^2)^2\}^j \quad (11)$$

すると、

$$S(x, y) = \sum_{j=0}^{n/8} (-1)^j a_j 2^{n/2-6j} (xy)^{n/2-4j} (x^4 - y^4)^{2j} \quad (12)$$

(v) $W^{(j)}(x, y)$ を $\mathcal{G}^{(j)}$ ($0 \leq j \leq 3$) の weight enumerator とする。すると、 $W^{(1)} - W^{(3)}$ は、

① $n \equiv 0 \pmod{8}$ なら、 $f_8 = x^8 + 14x^4 y^4 + y^8$
と $f_{24} = x^4 y^4 (x^4 - y^4)^4$ 中の多項式、

② $n \equiv 2 \pmod{8}$ なら、 f_8 と f_{24} 中の多項式の
 f_{18} 倍、 ($f_{18} = x^{17} y - 34x^{13} y^5 + 34x^5 y^{13} -$
 xy^{17})

③ $n \equiv 4 \pmod{8}$ なら、 f_8 と f_{24} 中の多項式の
 f_{12} 倍、 ($f_{12} = x^{10} y^2 - 2x^6 y^6 + x^2 y^{10} =$
 $f_{24}^{1/2}$)

④ $n \equiv 6 \pmod{8}$ なら、 f_8 と f_{24} 中の多項式の

$$f_{30} = f_{12} f_{18} \text{ 倍、}$$

(ii) は、 $\mathbb{Q}^{(0)\perp} / \mathbb{Q}^{(0)}$ が 4 元群になることより。(iii)

の(4)は、MacWilliams identity

$$W^\perp(x, y) = \frac{1}{|\mathbb{Q}|} W(x+y, x-y)$$

を $\mathbb{Q}^{(0)}$, $\mathbb{Q}^{(0)\perp}$ に適用することによりえられる。(iv)

は、Gleason の定理 (任意の Type I self-dual code の weight enumerator は、 $x^2 + y^2$ と $x^2 y^2 (x^2 - y^2)^2$

中の多項式である) により(11)がえられるが、これと(4)

より、同じ a_i をつかって(12)がえられる。(v)は invariant theory をつかう。

この定理によって、 $n \leq 60$ の possible highest minimal distance (Gleason の定理だけをつかったものより、強い制限がつけられている) をもつ weight enumerator が求まる。実際、その weight enumerator をもつ code が存在することがわかっているので、表1の結果がえられる。

3. [32, 16, 8] Type I self-dual code の分類

[32, 16, 8] Type II self-dual code が5つしかないことは、Conway, Press らによって知られているが、Type I code については、その分類が明らかではなかった。shadow を導入することにより、これが明らかになる。

[32, 16, 8] Type I self-dual code \mathcal{C} の weight enumerator と shadow \mathcal{S} の weight enumerator は

$$W(x) = 1 + 364x^8 + 2048x^{10} + \dots,$$

$$S(y) = 8y^4 + 592y^8 + \dots. \quad (x=1 \text{ としている})$$

ここに tetrad, octet を導入する。

t : tetrad : $w(x) = 4$ の vector

$$O : \text{octet} = \{ \text{tetrad } t_i \mid i=1, \dots, 8 \mid |t_i \cap t_j| = \emptyset \\ \text{and } t_i \cup t_j \in \mathcal{C} \quad \forall i, (\neq) j \}$$

$$(w(t_i \cup t_j) = 8)$$

$n \equiv 0 \pmod{4}$ のとき、 $\mathcal{C}^{(0)} \cup \mathcal{C}^{(1)}$, $\mathcal{C}^{(0)} \cup \mathcal{C}^{(3)}$ が self-dual code になるという性質と、shadow の8つの weight 4 の vector が、 $\mathcal{C}^{(1)}$ か $\mathcal{C}^{(3)}$ のどちらか一方に入っているという性質 (今 $\mathcal{C}^{(1)}$ に入っていると) から、 $\mathcal{C}^{(0)} \cup \mathcal{C}^{(3)}$ が [32, 16, 8] Type II self-dual code になることがわかる。かつ、この8つの vec-

tor が (新しくできた) Type II self-dual code の octet になっていることから、任意の Type I self-dual code に対し、octet をもつ Type II code \mathfrak{B} が 1 つ決まる。

今、5 つの $[32, 16, 8]$ Type II self-dual code の中に、octet をもつものは 3 つある。 \mathfrak{B} から \mathfrak{C} をつくるとき、

$\forall O \in \mathfrak{B}, \forall t \in O$ に対し、

$$\mathfrak{C} = \{u \in \mathfrak{B} \mid |t \cap u| = \text{偶数}\} \cup (\{u \in \mathfrak{B} \mid |t \cap u| = \text{奇数}\} + t)$$

とすればつくれるが、これが octet, tetrad の取り方によらず一意的に決まることより、Type I code が 3 つしかないことがわかる。

定理 4 $[32, 16, 8]$ Type I self-dual code は、3 つしかない。

また、その他の新しい結果として、

定理 5 $d \geq 6$ の minimal distance をもつ self-dual

code は $n \geq 22$ で存在する。 $d \geq 8$ の minimal distance をもつ self-dual code は $n = 24, 32, n \geq 36$ で存在する。 $d \geq 10$ の minimal distance をもつ self-dual code は $n \geq 46$ で存在する。

n が小さいところでは、表 1 より明らか。大きいところでは、average weight enumerator をつかうことで簡単に確かめられる。

4. 定理 1 の証明

$n > 72$ と仮定する。 $d \geq 2[(n+6)/10] + 2$ とする (実際計算するときは $d = 2[(n+6)/10] + 2$ とおく)。また、計算の便宜上 $n = 8k + 2t$ ($0 \leq t \leq 3$) とか、 $n = 10l + 2\delta$ ($-3 \leq \delta \leq 1$) として、 \mathcal{C} と \mathcal{D} の weight enumerator (11), (12) における整数、 a_i の bound を求めることで矛盾をひきだす。

(11) に解析的知識を導入し計算をすることで、 a_i が求まる。

$$a_i = \frac{n}{2^l} \sum_{j=0}^{l-1} (-1)^{l+j} \binom{2l+j-1}{j} \binom{2l+\delta-j-1}{l-j-1}$$

(12)に解析的知識を導入し計算をすることで、 a_l の bound が求まる。

$$a_l \leq \frac{n}{2^l} 2^{8l-n/2} \binom{2k-j'-1}{j'-1} \quad j' = k-l$$

$74 \leq n \leq 500$ の範囲で、 a_l が bound をこえることより矛盾。

$500 < n \leq 3000$ については、コンピュータで矛盾が成立していることを確認している。

$n > 3000$, $l > 300$ については、 $b_l = -2^l a_l / n$ として、 b_l の lower bound と bound を求める。近似法の saddle-point 法を導入し、積分の計算をすすめると、

$$b_l \geq \frac{0.0855 \dots c_1^l}{\sqrt{l}} \quad , c_1 = 4.95747 \dots$$

$$|b_l| < \frac{1.8806 \dots c_2^l}{\sqrt{l}} \quad , c_2 = 4.38425 \dots$$

を得る。これで証明が完成した。

Reference

参考文献は Conway, Sloane のものをそのまま転写する。

- [1] G. F. M. Beenker, "On double circulant codes", Report 80-WSK-04, Mathematics Dept., Technological Univ. Eindhoven, Eindhoven, Netherlands, July 1980.
- [2] E. R. Berlekamp, F. J. MacWilliams and N. J. A. Sloane, "Gleason's theorem on self-dual codes", IEEE Trans. Info. Theory, vol. 18 (1972), pp. 409-414.
- [3] V. K. Bhargava and C. Nguyen, "Circulant codes based on the prime 29", IEEE Trans. Info. Theory, vol. 26 (1980), pp. 363-364.
- [4] V. K. Bhargava and J. M. Stein, " (v, k, d) configurations and self dual codes", Inform. Control, vol. 28 (1975), pp. 352-355.
- [5] V. K. Bhargava, G. Young and A. K. Bhargava, "A characterization of a $(56, 28)$ extremal self-dual code", IEEE Trans. Info. Theory, vol. 27 (1981), pp. 258-260.
- [6] A. Blokhuis and A. R. Calderbank, personal communication.
- [7] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane and W. D. Smith, "A new table of constant weight codes", IEEE Trans. Info. Theory (submitted).
- [8] N. G. de Bruijn, "Asymptotic Methods in Analysis", North-Holland, Amsterdam, 3rd edition, 1970.
- [9] F. C. Bussemaker and V. D. Tonchev, "New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28", Discrete Math., vol. 76 (1989), pp. 45-49.
- [10] A. R. Calderbank, "Nonexistence of an extremal binary self-dual $[72, 36, 16]$ code", preprint.
- [11] J. H. Conway and V. Pless, "On the enumeration of self-dual codes", J. Combinatorial Theory, vol. A 28 (1980), pp. 26-53.
- [12] J. H. Conway, V. Pless and N. J. A. Sloane, "Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16", IEEE Trans. Info. Theory, vol. 25 (1979), pp. 312-322.

- [13] J. H. Conway, V. Pless and N. J. A. Sloane, "Corrections to *On the enumeration of self-dual codes* and *The children of the (32,16) doubly even codes*", in preparation.
- [14] J. H. Conway and N. J. A. Sloane, "Sphere Packings, Lattices and Groups", Springer-Verlag, NY 1988.
- [15] J. H. Conway and N. J. A. Sloane, "A new upper bound for the minimum of an integral lattice of determinant one", Bull. Amer. Math. Soc., submitted.
- [16] J. H. Conway and N. J. A. Sloane, "On the minimum of unimodular lattices I: Upper bounds", in preparation.
- [17] J. H. Conway and N. J. A. Sloane, "On the minimum of unimodular lattices II: Lower bounds", in preparation.
- [17a] R. Dougherty and H. Janwa, "Covering radius computations for binary cyclic codes", Math. Comp., submitted.
- [18] A. M. Gleason, "Weight polynomials of codes and the MacWilliams identities", Actes Congrès Intern. de Math., Gauthier-Villars, Paris, 1971, vol. 3, pp. 211-215.
- [19] P. Henrici, "Applied and Computational Complex Analysis", Wiley, NY 1974, vol. 1.
- [20] W. C. Huffman, "Automorphisms of codes with applications to extremal doubly-even codes of length 48", IEEE Trans. Info. Theory, vol. 28 (1982), pp. 511-521.
- [21] W. C. Huffman and V. I. Yorgov, "A [72,36,16] doubly even code does not have an automorphism of order 11", IEEE Trans. Info. Theory, vol. 33 (1987), pp. 749-752.
- [22] M. Karlin, "New binary coding results by circulants", IEEE Trans. Info. Theory, vol. 15 (1969), pp. 81-92.
- [23] M. Kneser, "Klassenzahlen definiter quadratischer Formen", Archiv Math., vol. 8 (1957), pp. 241-250.
- [24] H. V. Koch, "On self-dual, doubly-even codes of length 32", Report P-Math-32/84, Institut für Mathematik, Akademie der Wissenschaften der DDR, Berlin, 1984.
- [25] H. Koch, "Unimodular lattices and self-dual codes", in "Proc. Intern. Congress Math., Berkeley 1986", Amer. Math. Soc., Providence RI, 1987, vol. 1, pp. 457-

- [26] H. Koch and B. B. Venkov, "Ueber ganzzahlige unimodulare euklidische Gitter", *J. Reine Angew. Math.*, vol. 398 (1989), pp. 144-168.
- [27] J. S. Leon, J. M. Masley and V. Pless, "Duadic codes", *IEEE Trans. Info. Theory*, vol. 30 (1984), pp. 709-714.
- [28] J. S. Leon, V. Pless and N. J. A. Sloane, "On ternary self-dual codes of length 24", *IEEE Trans. Info. Theory*, vol. 27 (1981), pp. 176-180.
- [29] F. J. MacWilliams, "Orthogonal circulant matrices over finite fields, and how to find them", *J. Comb. Theory*, vol. 10 (1971), pp. 1-17.
- [30] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, "Generalizations of Gleason's theorem on weight enumerators of self-dual codes", *IEEE Trans. Info. Theory*, vol. 18 (1972), pp. 794-805.
- [31] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.
- [32] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson, "Good self-dual codes exist", *Discrete Math.*, vol. 3 (1972), pp. 153-162.
- [33] C. L. Mallows, A. M. Odlyzko and N. J. A. Sloane, "Upper bounds for modular forms, lattices, and codes", *J. Alg.*, vol. 36 (1975), pp. 68-76.
- [34] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes", *Information and Control*, vol. 22 (1973), pp. 188-200.
- [35] Mathlab Group, "MACSYMA Reference Manual", Laboratory for Computer Science, M.I.T., Cambridge, MA, version 10, 1983.
- [36] R. J. McEliece, personal communication.
- [37] R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr. and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities", *IEEE Trans. Info. Theory*, vol. 23 (1977), pp. 157-166.
- [38] M. Ozeki, "Hadamard matrices and doubly-even self-dual error-correcting codes", *J. Comb. Theory*, vol. A 44 (1987), pp. 274-287.

- [39] M. Ozeki, "Examples of even unimodular extremal lattices of rank 40 and their Siegel theta series of degree 2", *J. Number Theory*, vol. 28 (1988), pp. 119-131.
- [40] G. Pasquier, "A binary extremal doubly even self-dual code (64,32,12) obtained from an extended Reed-Solomon code over F_{16} ", *IEEE Trans. Info. Theory*, vol. 27 (1981), pp. 807-808.
- [41] G. Pasquier, "Projections et images binaires de codes sur F_2^m ", *Rev. CETHEDC Cahier*, (no. 2, 1981), pp. 45-56.
- [42] G. Pasquier, "Binary images of some self-dual codes over $GF(2^m)$ with respect to trace-orthogonal basis", *Discrete Math.*, vol. 37 (1981), pp. 127-129.
- [43] V. Pless, "On the uniqueness of the Golay codes", *J. Comb. Theory*, vol. 5 (1968), pp. 215-228.
- [44] V. Pless, "A classification of self-orthogonal codes over $GF(2)$ ", *Discrete Math.*, vol. 3 (1972), pp. 209-246.
- [45] V. Pless, "The children of the (32,16) doubly even codes", *IEEE Trans. Info. Theory*, vol. 24 (1982), pp. 738-746.
- [46] V. Pless, "Extremal codes are homogeneous", preprint.
- [47] V. Pless, J. M. Masley and J. S. Leon, "On weights in duadic codes", *J. Comb. Theory*, vol. A 44 (1987), pp. 6-21.
- [48] V. Pless and N. J. A. Sloane, "On the classification and enumeration of self-dual codes", *J. Comb. Theory*, vol. A 18 (1975), pp. 313-335.
- [49] A. Poli and C. Rigoni, "Enumeration of self-dual $2k$ circulant codes", *Lect. Notes. Comp. Sci.*, vol. 228 (1986), pp. 61-70.
- [50] N. J. A. Sloane, "Is there a (72,36) $d=16$ self-dual code?", *IEEE Trans. Info. Theory*, vol. 19 (1973), p. 251.
- [51] N. J. A. Sloane, "Weight enumerators of codes", in "Combinatorics", ed. M. Hall, Jr. and J. H. van Lint, Reidel, Dordrecht, Holland, 1975, pp. 115-142.
- [52] N. J. A. Sloane, "Binary codes, lattices and sphere packings", in "Combinatorial Surveys", edited P. J. Cameron, Academic Press, NY, 1977, pp. 117-164.
- [53] N. J. A. Sloane, "Error-correcting codes and invariant theory: new applications of

- a nineteenth-century technique", Amer. Math. Monthly, vol. 84 (1977), pp. 82-107.
- [54] N. J. A. Sloane, "Self-dual codes and lattices", Proc. Symp. Pure Math., vol. 34 (1979), pp. 273-308.
- [54a] N. J. A. Sloane and J. G. Thompson, "Cyclic self-dual codes", IEEE Trans. Info. Theory, vol. 29 (1983), pp. 364-366.
- [55] T. A. Springer, "Regular elements of finite reflection groups", Invent. Math., vol. 25 (1974), pp. 159-198.
- [56] R. P. Stanley, "Relative invariants of finite groups generated by pseudoreflections", J. Algebra, vol. 49 (1977), pp. 134-148.
- [57] V. D. Tonchev, "Inequivalence of certain extremal self-dual codes", Compt. Rend. Acad. Bulg. Sci., vol. 36 (1983), pp. 181-184.
- [58] V. D. Tonchev, "Hadamard-type block designs and self-dual codes" (in Russian), Problemy Peredachi Inform., vol. 19 (no. 4, 1983), pp. 25-30. English translation in Problems of Information Transmission, vol. 19 (1983), pp. 270-274.
- [59] V. D. Tonchev, "Symmetric designs without ovals and extremal self-dual codes", in "Combinatorics '86", North-Holland, Amsterdam, 1988, pp. 451-457.
- [60] V. D. Tonchev, "Self-orthogonal designs and extremal doubly even codes", J. Comb. Theory, vol. A 50 (1989), to appear.
- [61] V. D. Tonchev, "Self-orthogonal designs", Contemp. Math., to appear.
- [62] V. D. Tonchev and R. V. Raev, "Cyclic 2-(17,8,7) designs and related doubly even codes", Compt. Rend. Acad. Bulg. Sci., vol. 35 (no. 10, 1982).
- [63] M. Ventou and C. Rigoni, "Self-dual doubly circulant codes", Discrete Math., vol. 56 (1985), pp. 291-298.
- [64] H. N. Ward, "A restriction on the weight enumerator of a self-dual code", J. Comb. Theory, vol. A 21 (1976), pp. 253-255.
- [65] E. T. Whittaker and G. N. Watson, "A Course of Modern Analysis", 4th ed., Cambridge Univ. Press, 1963.
- [66] J. Wolfmann, "A class of doubly even self dual binary codes", Discrete Math.,

- vol. 56 (1985), pp. 299-303.
- [67] J. Wolfmann, "A group algebra construction of binary even self dual codes", *Discrete Math.*, vol. 65 (1987), pp. 81-89.
- [68] V. Y. Yorgov, "Binary self-dual codes with automorphisms of odd order" (in Russian), *Prob. Pered. Inform.*, vol. 19 (no. 4, 1983), pp. 11-24. English translation in *Problems Info. Transmission*, vol. 19 (1983), pp. 260-270.
- [69] V. Y. Yorgov, "Extremality of self-dual doubly even codes of length 56" (in Bulgarian), in "Mathematics and Education", *Bulgarian Acad. Sci.*, 1987, pp. 435-439.
- [70] V. Y. Yorgov, "A method for constructing inequivalent self-dual codes with applications to length 56", *IEEE Trans. Info. Theory*, vol. 33 (1987), pp. 77-82.
- [71] V. Y. Yorgov, "Doubly-even extremal codes of length 64" (in Russian), *Prob. Pered. Inform.*, vol. 22 (no. 4, 1986), pp. 35-42. English translation in *Problems Info. Transmission*, vol. 22 (1986), pp. 277-284.
- [72] V. Y. Yorgov, "On the extremal doubly-even codes of length 32", *Proceedings Fourth Joint Swedish-Soviet International Workshop on Information Theory, Gotland, Sweden, 1989*, pp. 275-279.
- [73] V. Y. Yorgov and N. P. Ziapkov, "Extremal codes of length 40 and automorphism of order 5", preprint.

Hall set を持つ 28 次の Hadamard 行列の分類

木村 浩
愛媛大理

H を Hadamard 行列 (以下 H -行列と書く) とする。
 $n = 4m + 4$ を H の次数とする。一般の n について
 云えることも多くあるが、ここでは $n = 28$ として話し
 を進める。

H の 4 行が Hall set をなすとは 適当な変換
 (Hadamard 変換の意) によつて 次の形に出来るもの;

$$\begin{array}{cccccc}
 + & + \cdots + & + + + + & + \cdots + & + \cdots + & + \cdots + & + \cdots + \\
 + & + \cdots + & + + & + \cdots + & & & \\
 + & + \cdots + & + + & & + \cdots + & & \\
 + & + \cdots + & + + & & & + \cdots + & \\
 \hline
 & \underbrace{\hspace{2cm}}_5 & \underbrace{\hspace{2cm}}_4 & \underbrace{\hspace{2cm}}_6 & \underbrace{\hspace{2cm}}_6 & \underbrace{\hspace{2cm}}_6 & \underbrace{\hspace{2cm}}_6
 \end{array}$$

ここでは Hall set を持つ H -行列のみ考える。

Prop. 1. H^T も Hall set を持つ ([5]).

H を 次の形に変換できる。このことより構成、分類
 ともこの形のもののみ考えればよい。ここではこの形を
normal form と云う。

$\begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & & & \\ 1 & & & \\ 1 & & & \end{array}$	$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}$	$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}$	$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}$	$\begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array}$
$\begin{array}{cccc} 1 & 1 & 1 & \\ 1 & & & \\ 1 & & & \\ 1 & & & \end{array}$	A_1	B_2	B_3	B_4
$\begin{array}{cccc} 1 & 1 & & 1 \\ 1 & & & \\ 1 & & & \\ 1 & & & 1 \end{array}$	C_1	A_2	C_3	C_4
$\begin{array}{cccc} 1 & & 1 & 1 \\ 1 & & & \\ 1 & & & \\ 1 & & 1 & \end{array}$	D_1	D_2	A_3	D_4
$\begin{array}{cccc} 1 & & & \\ 1 & & & \\ 1 & & & \\ 1 & & & \end{array}$	E_1	E_2	E_3	\bar{A}_4

空白は-1を示す.

性質

- (1) A_i ($i=1,2,3$), $-\bar{A}_4$; 各行,各列に1が2個,-1が4個である6次の正方行列.
- (2) B_i, C_i, D_i, E_i ; 各行,各列に1,-1が3個である6次の行列.

◦ 同値類について.

H と同値な H 行列の個数(必ずしも normal form ではない)は $(n!)^2 (2^n)^2 / |\text{Aut } H|$ である. (しかも $|\text{Aut } H| = 2$ である H が多く

が 'trivial' なものについて K -Box に依りて分類した (5個). この結果があるので 次の 4 case に分けて分類した.

[III]' A_1 が (3) 480 個

K -行列, K -Box に依る分類と一致した.

[I]' A_1 が (1) であって, H のすべての Hall set に属する normal form に (3) が現われぬ.
0 個

[II]' A_1 が (2) であって, H のすべての Hall set に属する normal form に (1), (3) が現われぬ
6 個

[IV] 0 個

定理 Hall set をもつ 28 次の H -行列の同値類は 486 個である.

ここで得られた新しい 6 個 (case [II]') とその K -行列を書きこく.

[注] (1) K -行列が 'trivial' な 5 個をのぞいて K -行列と同値類が 1対1に対応している.

- (2) 24 次の H -行列 について、この方法を用いて
59 個が確認された。
- (3) 476 個の K -行列 は [6]。
- (4) 自己同形群 が trivial のものがたくさんある。
これは K -行列 を見ればわかる。

104391559 130231431 130339225 106891049 112015953 120773729 175462415
 195339819 194200403 178161845 189378917 174744793 221123863 211391691
 223103715 216173389 214988341 221325753 22723099 15322419 16134627
 28005037 27028813 24479445 33562623 67625087 134741889 1

41111111122
 21111111112
 211111111222
 411111111122
 211111111125
 2111111111233
 2111111112223
 2111111112222
 4111111112223
 21111111122222
 211111111122333

104391559 130231431 130339225 106891049 112015953 120773729 179521819
 186527923 182756707 174821581 190081613 193578549 211590159 222989139
 215044835 228733741 221578709 208170169 23943463 24229403 281986603
 16157365 14316885 26847721 33562623 67625087 134741889 2

4111222
 1211111111123
 1211111122222

4111222
 1211111111222
 1211111122223

transpose of No.6

104391559 130231431 130339225 106891049 112015953 120773729 175207451
 187533483 181055843 195248973 194291253 173951189 221123863 223447891
 216286947 222853677 211391693 213002681 16161295 27028811 26956467
 15322421 24457701 23766745 33562623 67625087 134741889 3

2111111122222
 2111111111223
 2111111112222
 2111111122233
 21111111222334
 21111111112233
 21111111122223
 41111111122222
 211111111222234
 211111112222222
 2111111111112223
 2111111111112222
 21111111111122333

211111111222
 41111111111123
 21111111112233
 211111111111224
 211111111112235
 211111111122225
 2111111111112222
 21111111111122224
 41111111111122233
 211111111122223
 2111111111122223
 2111111111222222

transpose of No.4

104391559 130231431 114119065 123111209 128236113 104553569 189584455
 174819867 179643723 175517877 194103605 193618665 224426283 220072403
 215061219 219756061 212634797 216155989 28250919 28497051 14446131
 24464077 14334285 23700977 33562623 67625087 134741889 4

211111111222
 4111111111123
 21111111112233
 21111111111224
 211111111112235
 2111111111122225
 2111111111112222
 21111111111122224
 41111111111122233
 21111111111222223
 21111111111122223
 21111111111122222

21111111122222
 21111111111223
 21111111112222
 21111111122233
 211111111222334
 21111111112233
 211111111122223
 41111111122222
 211111111222234
 211111112222222
 21111111111112223
 21111111111122222
 21111111111122333

transpose of No.3

104391559 130231431 114119065 123111209 112605777 120183905 173955111
 194103835 174925387 195342509 182633813 186327537 221582615 211457227
 230716259 212536109 223120085 208694457 23771419 28198579 16091619
 24335053 27028813 14267957 33562623 67625087 134741889 5

1
 1111222
 31111111112
 311111111223
 311111111113
 611111111112
 1111111112223
 3111111222233
 31111111222224
 11111111111113
 311111111122224

104391559 130231431 114119065 123111209 112605777 120183905 193892679
 179669163 189887051 191129909 177948213 174761177 220924699 219952307
 215010643 214481453 228869837 208867813 8281103 31642291 15542115
 28423453 22907605 26896873 33562623 67625087 134741889 6

4111222
 1211111111222
 1211111122223

4111222
 1211111111123
 1211111222222

transpose of No.2

References

1. M. Hall Jr. : Combinatorial Theory, Boston, Ginn(Blaisdell), 1967
2. N. Ito, J. S. Leon and J. Q. Longyear: Classification of 3-(24,12,5) designs and 24-dimensional Hadamard matrices, J. Combin. Theory(A), 27(1979), 289-306
3. H. Kimura : On equivalence of Hadamard matrices, Hokkaido Math. J., 17(1988), 139-146
4. H. Kimura : New Hadamard matrices of order 24, Graphs and Combinatorics, 5(1989), 235-242
5. H. Kimura and H. Ohmori: Construction of Hadamard matrices of order 28, Graphs and Combinatorics, 2(1987), 247-257
6. H. Kimura and H. Ohmori: Hadamard matrices of order 28, Mem. Fac. Educ. Ehime Univ., Nat. Sci., 7(1987)
7. Z. Kiyasu: Hadamard matrices and its applications(in Japanese), Denki-tsusin Gakkai, 1980
8. V. D. Tonchev, Hadamard matrices of order 28 with automorphisms of order 13, J. Combin. Theory(A), 35(1983), 43-57
9. V. D. Tonchev, Hadamard matrices of order 28 with automorphisms of order 7, J. Combin. Theory(A), 40(1985), 62-81

28次のHadamard 行列の木村予想について

木村 浩(愛媛大理)

喜安 善市(半導体研)

1. はしがき

28次のHadamard行列(以後H行列と略す)の同値類は第1種(特性数が1のもの[K2], またはHall setのあるもの[K1])と第2種(特性数が2のもの, またはHall setのないもの)とに大別される. 第1種は486個であることが木村ら[K3]によって明かにされた. 第2種は不明であったが, 1987年木村はPaley型ただ1個に同値であると予想した. この木村予想を証明する.

この証明ではH行列のk-標準形の性質を利用した. そのあらすじは次の通り. 1. 第2種が多数存在すると仮定すれば, M_1, M_2, M_3 の3型に分類される. さらに M_1 はL1, L2(Paley型はL2に属す)に細分される. 2. M_2, M_3 の不存在を証明する. 3. L1の不存在を証明する. 4. L2は同値類をただ1つだけ含むことを証明する.

2. H行列の予備考察

H行列の定義, 次数 n , 同値などは文献[W1, K2]参照. ここでは $n=4k=28, k=7$; $[n_{28}] = \{1, 2, \dots, 28\}$; $[k_7] = \{1, 3, 5, 7\}$; HはH行列とする. Hまたはその部分行列の元で $1 \rightarrow 0, -1 \rightarrow 1$ としたものを2進形または2進表示という.

2.1. k-標準形

定義1: 全成分が1である k 次元ベクトルを j であらわし, Hにおいて最初の3行が

$$\begin{array}{cccc} j & j & -j & -j \\ j & -j & j & -j \\ j & -j & -j & j \end{array}$$

であるとき, このHを k -標準形という.

定義2: Hを行について4等分した部分行列を, 上から順にA, B, C, Dであらわし, それぞれ第1, 2, 3, 4行quadrantという. 同様に列quadrant A^*, B^*, C^*, D^* を定義する. またHの部分行列Xが 列quadrant Y^* と重なる部分 $X \cdot Y^*$, $Y=A, B, C, D$ をXの Y^* 部分といい, X_{Y^*} であらわす.

XがHの行に関するもの場合は, X^* はそれに対応する列に関するものをあらわす.

定義3: Xを $\{1, -1\}$ 上の n 行 m 列の行列とする. Xの第 i 行

ベクトルを X_i で、 X_i の高さ (X_i の元の総和) を $\text{ex}(X_i)$ であらわす。 X の n 個の行ベクトル X_i の高さの絶対値 $|\text{ex}(X_i)|$, $i \in [n_{28}]$ を元素とするベクトルを s ベクトルといい、 $s(X)$ であらわす。

定義4: 次のようなベクトル x を n 次の eq ベクトルといい、 $V=(k-x_4)/2$ を eq ベクトル x の特性数と呼ぶ。

$$x=(x_1, x_2, x_3, \dots, x_n), \quad x_i \in [k_7], \quad i \in [n_{28}];$$

$$\|x\|^2 = (x_1)^2 + (x_2)^2 + (x_3)^2 + \dots + (x_n)^2 = nk,$$

$$k = x_1 = x_2 = x_3 \geq x_4 \geq \dots \geq x_n \geq 1.$$

命題1: 28 次の eq ベクトルは 次の 2 つだけである。

$$\text{eq}[28, 1] = 7^3 5^1 1^{24}; \quad \text{eq}[28, 2] = 7^3 3^3 1^{22}.$$

ただし、 7^3 等は部分ベクトル $(7, 7, 7)$ を意味する。 証明略。

命題2: 28 次第 2 種の H 行列 H の場合 $s(A')$ の元を大きさ順に並べ換えれば、 eq ベクトル $\text{eq}[28, 2]$ (H の生成 eq ベクトルという) となる。 証明略。

定義5: H の生成 eq ベクトルの特性数 V を H の特性数といい、 $V(H)$ であらわす。

$$\text{命題3}([K1] \text{ の Theorem 2}): V(H)=2 \Rightarrow V^*(H)=V(H^T)=2.$$

証明略。

定義7: $s(A^*) = \text{eq}[28, 2]$ となる H を s -標準形という。

命題4: Paley行列型のHは第2種である. 証明略.

定義8: Hから3行をとって作った行列をtripletという.
各行の高さが一様なtripletを次数nの UETと呼び,
 $\text{Tr}(p, q, r)$ (p, q, r は行番号) であらわす. $\text{ex}(\text{Tr}_1)$ をUET
 Tr の高さといい, $\text{ex}(\text{Tr})$ であらわす.

以後 次の記号を使用する.

$\{1, -1\}$ 上の行列をXとするとき, $-X$ を X' であらわす.
したがって $1' = -1$.

$$(1, 1, 1) = j, \quad j^T = e, \quad (1', 1, 1) = a^T, \quad (1, 1', 1) = b^T,$$

$$(1, 1, 1') = c^T; \quad \{i\} = \{i, i'\}, \quad i = a, b, c, e, j,$$

$$\{abc\} = \{a, a', b, b', c, c'\}, \quad \{eabc\} = \{e\} \cup \{a, b, c\}.$$

$$w(\text{Tr}, i) = |\{x \mid x \in \{i\}, x \in \text{Tr}\}|, \quad i = e, a, b, c,$$

$$w(\text{Tr}, +i) = |\{x \mid x = i, x \in \text{Tr}\}|, \quad i = e, a, b, c,$$

$$w(\text{Tr}, -i) = |\{x \mid x = i', x \in \text{Tr}\}|, \quad i = e, a, b, c$$

をそれぞれ Tr の i 重さ, $+i$ 重さ, $-i$ 重さといい, Tr の正
味 i 重さ w^* を

$$w(\text{Tr}, +i) - w(\text{Tr}, -i) = w^*(\text{Tr}, i), \quad i = a, b, c, e$$

と定義する. まぎれない限り, $w(\text{Tr}, i)$ を $w(i)$ と書く.

命題5: $\text{Tr} \in H \Rightarrow w(\text{Tr}, i) = k, \quad i = e, a, b, c.$ 証明略.

2.2. L-標準形とL行列

定義1: $\{1, -1\}$ 上の2つの等長ベクトル x, y 間の距離を、これらを2進表示したときのHamming距離で定義する。

定義2: k -標準形で、 A^* に高さ3の行が3行あるとき、これを sk -標準形という。

$\{i \mid \text{ex}(A^*_i)=3\}=[c2]$ と置き、 $[c2]$ の行からの UET を $\text{Tr}(c2)$ であらわす。 $\text{Tr}(c2)_X$ ($X=A, B, C, D$) ごとに Hamming距離を3辺の長さとする3角形 ($c2$ -3角形) を作る。これら4つの $c2$ -3角形によって第2種 H 行列を M_1, M_2, M_3 の3つの型に分類する。これら以外に型はない。この分類は H の同値変換で固定される。

命題1: A の $c2$ -3角形は、 M_1, M_2, M_3 に応じてそれぞれ $(2, 2, 2), (2, 2, 4), (2, 4, 4)$ に分類される。 証明略。

定義3: H も H^T も k -標準形で、 A が含む $\text{Tr}(c2)$ の行数が最大のものを L -標準形といい、このときの $A \cdot A^*$ から最初の3行3列を除いたものを L 行列という。

命題2: H は常に sk -標準形にも L -標準形にも同値変換することができる。 証明略。

命題3: L -行列によって、 M_1 は $L1, L2$ に、 M_2 は $L3, L4$ に、 M_3 は $L5, L6, L7, L8$ に細分される。これらは H の同値変換で

固定される. sk-標準形とL-標準形とは, M_1, M_2 では一致し, M_3 では一致しない. Paley型はL2に属する. 証明略.

これら8個の2進形のL行列は次の通りである.

$$L_i = \begin{pmatrix} 0011 \\ 0101 \\ 1001 \\ 111f \end{pmatrix}, \begin{matrix} f=0 \Rightarrow i=1, \\ f=1 \Rightarrow i=2. \end{matrix}$$

$$L_i = \begin{pmatrix} 0011 \\ 0101 \\ 1010 \\ 11f1 \end{pmatrix}, \begin{matrix} f=0 \Rightarrow i=3, \\ f=1 \Rightarrow i=4. \end{matrix}$$

$$L_i = \begin{pmatrix} 0011 \\ 0101 \\ 1011 \\ 111f \end{pmatrix}, \begin{matrix} f=0 \Rightarrow i=5, \\ f=1 \Rightarrow i=6. \end{matrix}$$

$$L_i = \begin{pmatrix} 0011 \\ 0101 \\ 1f11 \\ 11f1 \end{pmatrix}, \begin{matrix} f=0 \Rightarrow i=7, \\ f=1 \Rightarrow i=8. \end{matrix}$$

命題4: 上の8個のL行列は, 同値なものを除いて, すべてを尽くしている. 証明略.

3. 制限定理

木村予想の証明のため $M_2, M_3, L1$ を1つずつ除いてゆく. これには 後出の3.2.の3命題(命題1,2,3)が主役を演じる. 準備をする.

3.1. HのdoubletとUET.

定義1: $p, q \in [n_{2s}], p \neq q$. $Db(p, q)$ で H_o, H_o で作った

Hの部分行列 (doubletという) をあらわす。これから次の2つの3値ベクトルを誘導する。

$$Db(p, q, +) = (1/2)(H_i + H_{i'}), \quad Db(p, q, -) = (1/2)(H_i - H_{i'}).$$

定義2: $\alpha^T = (1, 1), \beta^T = (1, 1'), 1' = -1;$

$$Db(p, q)_+ = (Db(p, q) | \alpha) = \alpha Db(p, q, +),$$

$$Db(p, q)_- = (Db(p, q) | \beta) = \beta Db(p, q, -).$$

$Db(p, q)_+, Db(p, q)_-$ をそれぞれ $Db(p, q)$ の α, β 部分という。

$p, q, r, s, t \in [n_{2g}]$ で、どの2つも disjoint とする。

命題1: (1) $Db(p, q, +), Db(p, q, -)$ は H_t と直交する。

(2) $Db(p, q, +), Db(p, q, -), Db(r, s, +), Db(r, s, -)$ の4者のいずれの2つも直交する。

(3) $ex(Db(p, q, +)) = (ex(H_p) + ex(H_q))/2,$

$$ex(Db(p, q, -)) = (ex(H_p) - ex(H_q))/2.$$

(4) $ex(Db(p, q, +)_X) = ex(Db(p, q, +))/4,$

$$ex(Db(p, q, -)_X) = ex(Db(p, q, -))/4; X=A, B, C, D.$$

命題2: Tr が UET で、 $ex(Tr) \neq 0$ ならば、 $Tr_X (X=A, B, C, D)$ の行の高さは一様で、 $ex(Tr_X) = ex(Tr)/4.$

定義3: $Tr_X, X=A, B, C, D$ において、 $ex(Tr_X)$ に寄与しな

い元 $x (\in \{eabc\})$ を Tr_x から取り除いたものを Tr_x の主部といい、 $HT(Tr_x)$ であらわす。

列の置換による同値を \sim で あらわす。

命題2: $X=A, B, C, D$ として

$ex(Tr_x)=1 \Rightarrow HT(Tr_x) \sim e, e'abcabc, eea'b'c', abc;$

$ex(Tr_x)=3 \Rightarrow HT(Tr_x) \sim eabcabc, eeabc, eee.$ 証明略.

3.2. Hの特別なUET

ここではHをsk-標準形とし、以後 次の記号を使用する。

$eee = J; abc = S_0, bca = S_1, cab = S_2, acb = S_0^-, bac = S_1^-, cba = S_2^-.$ $\{J\} = \{J, J'\}; \{S, +\} = \{S_0, S_1, S_2, \};$
 $\{S\} = \{S_0, S_1, S_2, S_0', S_1', S_2'\}; \{JS\} = \{J\} \cup \{S\}.$

注意: J_0, S_0 等の添え字 0, 1 等は例外で、行ベクトルではない。 $\{JS\}$ は $\{1, 1'\}$ 上の3次の巡回行列全体の集合、 $S_i^-, S_i'^-$ 等は逆巡回行列である。

$Tr(1, 2, 3) = G1, Tr(c2) = G2$ と置く。TrをUETとして、

$Tr_A^\circ = Tr \setminus Tr_A.$ この記号は他にも流用する。

一般性を害することなく、 $G1, G2_A$ を次のように標準化する。これをS標準化という。

$$G1 = JJe(S_0)^T.$$

$$G1_A = JJe, \quad (G1_A)^\circ \sim (S_0')^T,$$

$$G2_A = JS_0 e', \quad (G2_A)^c \sim J(S_0)^2 (S_1)^2 (S_2)^2, \quad (M_1 \text{型}),$$

$$G2_A = JS_2^{-1} c', \quad (G2_A)^c \sim J(S_0)^2 (S_1)^2 S_2 eaa', \quad (M_2 \text{型}),$$

$$G2_A = eecS_2^{-1} c', \quad (G2_A)^c \sim JS_0 S_1 (S_2)^2 eaaa' bb', \quad (M_3 \text{型}).$$

$ex=4$ である次の2つのUETをG3,G4であらわす。

$$(G3)_A = S_0' Je', \quad (G4)_A = S_0' Se, \quad .S \in \{S, +\}.$$

命題1: M_2, M_3 では, G2はG3,G4のどれとも直交しない。

証明には, 次のようなtripletの変換を応用する。

ω を1の3乗根, $\eta^T = (\omega, \omega^2, 1)$ とし, $x (\in \{eabc\})$ を $f(x) = (\eta, x)(-1/2)$ に変換すれば, $f(e)=0, f(a)=\omega, f(b)=\omega^2, f(c)=1; f(a)+f(b)+f(c)=0$ となる。この変換fを UET Trの列ベクトルごとに行ったものをf(Tr)とする。このとき2つのUET Tr1, Tr2に対して

$$(Tr1, Tr2) = 0 \Rightarrow (f(Tr1), f(Tr2)) = 0$$

が成立する。ただし, (x, y) は x, y の内積である。この性質を活用して証明を完了させることができる。

$Q = Qu(p, q, r, s)$ の行の高さは1様で, ± 4 とする。Qを2進表示して, $W = w(Q_1 + Q_2 + Q_3 + Q_4), V(Q) = \min(n - W, W) / 4$ と置けば, 第2種では 次の公式(a)が成立する[K2].

$$V(Q) = 2, 3. \quad (a)$$

さらに, $Db(p, q) = Db1, Db(r, s) = Db2$ と置く。

命題2: 次の条件(B)を満足させるHは存在しない.

(B): HはL-標準形で, 上記のQについて

$$(Db1_A, Db2_A) \geq 3\alpha, \quad w(Db1_A, \alpha) = w(Db2_A, \alpha) \geq 5$$

が成立する.

証明: Qの直交性, 公式(a), 条件(B)の三者は両立しない故, 命題不成立なら矛盾が生じる. 証明終.

命題3: HがL-標準形であれば, H^T に組(G1, G2, G3)または組(G1, G2, G3)が含まれる.

証明: G1, G2が含まれることは自明, G3, G4だけを論じればよい. M_1 では明かである. M_2 および M_3 の場合はそれぞれ3.3.および3.4.で証明する.

3.3. M_2 の不存在

3.2.の命題3の証明 (M_2 の場合). 3.1.の命題2によって, $(G2)_X$, $X=B, C, D$ には少なくとも1個 eがあり, H^T にはG3が存在する. またG4も存在する. 証明終.

定理1 (第1制限定理): M_2 は存在しない.

証明: M_2 では3.2.の命題1, 3の2つが同時に成立する. L3型では, L-行列が対称であるから, L3型が存在するとすれば, 矛盾が生じる. L4, L7型のHのL-行列には $(L4)^T = (L7)$ の関係があり, 3.2.の命題1は両者に共通

であるから、 L_4 の存在は矛盾である。

証明終。

3.4. M_3 の不存在

3.2.の命題3の証明 (M_3 の場合)。3.3.の議論で L_7 は存在しない。 L_5, L_6, L_8 型は、3.2.の命題2に該当するものを除外した残りが G_3 または G_4 を含む。

証明終。

定理2 (第2制限定理) : M_3 は存在しない。

証明略。

3.5. L_1 の不存在

定理3 (第3制限定理) : L_1 型は存在しない。

証明 : $Qu(4, 5, 6, 7)$ を考察すれば、3.2.の命題2の条件(B)に該当するものが必ず存在することがわかる。よって L_1 型は存在しない。

証明終。

4. L_2 型の H の同値類の単一性

定理1, 2, 3によって、第2種は L_2 型に限定された。これはPaley型が L_2 型に属することと矛盾しない。以後 H はすべて L_2 型とする。 L_2 型の H の同値類を検討することが残された問題である。これについて次の定理が成立する。

定理4 : L_2 ,したがって 第2種の H の同値類は ただ1つである。

2つの方法で証明される。Hの同値変換の自己同型群 $\text{Aut}(H)$ の部分群の3重可移性を応用する法と、Hの構成法から単一性を示す法である。ここでは前者による。証明の準備をする。

4.1. L2の型の標準化

L2型の性質を整理する。以後 sk -標準形で、一般性を害することなく、さらに次のように標準化する。

$$G_1 = JJe \quad (S_0')^7,$$

$$G_2 = JS_0e' \quad JS_0S_1S_2 \quad S_0S_1S_2,$$

$$G_{3a} = a'b'c'eeee' = S_0'Je',$$

$$G_{4a} = a'b'c'abce = S_0'S_0e.$$

Hの行を、disjointな9組のUET $G_i, i=1, 2, \dots, 9$ と1つの行とに、次のように分解する。

$$H = \{G_1, G_2, H_7, G_3, G_4, G_5, G_6, G_7, G_8, G_9, \}.$$

ただし $G_1 = \text{Tr}(1, 2, 3)$, $G_2 = \text{Tr}(4, 5, 6)$, $G_3 = \text{Tr}(8, 9, 10)$,
 $G_4 = \text{Tr}(11, 12, 13)$, \dots , $G_9 = (26, 27, 28)$;

$$\text{ex}(G_i) = 4, \quad i=3, 4, 5, 6; \quad \text{ex}(G_i) = -4, \quad i=7, 8, 9.$$

同じことを列についても行う。これらをおの順序に G_i が並んだ部分行列の記号としても流用する。

4.2. HのJS標準形

定義1: H から H_7 と H_7^* とを除いた心行列が $\{JS\}$ 上の行列である(逆巡回を含まぬ)とき, H はJS型であるといい, $H \in \{JS\}$ であらわす.

命題1: $H \in \{JS\}$, $(H_7^*)^T = H_7 = ee'1'eeee'e'e'$.

証明: 3.2.の命題1の証明の手法による. 証明終.

JS型では $(G1)^* = (G1)^T$, $(G2)^*_A = (G2)_A^T$, $H_7^* = H_7^T$ であるが, 一般性を害することなく, $(G2)^* = (G2)^T$ とすることができる. つまり $A^* = A^T$ で, H は A と A^* とでふちどられた形になる.

定義2: 上に述べた形のJS型をJS標準形という.

命題1: H はJS標準形に同値変換することができる.

証明略.

以後 H はJS標準形であるとする.

4.3. H の自己同型群

$\text{Aut}(H)$ は H の行と列とに作用するが, ここでは行への作用に着目し, 簡単のため行 H_i を i と書き, $[n_{28}]$ を Ω で, $\text{Aut}(H)$ から中心を除いたものを $\text{Aut}^*(H)$ であらわし, $\text{Aut}^*(H_p) = \Sigma$ と置く. Paley型を H_p であらわす.

命題1: Σ は1次分数変換群 $LF(3^3)$ に同型であって, (Σ, Ω) は3重可移, $(\Sigma_7, \Omega - 7)$ は2重可移のFrobenius群

である。 ([H1],[K4],[O1] 参照。) 証明略。

定義1: 置換 s_1 を次のように定義する。

$$s_1 = (123)(456)(7)(8910)(11\ 12\ 13)(14\ 15\ 16) \\ (17\ 18\ 19)(20\ 21\ 22)(23\ 24\ 25)(26\ 27\ 28).$$

命題2: $\text{Aut}^*(H) \supseteq \langle s_1 \rangle$.

証明: H が JS 標準形であるからである。 証明終。

命題3: H_p には s_1 の他に 2 つの置換 s_2, s_3 があり

$$|\langle s_i \rangle| = 3; \langle s_i \rangle \in \Sigma_7; i=1, 2, 3. \quad \text{証明略.}$$

$$\sigma = \langle s_1 \rangle \times \langle s_2 \rangle \times \langle s_3 \rangle \text{ と置く.}$$

命題4: $\sigma \subseteq \text{Aut}^*(H)$.

証明: H 行列の同値を \simeq であらわす。 $H_p \simeq H$ なら明か。

$H_p \simeq H$ でないとする。 H_p の s_1 を s_2 に移す同値変換で、 H_p を固定するものを t とする。 t を H に施せば、 H の s_1 は H^t の s_4 ($\neq s_1$) に移る。 ここで、 H も H_p も A^* を共有していることに注意すれば、 $s_4 = s_1$ である。 故に $\langle s_1 \rangle \subseteq \text{Aut}^*(H)$.

s_2 についても同様であるから、 $\sigma \subseteq \text{Aut}^*(H)$. 証明終。

4.4. 定理 3 の 証明

もし定理が成立しなければ、少なくとも 1 つ H_p に同値でない H がある。 H_i と $(H_p)_i$ とをできるだけ一致させるようにしても、 $i=8, 9, \dots, 28$ の なかに一致しないものが

少なくとも1つある。これを i とする。 Σ は3重可移であるから、その中の一つの元 r を選んで、
 $(H_i)^r = H_i = H_{p_i} = (H_{p_i})^r$ となるようにすることができる。
 他方 $H_i \neq H_{p_i}$ 。これは矛盾である。 証明終。

5. 結言

以上の議論で28次のHadamard行列の第2種に関する木村予想は真であることがわかった。

この結果から、28次のHadamard行列の同値類の個数は第1種が486、第2種が1、合わせて487である。

n 次の H 行列の同値類の個数を $N(n)$ とすれば、次のよう
 で、28次まではすべて明かになった。 ~~これらはすべて奇数である。~~ ^{ku}

$$N(2) = 1, N(4) = 1, N(8) = 1, N(12) = 1, N(16) = 5,$$

$$N(20) = 3, N(24) = \overset{60}{\cancel{59}}, N(28) = 487.$$

終わりに当たって 榎本、伊藤の両教授に謝意を表する次第である。

文献および注

[H1] M. Hall: Note on the Mathieu group M_{12} ,
 Archiv der Mathematik, 13, 334-340(1962).

[I1] N.Ito: Hadamard matrices with "doubly transitive" automorphism groups, Archiv der Mathematik, 35, 100-111(1980).

[K1] H. Kimura, H. Ohmori: Graphs and Combinatorics 2, 247-257(1986).

[K2] 喜安: アダマール行列とその応用, 1980.

[K3] 木村のその後の研究によって, 486個と決定.

[K4] W.M.Kantor: Automorphism groups of Hadamard matrices, Journ.Comb. Theory, 6, 279-281(1969).

[O1] 大山 豪: 有限置換群, 1971.

[W1] W.D.Wallis, A.P.Street, J.S.Wallis: Combinatorics, 1972.

Translation planes of order q^3

that admit a collineation group of order q^3

福岡大学理学部 秋山 献之

尼崎南高校 末竹 千博

1. Introduction

translation plane についての研究は新しい plane を構成すること, collineation group の一般的性質を調べること, 知られた plane をその collineation group のもつ (置換群または抽象群としての) 性質から特徴付けることなどを中心として行なわれている。とくに新しい plane の構成については最近非デサール plane の無限列が次々とみつかっているがその大部分は translation plane でありしかも kernel 上 2次元のものが圧倒的に多い。したがって collineation group による特徴付けも kernel 上 2次元の plane に対して行なわれることが多い。

ここで述べる結果は kernel 上 3次元の translation plane についての1つの試みであり挑戦である。

2. Translation plane

$F = GF(q)$ ($q = p^e$, p : 素数, $e > 0$: 整数), $d > 0$: 整数

$V = V(2d, q)$ とする.

(1) V のいくつかの d -次元 F -部分空間 W_i の集合 S が次の条件をみたすとき, V の spread という.

i) $V = \cup W_i$

ii) $V = W_i \oplus W_j$ ($i \neq j$)

$W_i \in S$ の 成分 という. 定義より $|S| = q^d + 1$ である.

(2) $GL(d, q) \cup \{0\}$ の部分集合 Σ が次の条件をみたすとき, spread set という.

i) $|\Sigma| = q^d$, $0 \in \Sigma$

ii) $A, B (\neq) \in \Sigma \Rightarrow \det(A - B) \neq 0$

spread が与えられると, 適当な基底をとることにより spread set が得られ, 逆も成立することが知られている.

(3) $S = \{W_i\}$ を spread とする. このとき

点として, V の q^{2d} 個のベクトル全体 \mathcal{E} ,

直線として, $q^{2d} + q^d$ 個の剰余類 $W_i + v$ ($W_i \in S, v \in V$)

の全体を, Incidence として 集合の包含関係を考える.

これらで定まる結合構造 Π を 位数 q^d の

translation plane という.

このとき $T = \{ \tau_a : V \rightarrow V; x \mapsto x+a \mid a \in V \}$ を

Π の translation group といふ。

spread が与えられると上のようにして translation plane が得られ、逆も成立することが知られている。

(4) 有限集合 \mathcal{Q} に加法と乗法が定義されていて次の条件をみたすとき、quasi field といふ。

i) \mathcal{Q} は加法に関して群をなす (零元 $\in 0$ とかく)。

ii) $\mathcal{Q} - \{0\}$ は乗法に関して loop をなす (単位元 $\in 1(a)$ とかく)。

iii) $a0 = 0 \quad (\forall a \in \mathcal{Q})$

iv) $(a+b)c = ac + bc \quad (\forall a, b, c \in \mathcal{Q})$

このとき

$K(\mathcal{Q}) = \{ k \in \mathcal{Q} \mid k(a+b) = ka + kb, (ka)b = k(ab) \quad (\forall a, b \in \mathcal{Q}) \}$

を \mathcal{Q} の kernel といふ。 $K(\mathcal{Q})$ は体であり、 \mathcal{Q} は $K(\mathcal{Q})$ 上のベクトル空間をなすことが知られている。

translation plane が与えられると座標系を定めることにより quasi field が得られ、逆も成り立つことが知られている。

Π を translation plane とし、 \mathcal{Q} を対応する quasi field とする。 \mathcal{Q} がより良い代数系であれば、 Π もより良い構造をもつ plane であることが期待される。

例えば、 \mathbb{Q} が体であれば、 \mathbb{T} は "デカルト" plane になる。

quasifield \mathbb{Q} がさらに次の条件をみたすとき semifield といふ。

$$v) a(b+c) = ab+ac \quad (\forall a, b, c \in \mathbb{Q})$$

semifield から定義される plane を semifield plane といふ。

この plane は dual plane と translation plane であることが知られている。

また、 \mathbb{Q} の $K(\mathbb{Q})$ 上の次元を \mathbb{T} の次元 といふ。次元が小さい程 \mathbb{T} が良い構造の plane であることが期待される。次元 1 の plane は "デカルト" plane であり、2次元の plane がよく調べられている。

\mathbb{T} の自己同型を collineation といふ、collineation 全体 $\text{Aut } \mathbb{T}$ は、 $\text{Aut } \mathbb{T} = T \cdot (\text{Aut } \mathbb{T})_0$ (半直積) とかけることが知られている。ここで $(\text{Aut } \mathbb{T})_0$ は 0 の stabilizer でありこれを $C(\mathbb{T})$ とおき、 \mathbb{T} の translation complement といふ。また、 $C(\mathbb{T}) \leq PL(2d, \mathbb{Q})$ であることが知られている。そこで $LC(\mathbb{T}) = C(\mathbb{T}) \cap GL(2d, \mathbb{Q})$ とおき、これを linear translation complement といふ。

\mathbb{T} の性質は $LC(\mathbb{T})$ の中に多くみつけられるので collineation group $G \leq LC(\mathbb{T})$ をとって特徴付けを考えることが多い。

3. Problems

Π を位数 q^d の semifield plane とすると, $LC(\Pi)$ は位数 q^d の部分群 G を含むことが知られている。

そこで次の問題が提出される。

Problem Π を位数 q^d の translation plane とし, Π の kernel を $GF(q)$ とする。 $LC(\Pi)$ が位数 q^d の部分群 G を含むとき, G 及び Π を決定せよ。

2次元 ($d=2$) の場合には, W.M. Kantor [7] や C. Bartolone [3] 等により別の問題として議論され, N.L. Johnson, V. Jha [5,6] 等により本格的に議論された。その結果, 新しいいくつかの plane が構成され, 特徴付けられ, いくつかの分類定理が得られている。これらについての最近の結果については [4] を参照されたい。

N.L. Johnson 等は 3次元以上の例を知らなかったようだが, 3次元の plane の例がある。3次元についての問題が我々の議論の対象である。

4. Sherk plane of order 27

F. A. Sherk は $GF(3)$ 上の 27 個の 3 次行列で spread set となるものをみつけ、位数 27 の translation plane Π を構成した [9]。この plane を位数 27 の Sherk plane といふ。F. A. Sherk の興味は $C(\Pi) (= LC(\Pi))$ が小さい plane といふことであつた。

M. L. Narayana Rao and K. Satyanarayana は $C(\Pi)$ を完全に決定した [8]。 $C(\Pi)$ の位数は $3^4 \cdot 2$ である。

と 3 で、この $C(\Pi)$ をよく調べてみると位数 27 の部分群 G が存在し、次の性質をもっていることが分つた。

i) G は アーベル群である。

ii) G は 無限遠点 (∞) を固定し、無限遠直線 l_∞ から (∞) を除いた $l_\infty - \{(\infty)\}$ 上に正則に作用する。

iii) E は G の elation group とすると、 $|E| = 3$ で、 G/E は アーベル群である。

$$iv) G = \left\{ M(a, b, u) = \begin{bmatrix} A(a, b) & B(a, b, u) \\ 0 & A(a, b) \end{bmatrix} \mid a, b, u \in GF(3) \right\}$$

とかける。

$$\text{ここで } A(a, b) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}, \quad B(a, b, u) = \begin{bmatrix} u & f & g \\ b & u & f \\ a & b & u \end{bmatrix},$$

$$f = 2a + 2b + 2b^2 + 2a^2b + au$$

$$g = a + a^2 + 2b + 2ab + ab^2 + bu.$$

Sherk plane について 次の結果を得た.

定理 [1] Π を位数 27 の translation plane で semifield plane でないとする. $LC(\Pi)$ が位数 27 のアーベル群 G を含むならば, Π は位数 27 の Sherk plane である.

5. Translation planes of order q^3

前節の定理の一般化を考える. 次の情況を考えることにする.

仮定. Π を位数 q^3 の translation plane で Π の kernel は $GF(q)$ であるとする. $LC(\Pi)$ が位数 q^3 の群 G を含み, G は次の条件をみたすとする.

- i) G は $(\omega) \in$ 固定し, $(\omega - \{(\omega)\})$ 上に正則に作用する.
- ii) $E \in G$ の elation group とするとき, $|E| = q$ で G/E はアーベル群である.

主定理 [2] (Π, G) 以上の仮定をみたすとき, 適当に基底 \mathcal{E} とることにより

$$G = \left\{ \left[\begin{array}{cc|c} A(a, b) & B(a, b, u) & \\ 0 & A(a, b) & \end{array} \right] \mid a, b, u \in GF(q) \right\} \text{ とかける.}$$

ここで, $A(a, b)$, $B(a, b, u)$ は $GF(q)$ から $GF(q)$ への $1 < \nu < 3$ の関数と $GF(q)$ の定数により一意的に書ける (定理 1, 1', 2', 3' を見よ).

よって Π は spread set $\Sigma = (X=0) \cup \{(Y=0) \mid a \in G\}$ から得られる plane である。

ここで, $(X=0) = \{(0, y) \mid y \in V(d, \mathfrak{g})\}$, $(Y=0) = \{(x, 0) \mid x \in V(d, \mathfrak{g})\}$.

遂に, (Π, G) が上で与えられるならば, 上の仮定をみたす。

以下, この定理をより正確に述べることにする。

(Π, G) が仮定をみたすとする。

G がアーベル群のとき, Π を desirable plane といい,

G が非アーベル群のとき, Π を elusive plane といい。

(これは $d=2$ のときの N.L. Johnson and F.W. Wilke [6] に従ったものである。)

仮定より

$$\Pi \text{ が desirable のとき, } A(a, b) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Pi \text{ が elusive のとき, } A(a, b) = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{array}{l} \text{よって} \\ \text{type I といい} \end{array}$$

$$\text{または} \quad \begin{bmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{array}{l} \text{よって} \\ \text{type II といい} \end{array}$$

$$\text{または} \quad \begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \quad \begin{array}{l} \text{よって} \\ \text{type III といい} \end{array}$$

とわかる。

また、仮定より

$$E = \left\{ \left[\begin{array}{cc} I & C(u) \\ 0 & I \end{array} \right] \mid C(u) \in GL(3, \mathbb{F}) \cup \{0\}, u \in GF(\mathbb{F}) \right\}$$

とかける。このとき $C(u)$ は

$$\Pi \text{ が desirable のとき, } C(u) = \begin{bmatrix} u & r & s \\ 0 & u & r \\ 0 & 0 & u \end{bmatrix},$$

$$\Pi \text{ が elusive of type I のとき, } C(u) = \begin{bmatrix} u & 0 & s \\ 0 & u & r \\ 0 & 0 & u \end{bmatrix},$$

$$\Pi \text{ が elusive of type II のとき, } C(u) = \begin{bmatrix} u & r & s \\ 0 & u & 0 \\ 0 & 0 & u \end{bmatrix},$$

$$\Pi \text{ が elusive of type III のとき, } C(u) = \begin{bmatrix} u & r & s \\ 0 & u & r \\ 0 & 0 & u \end{bmatrix},$$

ここで, $r, s: GF(\mathbb{F}) \rightarrow GF(\mathbb{F})$ は u の加法的関数で,

$r(1) = s(1) = 0$ である。

仮定より

$$B(a, b, u) = \begin{bmatrix} u & f & g \\ h & i & j \\ k & l & m \end{bmatrix} \text{ とよくとくことができる。}$$

ここで, $f, g, h, i, j, k, l, m: GF(\mathbb{F})^3 \rightarrow GF(\mathbb{F})$ は a, b, u の関数である。

さて, f, g, h, i, j, k, l, m を決めなければならぬが

A) desirable の場合と B) elusive の場合に別けて述べることにする。

A) desirable plane の場合

$r=s=0$ のとき, $\Pi \in$ likeable plane と"う。

(これは $d=2$ のとき, W.M. Kantor [7] に従ってのことである。)

次のことが"合"る。

定理 0 $\Pi \in$ 位数 $q^3 = p^{3e}$ (p :素数) の desirable plane とする。このとき

a) $p \neq 2, 5$

b) $p = 3 \Rightarrow \Pi$ は likeable plane と"ある。

desirable plane に"いて 次の結果が"得られる。

定理 1. $\Pi \in$ 位数 $q^3 = p^{3e}$, $p \geq 7$, の desirable plane

\Leftrightarrow i) 加法的関数 $r, s, f_1, f_2, g_1, g_2 : GF(q) \rightarrow GF(q)$

$r(u) = s(u) = 0$ と定数 $j_0 \in GF(q)$ が"存在して

$$f = f_1(a) - \frac{1}{2} f_2(a^2) + \frac{1}{3} r(a^3) + f_2(b) - r(ab)$$

$$+ \frac{1}{4} a^4 + \frac{1}{2} b^2 - a^2 b + au + r(a),$$

$$g = a f_1(a) - \frac{1}{2} a f_2(a^2) + \frac{1}{3} ar(a^3) - ar(ab)$$

$$+ g_1(a) - \frac{1}{2} g_2(a^2) + \frac{1}{3} s(a^3) + g_2(b) - s(ab)$$

$$+ \frac{1}{2} j_0 a^2 + \frac{1}{20} a^5 - \frac{1}{2} ab^2 + bu + ar(u) + su,$$

$$h = b, \quad i = u, \quad j = f + j_0 a$$

$$k = a, \quad l = b, \quad m = u.$$

ii) $\det A(a, b)^T B(a, b, u) = 0 \Leftrightarrow a = b = u = 0.$

系 $\Pi \in$ 位数 $q^3 = p^{3e}$, $p \geq 7$, の likeable plane

\Leftrightarrow i) 加法的関数 $f_1, f_2, g_1, g_2 : GF(q) \rightarrow GF(q)$ と定数

$j_0 \in GF(q)$ が存在して

$$f = f_1(a) - \frac{1}{2} f_2(a^2) + f_2(b) + \frac{1}{4} a^4 + \frac{1}{2} b^2 - a^2 b + au,$$

$$g = a f_1(a) - \frac{1}{2} a f_2(a^2) + a f_2(b) + g_1(a) - \frac{1}{2} g_2(a^2) + g_2(b)$$

$$+ \frac{1}{2} j_0 a^2 + \frac{1}{20} a^5 - \frac{1}{2} a b^2 + bu,$$

$$h = b, \quad c = u, \quad j = f + j_0 a,$$

$$k = a, \quad l = b, \quad m = u.$$

$$\text{ii) } \det A(a, b)^{-1} B(a, b, u) = 0 \Leftrightarrow a = b = u = 0.$$

B) elusive plane の場合

次のことが分る。

定理 0' $\Pi \in$ 位数 $q^3 = p^{3e}$ (p : 素数) の elusive plane

とある。このとき

a) $p = 3$

b) $r = s = 0$

elusive plane of type I と elusive plane of type II

について次の結果が得られる。

定理 1' Π Σ 位数 3^{3e} の elusive plane of type I

\Leftrightarrow i) 加法的関数 $f_1, f_2, j_1, j_2 : GF(3^e) \rightarrow GF(3^e)$ と

定数 $\hat{c}_0, f_0 (\neq 0), \hat{f}_0 \in GF(3^e)$ かつ存在して

$$f = f_0 a + \hat{f}_0 b + b^2,$$

$$g = f_1(a) + f_2(b) - f_0 a^2 - \hat{c}_0 b^2 + bu,$$

$$h = b - a^2, \quad i = \hat{c}_0 b - ab + u,$$

$$j = j_1(a) + j_2(b) + \hat{f}_0 a - b^2 + \hat{c}_0 ab - a^2 b + au,$$

$$k = a, \quad l = -b, \quad m = -\hat{f}_0 a + \hat{c}_0 b + ab + u.$$

$$\text{ii) } \det A(a, b)^{-1} B(a, b, u) = 0 \Leftrightarrow a = b = u = 0.$$

定理 2' Π Σ 位数 3^{3e} の elusive plane of type II

\Leftrightarrow i) 加法的関数 $f_1, f_2, g_1, g_2 : GF(3^e) \rightarrow GF(3^e)$ と

定数 $\hat{c}_0, \hat{f}_0, \hat{c}_0, \hat{c}_0, \hat{m}_0 \in GF(3^e)$ かつ存在して

$$f = f_1(a) - \hat{c}_0 a^2 + f_2(b) - \hat{c}_0 b^2 + a^2 b + au,$$

$$g = g_1(a) - \hat{f}_0 a^2 + g_2(b) - \hat{m}_0 b^2 + \hat{f}_0 ab - ab^2 + bu,$$

$$h = -b, \quad i = \hat{c}_0 a + ab + u, \quad j = \hat{f}_0 a + \hat{c}_0 b + b^2$$

$$k = a, \quad l = -a^2 + \hat{c}_0 b, \quad m = \hat{f}_0 a + \hat{m}_0 b - ab + u.$$

$$\text{ii) } \det A(a, b)^{-1} B(a, b, u) = 0 \Leftrightarrow a = b = u = 0.$$

elusive plane of type III について次の結果が得られる。
定理 3'. 位数 3^{3e} の elusive plane of type III は
存在しない。

以上 A), B) をあわせて, 仮定をみたす (Π, G) の
特徴付けが出来た。

最後に非存在に関するいくつかの結果を述べる
定理 Π を位数 p^3 , $p \geq 7$, の desirable plane とする。

a) $p \neq 7, 11, 13,$

b) $p \equiv 5 \pmod{12}$

定理 Π を位数 3^{3e} の likeable plane とする。

a) $e=1 \Rightarrow \Pi$ は位数 27 の sherk plane

b) $e \neq 2, 3.$

定理 1, 定理 1', 定理 2' により特徴付けられた
plane を決定することが当面の目標である。

新しい plane の構成も含めて 仮定をより一般化して
より広い class と, については完全な分類が大きな目標
となる。

参考文献

1. K. Akiyama : On the Sherk plane, (submitted)
2. K. Akiyama and C. Suekake : Translation planes of order q^3 that admit a collineation group of order q^3 , (submitted)
3. C. Bartolone : On some translation planes admitting a Frobenius group of collineations, *Ann. Disc. Math.* 18 (1983), 37-54.
4. M. Biliotti, V. Jha, N. L. Johnson and G. Menichetti : A structure theory for two-dimensional translation planes of order q^2 that admit collineation groups of order q^2 , *Geom. Dedicata* 29 (1989), 7-43.
5. J. B. Fink, N. L. Johnson and F. W. Wilke : A characterization on "likeable" translation planes, *Rend. Circ. Mat. Palermo* 32 (1983), 76-99.
6. N. L. Johnson and F. W. Wilke : Translation planes of order q^2 that admit a collineation group of order q^2 , *Geom. Dedicata* 15 (1984), 293-312.
7. W. M. Kantor : On point-transitive affine planes, *Isr. J. Math.* 42 (1982), 227-234.

8. M.L. Narayana Rao and K. Satyanarayana : On Sherk's plane of order 27, *Linear Alg. Appl.* 74 (1986), 1-9.
9. F.A. Sherk : A translation plane of order 27 with a small translation complement, *Geom. Dedicata* 9 (1980), 307-316.

Some recent works
on flag-transitive geometries of type
 $c^k X_m$.

Satoshi Yoshiara
Department of Information Science
Faculty of Science
Hirosaki University
Hirosaki, Aomori 036 JAPAN

Symposium on Algebraic Combinatorics
Hirosaki, July 26, 1990.

1 Introduction.

The aim of my talk is to give a survey of recent researches on flag-transitive $c^k X_n$ -geometries, focusing on $c.C_2$ -geometries, where X_n is a Coxeter diagram of spherical type. Since more than a half of the sporadic finite simple groups are known to have flag-transitive actions on some of these geometries (see §2), it is important to characterize these geometries as well as their automorphism groups. At present, the following 15 sporadic simple groups are characterized via their geometries of type $c^k X_n$: M_{22} , M_{23} , M_{24} , Fi_{22} , Fi_{23} , Fi'_{24} , McL , Suz , HS , J_2 , $Co.3$, $Co.1$, M_{12} , He and Ru .

The list of main contributors to these results involves: Buekenhout, Del Fra, Ghinelli, Hubaut, Hughes, Meixner, Pasini, Weiss, and Yoshiara:

There is another survey [13] of these geometries, including much more details, but not $c^k.G_2$ - nor $c^k.I_m$ -geometries.

Organization of this survey is as follows: Basic terminology on incidence geometry will be explained in §2 (see [3] for details), as well as a brief motivation for the study of incidence geometries in §3. Then the characterization theorems of flag-transitive geometries of type $c^k.A_m$, $c^k.D_m$; $c^k.C_m$; and $c^k.G_2$, $c^k.I_8$, $c.I_{12}$ are summarized in §4, §5, and §7, respectively. Some examples of flag-transitive $c^k.C_2$ -geometries will be briefly described in §6. The last section §8 involves several problems attracting my attention.

I would like to thank Professor Antonio Pasini, Professor Thomas Meixner and Professor Richard Weiss for giving me helpful information through letters, preprints and discussion.

2 Basic definitions.

2.1 (Incidence) geometries.

We consider an ordered sequence $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1, \dots, \mathcal{G}_{r-1}; *)$ of r ($r \geq 2$) pairwise disjoint nonempty sets \mathcal{G}_i together with a reflexive and symmetric relation $*$ on their union $\mathcal{G}_0 \cup \dots \cup \mathcal{G}_{r-1}$. The relation $*$ is called the *incidence* of \mathcal{G} . A *flag* of \mathcal{G} is a subset F of $\mathcal{G}_0 \cup \dots \cup \mathcal{G}_{r-1}$ of pairwise incident elements, that is, $x * y$ for any $x, y \in F$. Such an ordered sequence is called an (incidence) *geometry* on $I := \{0, \dots, r - 1\}$, if any flag is contained in a maximal flag C with $|C \cap \mathcal{G}_i| = 1$ for each $i \in I$.

The number r is called the *rank* of \mathcal{G} . A geometry \mathcal{G} of rank r is called *thick* (res. *thin*), if for any flag F with $|F| = r - 1$ there are at least 3 (res. exactly two) maximal flags containing F . The *incidence graph* of \mathcal{G} is the graph with the set of vertices $\mathcal{G}_0 \cup \dots \cup \mathcal{G}_{r-1}$ and the set of edges $\{\{x, y\} | x \in \mathcal{G}_i, y \in \mathcal{G}_j, x * y, i \neq j \in I\}$.

2.2 Residues.

For a flag F , the subset $\{i \in I \mid F \cap \mathcal{G}_i \neq \emptyset\}$ of I is called the *type* of F and denoted by $Type(F)$. For each $j \in I - Type(F)$, we set

$$\mathcal{G}_j(F) := \{x \in \mathcal{G}_j \mid x * y \text{ for all } y \in F\}.$$

The *residue* \mathcal{G}_F of \mathcal{G} at F is defined to be the subgeometry $(\mathcal{G}_{j_1}, \dots, \mathcal{G}_{j_m}; *)$ on $I - Type(F)$, where we arrange the elements j_1, \dots, j_m of $I - Type(F)$ so that $j_1 < j_2 < \dots < j_m$, $m = |I - Type(F)|$.

A geometry \mathcal{G} is called *residually connected* if incidence graphs of \mathcal{G}_F at any flags F (including $\mathcal{G}_\emptyset = \mathcal{G}$) are connected.

2.3 Flag-transitive geometries.

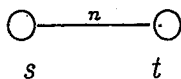
A geometry \mathcal{G} (or a pair (\mathcal{G}, G)) is called *flag-transitive* if there is a subgroup G of $Aut(\mathcal{G})$ acting transitively on the set of maximal flags of \mathcal{G} . If a flag-transitive geometry (\mathcal{G}, G) is residually connected, we have $G = \langle G_{x_0}, \dots, G_{x_{r-1}} \rangle$ for any maximal flag $F = \{x_0, \dots, x_{r-1}\}$.

2.4 Some geometries of rank 2.

1.4.1 Generalized n -gons. A geometry $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1; *)$ is called a *generalized n -gon* if its incidence graph is of diameter n and girth $2n$ for some $n \in \mathbb{N}$, $n \geq 2$.

If the numbers $|\mathcal{G}_0(y)|$ (res. $|\mathcal{G}_1(x)|$) do not depend on particular choices of $y \in \mathcal{G}_1$ (res. $x \in \mathcal{G}_0$), say $s + 1$ (res. $t + 1$), the pair (s, t) is called the *order* of a generalized n -gon \mathcal{G} . If \mathcal{G} is flag-transitive, its order can be defined.

We use the following convention to denote the fact that a geometry $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1; *)$ is a generalized n -gon of order (s, t) :



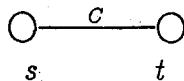
A geometry $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1; *)$ is a generalized 2-gon if and only if any element $x \in \mathcal{G}_0$ is incident with any element of \mathcal{G}_1 , that is, $x * y$ for any $x \in \mathcal{G}_0$ and $y \in \mathcal{G}_1$.

The projective points and lines of a projective plane form a generalized 3-gon (generalized triangle) with the incidence $*$ defined by (symmetrized) inclusion. The Desarguesian projective plane π defined on a finite field \mathbb{F}_q has order (q, q) (q is called the *order* of π).

Let V be a vector space over \mathbb{F}_q with a non-degenerate symplectic, orthogonal or unitary form f (or a quadratic form q for $q = 2^e$) of Witt index 2 (thus $\dim V \leq 6$). In the projective space $PG(V)$ associated with V , we let $\mathcal{Q}_0 :=$ the set of isotropic (singular) projective points with respect to f and $\mathcal{Q}_1 :=$ the set of isotropic (singular) projective lines with respect to f . The incidence $*$ is defined by inclusion. Then the geometry $\mathcal{Q} = (\mathcal{Q}_0, \mathcal{Q}_1; *)$ is a generalized 4-gon (*generalized quadrangle*). These generalized quadrangles \mathcal{Q} are called *classical*. They are flag-transitive, because they admit the corresponding simple Lie groups of rank 2 ($O_4^+(q)$, $S_4(q) \cong O_5(q)$, $U_4(q^2) \cong O_6^-(q)$, $U_5(q^2)$) as flag-transitive automorphism groups. Except the generalized quadrangle admitting $O_4^+(q)$, classical generalized quadrangles are thick, that is, their orders (s, t) satisfy $s \geq 2$ and $t \geq 2$.

1.4.2 Circle Geometries. A geometry $\mathcal{C} = (\mathcal{C}_0, \mathcal{C}_1; *)$ is called a $(k-)$ circle geometry if we can identify \mathcal{C}_0 , \mathcal{C}_1 and $*$ with the set of vertices, edges and the adjacency of a complete graph on k vertices for some $k \in \mathbb{N}$, respectively. If \mathcal{C} is a k -circle geometry, we have $|\mathcal{C}_0(y)| = 2$ for any $y \in \mathcal{C}_1$ and $|\mathcal{C}_1(x)| = k - 1$ for any $x \in \mathcal{C}_0$.

We use the following convention to denote the fact that a geometry $\mathcal{C} = (\mathcal{C}_0, \mathcal{C}_1; *)$ is a k -circle geometry:



2.5 Flag-transitive geometries belonging to diagrams.

From now on, we mainly consider flag-transitive and residually connected geometries \mathcal{G} . Then for each $i, j \in I$ ($i < j$) the residues $\mathcal{G}_F = (\mathcal{G}_i(F), \mathcal{G}_j(F); *)$ at flags F of type $I - \{i, j\}$ are isomorphic to each other. We denote by $\Delta(i, j)$ the isomorphism class of the residues \mathcal{G}_F at flags F of type $I - \{i, j\}$.

Assume that for a flag-transitive, residually connected geometry \mathcal{G} the isomorphism type $\Delta(i, j)$ is either a generalized $m_{i,j}$ -gon or a $k_{i,j}$ -circle geometry. Let Δ be the diagram on the index set I with bonds defined as follows:

- (1) i and j are joined by $m_{i,j} - 2$ edges
 $\bigcirc \text{---} \bigcirc$ if $\Delta(i, j)$ is a generalized $m_{i,j}$ -gon.
- (2) i and j are joined by the edge
 $\bigcirc \text{---}^c \bigcirc$ if $\Delta(i, j)$ is a $k_{i,j}$ -circle geometry.

We say that \mathcal{G} belongs to the diagram Δ .

3 Motivations.

The following observation attracted attentions of many mathematicians to the study of flag-transitive incidence geometries.

Observation. (Buekenhout, Kantor, Ronan and Smith, Ronan and Stroth etc. See, f. g. [4])

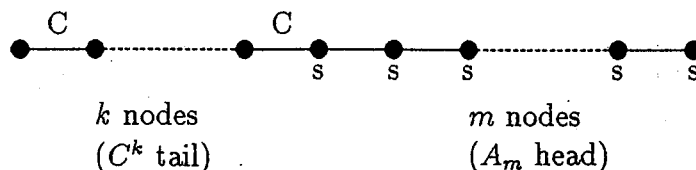
- (1) Any finite simple group G of Lie type X_n ($X = A, C, D, E, F, G$) acts flag-transitively on the *building* \mathcal{G} associated with it. The building \mathcal{G} belongs to the diagram isomorphic to the corresponding Coxeter diagram of type X_n .

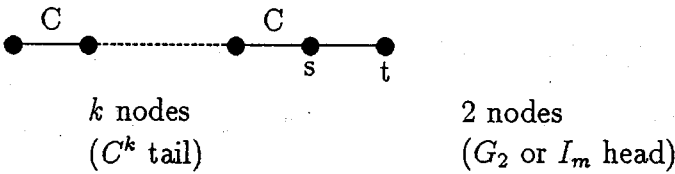
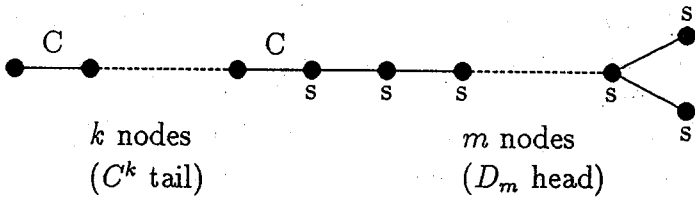
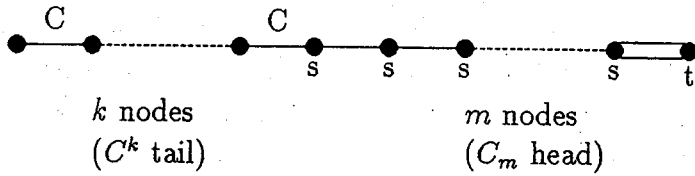
- (2) The alternating group A_n acts flag-transitively on the *thin buildings* of type A_{n-1} .
- (3) For a sporadic finite simple group G except J_4 , F_3 , F_5 and ON , there is a geometry \mathcal{G} on which G acts flag-transitively, belonging to a diagram Δ consisting of bonds $\bigcirc \overset{n}{-} \bigcirc$ and $\bigcirc \overset{c}{-} \bigcirc$.

If the diagram Δ consists of bonds $\bigcirc \overset{n}{-} \bigcirc$ only, a geometry belonging to Δ is called a *GAB* (Geometry which is an almost building). They are closely related to (infinite) buildings and deep investigation has been done (see [17], [9], [14]).

How about the case in which \mathcal{G} belongs to a diagram with bonds $\bigcirc \overset{n}{-} \bigcirc$ and $\bigcirc \overset{c}{-} \bigcirc$? The main aim of my talk is to give you a survey of recent characterizations of flag-transitive geometries belonging to diagrams of these types.

Specifically, we consider geometries belonging to a diagram Δ with k nodes consisting of circle geometries and a tail isomorphic to the Coxeter diagram X_n of spherical type (that is, $X_n = A_n$ ($n \geq 2$), C_n ($n \geq 2$), D_n ($n \geq 4$), E_n ($n = 6, 7, 8$), F_4 , G_2 or $I_2(m)$ ($m \geq 2$)). Such geometries are called flag-transitive geometries of type $c^k X_n$, or $c^k X_n$ -geometries. In a $c^k X_n$ -geometry \mathcal{G} , a $D(F)$ -residue means a residue \mathcal{G}_F at a flag F belonging to the diagram $D(F)$.





In this survey, except §7, we only consider flag-transitive $c^k X_m$ -geometries with *thick* X_m -residues. However, there are many known interesting flag-transitive $c^k X_n$ -geometries (see §7 and [13] for $X_n = C_2$) with non-thick X_m -residues. Furthermore, we assume that each residues of type $I - \{i, j\}$ is finite, that is, \mathcal{G} is locally finite (but not necessarily finite).

4 Flag-transitive geometries of type $c^k A_m$ and $c^k D_m$.

A $c^k A_1$ -geometry \mathcal{G} is isomorphic to the geometry of i -subsets ($i = 0, \dots, k$) of a set of size $k + s$. For $c^k A_m$ -geometries with $m \geq 2$, the classification has been done by D. Hughes in 1965. Note that here we do not need flag-transitivity.

Theorem 4.1 [8] *If \mathcal{G} is a flag-transitive $c^k A_m$ -geometry with $m \geq 2$, then $(\mathcal{G}, \text{Aut}(\mathcal{G}), k, A_m)$ is one of the following. In (3), (4), (5), $m = 2$ and A_m is a projective plane ($m = 2$) of order 4.*

- (1) *an r -dimensional affine geometry of order 2, $Af(r, 2)$, $k = 1$, A_m : $(r - 1)$ -dimensional projective space ($m = r - 1$) of order 2 ($r = 3, 4, \dots$);*
- (2) *the geometry of the Steiner system $S(3, 6, 22)$, $M_{22}.2$, $k = 1$;*
- (3) *the geometry of the Steiner system $S(4, 7, 23)$, M_{23} , $k = 2$;*
- (4) *the geometry of the Steiner system $S(5, 8, 24)$, M_{24} , $k = 3$;*

Meixner noticed that the above classification yields the following result. Here, again, we do not need flag-transitivity.

Theorem 4.2 *Any geometry \mathcal{G} belonging to the diagram of type $c^k D_m$ is an affine building of type \tilde{D}_m of order 2.*

5 Flag-transitive geometries of type $c^k C_m$.

It turns out that the classification of $c^k C_m$ -geometries is much harder than that of $c^k A_m$ - and $c^k D_m$ -geometries. Here we need essential use of flag-transitivity, which is enable us to use (locally finite) group theory. We separate the case $m \geq 3$ and $m = 2$, because the latter case

(low dimensional case) seems to be the crucial point, as is usual in geometry.

We first describe the results in the case $m \geq 3$. In this case, C_m -residues are buildings of spherical type of rank ≥ 3 , and therefore, they are associated with finite groups of Lie type B_m, C_m for $m \geq 3$ by Tits [18]. In particular, C_2 -residues are flag-transitive classical generalized quadrangles. For the details about each geometries, see [13] §3 and 4.1,2.

Theorem 5.1 [7], [10] *If \mathcal{G} is a flag-transitive $c^k C_m$ -geometry with $m \geq 3$, then \mathcal{G} is isomorphic to one of the following.*

- (1) *an affine polar space or its standard quotient for any $m \geq 3$, in which the C_m -residues are finite buildings and C_2 -residues are of order $(2, t)$;*
- (2) *the Neumaier geometry with $(k, m) = (1, 3)$, in which C_3 -residues are sporadic A_7 -geometry (Neumaier geometry);*
- (3) *one of the 3-transposition geometries for groups F_{22}, F_{23}, F'_{24} and the triple cover of that for F'_{24} with $(k, m) = (1, 3), (2, 3), (3, 3)$ and $(3, 3)$, respectively. In each of these geometries, C_3 -residues are $U_6(2)$ -buildings.*

On the other hand, the classification of flag-transitive $c.C_2$ -geometries leads us to the classification of flag-transitive finite generalized quadrangles, which seems to be much more difficult problems. At present, besides the classical quadrangles, there are only two (or four, counting their duals) known generalized quadrangles admitting flag-transitive automorphism groups (see [9] p.98). They are of order $(3, 5)$ and $(15, 17)$.

Thus we try to classify flag-transitive $c.C_2$ -geometries with C_2 -residues classical generalized quadrangles. A pioneering work has done by Buekenhout and Hubout [2] in 1977, under several restrictions on the action of groups. Del Fra, Ghinelli, Meixner and Pasini [7] tried to

reduce the classification to the case Buenhout and Hubout considered, as well as modifying some incorrect arguments in [2], but not entirely rewriting [2]. In [7], they left the characterization of flag-transitive $c.C_2$ -geometries with C_2 -residues $H(3, 3^2)$ as an open problem, which has been classified by Weiss and Yoshiara [22] by coset enumerations using computer. This method turns out to be very effective to solve all the cases and one more overlooked geometry in the case treated in [2] was found by coset enumeration during the re-classification. In [26], the author gives a short and comprehensible proof of the classification. Thus, now we have established the following results by [26], [22], [7] (though we may omit to quote this paper), [6] (for the case $s = 2$):

Theorem 5.2 *Assume that $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2; *)$ is a $c.C_2$ -geometry ($k = 1$ and $m = 2$) with C_2 -residues classical generalized quadrangles, admitting a flag-transitive group $G \subseteq \text{Aut}(\mathcal{G})$. Then the isomorphism classes of residues \mathcal{G}_p at $p \in \mathcal{G}_0$, $|\mathcal{G}_0|$ and G satisfy one of the following. In each case, \mathcal{G} is uniquely determined.*

(0) *an affine polar space or its standard quotient;*

$$(0.1) \quad \mathcal{G}_p \cong W(2), |\mathcal{G}_0| = 16, G \cong 2^4 : A_6 \text{ or } 2^4 : S_6, \text{ or (double cover) } \mathcal{G}_p \cong W(2), |\mathcal{G}_0| = 32, G \cong 2^5 : A_6 \text{ or } 2^5 : S_6;$$

$$(0.2) \quad \mathcal{G}_p \cong Q_5^-(2), |\mathcal{G}_0| = 28, G \cong S_6(2) \text{ or (double cover) } \mathcal{G}_p \cong Q_5^-(2), |\mathcal{G}_0| = 56, G \cong S_6(2) \times 2;$$

$$(0.3) \quad \mathcal{G}_p \cong W(2), |\mathcal{G}_0| = 64, G \cong 2^6 : O_6^-(2) \text{ or } 2^6 : O_6^-(2).2;$$

$$(1) \quad (\text{Two-set geo. } S(4)) \quad \mathcal{G}_p \cong W(2), |\mathcal{G}_0| = 28, G \cong A_8 \text{ or } S_8;$$

$$(2) \quad (\text{Orth. geo. } O^+(6)) \quad \mathcal{G}_p \cong H(3, 2^2), |\mathcal{G}_0| = 126, O_6^-(3) \subseteq G \subseteq O_6^-(3).2^2 \text{ or (triple cover } O^+(6)) \\ \mathcal{G}_p \cong H(3, 2^2), |\mathcal{G}_0| = 378, 3.O_6^-(3) \subseteq G \subseteq 3.O_6^-(3).2^2 ;$$

$$(3) \quad (\text{Unit. geo. } U(5)) \quad \mathcal{G}_p \cong W(3), |\mathcal{G}_0| = 176, G \cong U_5(2) \text{ or } U_5(2).2;$$

$$(4) \quad (\text{Orth. geo. } O^-(5)) \quad \mathcal{G}_p \cong W(2), |\mathcal{G}_0| = 36, G \cong O_5(3) \text{ or } O_5(3).2;$$

- (5) (3-local geometry for *McL*) $\mathcal{G}_p \cong Q_5^-(3)$, $|\mathcal{G}_0| = 275$, $G \cong \text{McL}$ or *McL.2*;
- (6) (3-local geometry for *Suz*) $\mathcal{G}_p \cong H(4, 3^2)$, $|\mathcal{G}_0| = 22880$ $G \cong \text{Suz}$ or *Suz.2*;
- (7) (a geometry for *HS.2*) $\mathcal{G}_p \cong H(4, 3^2)$, $|\mathcal{G}_0| = 1100$, $G \cong \text{HS.2}$.

Remarks. (a) The geometries (1)–(4) above are first members of infinite families of $c^k C_m$ -geometries (see the next theorem by Meixner and §6).

(b) The geometries (5)–(7) above are “sporadic” examples. The geometries (5) and (6) are 3-local geometries of *McL* and *Suz*, respectively. For the geometry (7) for *HS.2* (sometimes called Yoshiara geometry), see 6.4.

Meixner extended the above classification to flag-transitive geometries of type $c^k C_2$. He also gave independent proofs of characterizations of several flag-transitive $c.C_2$ -geometries by means of graph theory. As for geometries S_n , $O^\pm(n+1)$, and $U(n+1)$, see §6.

Theorem 5.3 [10],[11] *Assume that \mathcal{G} is a flag-transitive $c^k.C_2$ -geometry with $k \geq 2$, in which C_2 -residues are classical generalized quadrangles. Then \mathcal{G} and a perfect flag-transitive automorphism group of \mathcal{G} are isomorphic to one of the following.*

- (1') the two-set geometry $S(k+1)$ for $A_{2(k+1)}$;
- (2') the positive orthogonal geometry $O^+(k+5)$ for $O_{k+5}^\mu(3)$, where $\mu = 1$ if $4|k+5$ and $\mu = -1$ otherwise (the sign μ is defined only when $k+5$ is even);
- (3') the unitary geometry $U(k+2)$ for $U_{k+4}(2)$;

- (4') *the negative orthogonal geometry $\mathcal{O}^-(k+4)$ for $O_{k+4}^\mu(3)$, where $\mu = -1$ if $4|k+4$ and $\mu = 1$ otherwise (the sign μ is defined only when $k+5$ is even);*
- (5') *a geometry for Co.3 or $2 \times$ Co.3;*
- (6') *a geometry for Co.1;*
- (2'') *the $c.C_2$ -residues are isomorphic to the triple cover of the positive orthogonal geometry for $3O_6^-(3)$;*
- (3'') *the $c^2.C_2$ -residues are isomorphic to the double or quadruple cover of the unitary geometry for $2U_6(2)$ or $2^2U_6(2)$, respectively;*
- (4'') *the $c^3.C_2$ -residues are isomorphic to the triple cover of the negative orthogonal geometry for $3O_7(3)$;*

6 Examples.

In this section, we briefly describe the four infinite families $\mathcal{S}(n)$, $\mathcal{U}(n+1)$, $\mathcal{O}^\pm(n+1)$ of flag-transitive $c^k C_2$ -geometries and a flag-transitive $c.C_2$ -geometry \mathcal{Y} for HS.2.

6.1 Two-set geometries $\mathcal{S}(n)$.

Let $I = \{1, \dots, 2n\}$, $n \in \mathbb{N}$ with $n \geq 4$. Define a graph $\Gamma = (V, E)$ by

$V :=$ the 2-subsets of I and for $A, B \in V$, $\{A, B\} \in E$ if and only if $A \cap B = \emptyset$.

Any maximal clique of Γ is of size n , which is uniquely determined by its subset of size $2(n-1)$. Define $\mathcal{S}_1, \mathcal{S}_2, \dots, \mathcal{S}_{n-2}$ and \mathcal{S}_n be the sets of 2-cliques, \dots , $2(n-2)$ -cliques and maximal cliques, respectively. It can be verified that the geometry $\mathcal{S}(n) := (\mathcal{U}_1, \dots, \mathcal{U}_{n-2}, \mathcal{U}_n; *)$ with $*$ determined by inclusion belongs to the diagram of type $c^{(n-3)}C_2$, on which A_{2n} acts flag-transitively.

6.2 Unitary geometries $\mathcal{U}(n+1)$.

Let W be an $(n+1)$ -dimensional vector space over \mathbb{F}_{2^2} with a non-degenerate hermitian form f . Define a graph $\Gamma = (V, E)$ by

$V := \{[x] \mid x \in V, f(x, x) = 1\}$, the set of non-isotropic points, and

for $[x], [y] \in V$, $\{[x], [y]\} \in E$ if and only if $f(x, y) = 0$.

Any maximal clique of Γ is of size $n+1$, which is uniquely determined by its subset of size $n-1$. Define $\mathcal{U}_1, \mathcal{U}_2, \dots, \mathcal{U}_{n-2}$ and \mathcal{U}_{n+1} be the sets of non-isotropic points, 2-cliques, \dots , $(n-2)$ -cliques and maximal cliques, respectively. It can be verified that the geometry $\mathcal{U}(n+1) := (\mathcal{U}_1, \dots, \mathcal{U}_{n-2}, \mathcal{U}_{n+1}; *)$ with $*$ determined by inclusion belongs to the diagram of type $c^{(n-3)}C_2$, on which $U_{n+1}(2^2)$ acts flag-transitively.

6.3 Orthogonal geometries $\mathcal{O}^\pm(n+1)$.

Let W be an $(n+1)$ -dimensional vector space over \mathbb{F}_3 with a non-degenerate symmetric form f with discriminant ε . Witt index of W is given by $w(n, \varepsilon) := (-\varepsilon)^m$ if $n+1 = 2m$. Define a graph $\Gamma = (V, E)$ by

$V = \{[x] \mid x \in V, f(x, x) = 1\}$, the set of non-isotropic points, and

for $[x], [y] \in V$, $\{[x], [y]\} \in E$ if and only if $f(x, y) = 0$.

Any maximal clique of Γ is of size $n+1$ for $\varepsilon = 1$ and n for $\varepsilon = -1$. We denote by $\mathcal{O}_i^\varepsilon$ the set of i -cliques. It can be verified that the geometries $\mathcal{O}^+(n) := (\mathcal{O}_1^+, \dots, \mathcal{O}_{n-4}^+, \mathcal{O}_{n+1}^+; *)$ and $\mathcal{O}^-(n) := (\mathcal{O}_1^-, \dots, \mathcal{O}_{n-3}^-, \mathcal{O}_n^-; *)$ with $*$ determined by inclusion belong to the diagrams of type $c^{(n-4)}C_2$ and $c^{(n-3)}C_2$, respectively. The group $O_{n+1}^w(3)$ acts flag-transitively on $\mathcal{O}^\varepsilon(n+1)$, where the index $w = 1$ if $n+1$ is odd and $w = w(\varepsilon, n)$ if $n+1$ is even.

6.4 Yoshiara geometry.

Let $\Gamma = (V, E)$ be the graph for HS on 100 points. We define a new graph Γ' with E as the set of vertices by declaring

two edges $A = \{a_1, a_2\}$ and $B = \{b_1, b_2\}$ of E are joined in Γ' whenever $\{a_i, b_j\} \notin E$ for all $i, j = 1, 2$.

Let $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2$ be the sets of vertices, edges and the maximal clique of size 11 of the new graph above, respectively. Defining $*$ by inclusion, we have a geometry $\mathcal{H} = (\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2; *)$. It can be verified that \mathcal{H} belongs to the diagram of type $c.C_2$, on which $HS.2$ acts flag-transitively but HS does not (see [23]).

This geometry was first found by Yoshiara [23], and turns out to be the unique flag-transitive $c.C_2$ -geometry, in which the stabilizer of a point p does not induce the simple Lie group of rank 2 on the associated generalized quadrangle \mathcal{G}_p (see [22]).

7 Flag-transitive geometries of type $c^k.G_2$, $c^k.I_8$ and $c^k.I_{12}$.

Weiss [19], [20], [21] has classified flag-transitive $c^k.G_2$ -, $c^k.I_8$ and $c^k.I_{12}$ -geometries, under an interesting condition. As is shown in [14], the universal 2-covers of geometries \mathcal{G} of type $c.G_2$ and $c.I_m$ are infinite ($m \geq 8$). This shows that the classification of such geometries \mathcal{G} are almost hopeless and that we need some condition implying the finiteness of \mathcal{G} . Weiss consider the following condition $(*)$ for a geometry $\mathcal{G} = (\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2; *)$ of type $c.X_2$:

- $(*)$ there exists three elements $p_i \in \mathcal{G}_0$ ($i = 1, 2, 3$) for which p_i and p_j are incident with an element $c(i, j) \in \mathcal{G}_2$ for any $1 \leq i \neq j \leq 3$, but there is no element $c \in \mathcal{G}_2$ incident with all p_i ($i = 1, 2, 3$).

This condition is mainly used to restrict the size of the kernel on a residue at $p \in \mathcal{G}_0$ (see [19] (2.3), [20] (2.2), [21] (2.4)) for flag-transitive

$c.G_2$ -, $c.I_8$ - and $c.I_8$ -geometries. On the other hand, among 13 classes of $c.C_2$ -geometries in Theorem 5.2, the geometry (7) for $HS.2$ is the unique one satisfying the condition (*). Nevertheless, we can restrict the size of kernels for arbitrary flag-transitive classical $c.C_2$ -geometries (see [22] Lemma 3, Cor. 4). This seems to be closely related to the following fact: the diameter of the collinearity graph of a $c.C_2$ -geometry is bounded by $s + 1$ [5], where (s, t) is the order of a residue at $p \in \mathcal{G}_0$.

In Weiss' theorems below, *classical hexagons* mean thick hexagons associated with $G_2(q)$ and ${}^3D_4(q)$ or the point-thin hexagons obtained from Desarguesian projective planes. Similarly, *classical octagons* are thick octagons for ${}^2F_4(2^m)$ or the point-thin octagons obtained from self-dual classical generalized quadrangles for $S_4(2^m)$. *Classical dodecagons* mean point-thin dodecagons obtained from self-dual hexagons for $G_2(3^m)$.

Theorem 7.1 *Assume that \mathcal{G} is a flag-transitive $c^k.G_2$ -geometry with G_2 -residues classical hexagons, which satisfies the condition (*) and admits a flag-transitive group $G \subseteq \text{Aut}(\mathcal{G})$. Furthermore, if $G_2(2)$ -residue is point-thin, we assume that the stabilizer of a flag F corresponding to $G_2(2)$ induces $L_3(q).2$ on \mathcal{G}_F .*

(a) *If $k = 1$, then $|\mathcal{G}_0|$ and G satisfy one of the following. In each case, \mathcal{G} is uniquely determined.*

- (1) $|\mathcal{G}_0| = 100$ and $G \cong J_2$ or $J_2.2$;
- (2) $|\mathcal{G}_0| = 1782$ and $G \cong \text{Suz}$ or $\text{Suz}.2$;
- (3) $|\mathcal{G}_0| = 64$ and $G \cong 2^6 : U_3(3)$ or $2^6 : G_2(2)$ or (double cover)
 $|\mathcal{G}_0| = 128$ and $G \cong 2^7 : U_3(3)$ or $2^7 : G_2(2)$;
- (4) $|\mathcal{G}_0| = 36$ and $G \cong U_3(3).2$;
- (5) $|\mathcal{G}_0| = 162$ and $G \cong U_4(3).2_3$ or $U_4(3).(2^2)_{133}$;

(b) *If $k > 1$, there are two such $c^2.G_2$ -geometries, in which $c.G_2$ -residues are isomorphic to the (point-thin) geometries (5) above.*

- (1) $|\mathcal{G}_0| = 275$ and $G \cong McL.2$;
- (2) $|\mathcal{G}_0| = 276$ and $G \cong Co.3$ or (double cover)
 $|\mathcal{G}_0| = 552$ and $G \cong Co.3 \times 2$.

Theorem 7.2 *Assume that \mathcal{G} is a flag-transitive $c^k.I_8$ -geometry with I_8 -residues classical octagons, which satisfies the condition (*) and admits a flag-transitive group $G \subseteq Aut(\mathcal{G})$. Then $k = 1$. Furthermore, $|\mathcal{G}_0|$ and G satisfy one of the following. In each case, \mathcal{G} is uniquely determined.*

- (1) $|\mathcal{G}_0| = 4060$ and $G \cong Ru$;
- (2) $|\mathcal{G}_0| = 56$ and $G \cong L_3(4).2^2$ or (double cover)
 $|\mathcal{G}_0| = 112$ and $G \cong 2.L_3(4).2^2$;
- (3) $|\mathcal{G}_0| = 66$ and $G \cong M_{12}$ or (double cover)
 $|\mathcal{G}_0| = 132$ and $G \cong 2.M_{12}$;
- (4) $|\mathcal{G}_0| = 2058$ and $G \cong He.2$;

Theorem 7.3 *There is no flag-transitive $c^k.I_{12}$ -geometry \mathcal{G} with I_{12} -residues classical dodecagons, which satisfies the condition (*) and admits a flag-transitive group $G \subseteq Aut(\mathcal{G})$.*

8 Problems.

Finally, I pick up at random several problems attracting my attention.

1. Complete the classification of flag-transitive classical $c^k.C_2$ -geometry for the cases $(2^n), (3^n), (4^n)$ in the Meixner's theorem (see §6).
2. How about non-classical cases in the classification of flag-transitive $c.C_2$ -geometries (see §6) ?

3. Study geometrical conditions which implies the finiteness of the geometries of some fixed type, like (*) in the previous section (see §7).
4. Specifically, determine whether the universal 2-cover of the geometry of type:



5. Characterize F'_{24} or Monster via the diagram above (see [1]).
6. Determine the embeddings of these geometries (see [24], [25]).

References

- [1] F. Buekenhout and B. Fischer, A locally dual polar space for the Monster, unpublished (1982).
- [2] F. Buekenhout and X. Hubaut, Locally polar spaces and related rank 3 groups, *J. Algebra* 45 (1977), 391-434.
- [3] F. Buekenhout, Diagrams for geometries and groups, *J. Comb. Th. Ser. A* 27(1979), 121-151.
- [4] F. Buekenhout, Diagram geometries for the sporadic groups, in *Finite Groups: Coming of Age (Montreal Proceedings, 1982)*, 1-32, Contemporary Math. 45, Amer. Math. Soc., 1985.
- [5] P. Cameron, D. Hughes and A. Pasini, Extended Generalized Quadrangles, preprint, 1988.
- [6] H. Cuypers, Locally generalised quadrangles with affine spaces, preprint, 1989.
- [7] A. Del Fra, D. Ghinelli, T. Meixner and A. Pasini, Flag-transitive extensions of C_n -geometries, to appear in *Geom. Dedicata*.

- [8] D. Hughes, Extensions of designs and groups: projective, symplectic and certain affine groups, *Math. Z.* 89, (1965), 199-205.
- [9] W. Kantor, Generalized polygons, SCABs and GABs, in *Buildings and the Geometry of Diagrams*, Springer Lecture Notes 1181, Springer, 1986, 79-158.
- [10] T. Meixner, Some polar towers, preprint, 1989.
- [11] T. Meixner, Two geometries related to the sporadic groups Co_1 and Co_3 , preprint, 1989.
- [12] A. Pasini, A classification of a class of Buekenhout geometries exploiting amalgams and simple connectedness (groups for geometries in given diagrams, III), to appear in *Att. Sem. Mat. Fis., Univ. Modena*.
- [13] A. Pasini and S. Yoshiara, Flag-transitive Buekenhout geometries, preprint, July, 1990.
- [14] M. Ronan, Coverings of certain finite geometries, in *Finite Geometries and Designs*, eds. P. Cameron, J. Hirschfeld and D. Hughes, London Math. Soc. Lecture Notes 49 (1981), 316-331.
- [15] M. Ronan and G. Stroth, Minimal parabolic geometries for the sporadic groups, *Eur. J. Comb.* 5 (1984), 59-91.
- [16] G. Seitz, Flag-transitive subgroups of Chevalley groups, *Ann. Math.* 97 (1973), 27-56.
- [17] J. Tits, A local approach to buildings, in *The Geometric Vein*, Springer 1981, 519-547.
- [18] J. Tits, "Buildings of Spherical Type and Finite BN-pairs", Springer Lecture Notes 386, Springer, 1974.
- [19] R. Weiss, Extended generalized hexagons, to appear in *Math. Proc. Cambridge Phil. Soc.*

- [20] R. Weiss, A geometric characterization of the groups McL and Co_3 , submitted for publication.
- [21] R. Weiss, A geometric characterization of the groups M_{12} , He and Ru , preprint, August 1990.
- [22] R. Weiss and S. Yoshiara, A geometric characterization of the groups Suz and HS , *in press* (J. Algebra 133 (1990)).
- [23] S. Yoshiara, A locally polar geometry associated with the group HS , *Eur. J. Comb.*, 11 (1990), 81-93.
- [24] S. Yoshiara, The embeddings of flag-transitive classical locally polar geometries of rank 3. I, Odd characteristic case, to appear in *Geom. Dedicata*.
- [25] S. Yoshiara, The embeddings of flag-transitive classical locally polar geometries of rank 3. II, Even characteristic case, to appear in *Geom. Dedicata*.
- [26] S. Yoshiara, A classification of flag-transitive classical $c.C_2$ -geometries by means of generators and relations, submitted to *Eur. J. Comb.*

Note on a p -block of a finite group with abelian defect group

熊本大学 教養部 渡辺 アツミ

§1 序

(K, ϕ, F) を p -modular 系, 但し K は代数的閉体とする。 G を有限群, B を G の p -block, $k(B), l(B)$ とそれぞれ B の通常既約指標の個数, modular 既約指標の個数とする。 B の不足群 $D(B)$ が可換群である場合, B とその Brauer 対応子 B_0 との間には, $k(B) = k(B_0)$ であろうとの有名な予想がある。この予想については, G が p -可解群であるとき (Okuyama-Wajima [10], Dade [5]), G が一般の場合には $D(B)$ が巡回群のとき (Dade [4]), B の inertial index が 1, 2, 3 のとき (Brauer [1], Broué-Puy [3], Usami [11]) などいくつかの場合に肯定的に確かめられているが, $D(B)$ が位数 q の基本可換群の場合では未解決である (Kiyota [8] 参照)。最近 M. Broué は [2] において B と B_0 とは "同じタイプ" であるとの予想を出した。[2] の議論からその予想が正しければ上の $k(B)$ に関する予想及び Brauer の height 予想も正しくなる

が、さらに多元環として B と B_0 の中心 $Z(B)$ と $Z(B_0)$ が同型となる、 B と B_0 の下位不足群の重複度が等しくなるなどの B と B_0 との間の関係が成立することになる。本稿では G が p -可解群のとき B と B_0 の下位不足群の重複度が等しいことと指標論的方法で示す (§2, 定理)。なお下位不足群の重複度は block の Cartan 行列の単因子と決定するが、一般には B と B_0 の Cartan 行列は一致しない。

§2 下位不足群

G の p -block の全体を $Bl(G)$, 共役類の全体を $Cl(G)$ とする: $Bl(G) = \{B_1, B_2, \dots, B_r, \dots\}$ 。又 B_i に対応する群環 FG の block 中等元を E_i とする。このとき $Cl(G)$ は次の (i), (ii) と満たすように分割される。

(i) 各 $C \in Cl(G)$ は m かり 1 個の p -block に associate される。

(ii) 各 $B_i \in Bl(G)$ には $r(B_i)$ 個の共役類が associate され、それらを $C_1^i, C_2^i, \dots, C_{r(B_i)}^i$ とするとき $\{\hat{C}_j^i E_i \mid j = 1, 2, \dots, r(B_i)\}$ は $Z(FG)E_i$ の F -基底となる、但し \hat{C}_j^i は C_j^i の FG における

類組である。

上のような $\mathcal{C}(G)$ の分割と $\mathcal{C}(G)$ の block 分割とよぶ。
 $C \in \mathcal{C}(G)$ に対して $C_G(x)$ ($x \in C$) のシロ- p -部分群
 の一つを $D(C)$ と表わし $D(C)$ を C の不足群とよぶ。 G
 の部分群 L, M が G -共役であるとき、 $L \cong G M$ と
 書く。さて、上の (i), (ii) の下で Q を G の p -部分
 群とし

$$m(B_C, Q) = \# \{ C_j^T \mid D(C_j^T) \cong Q \},$$

$$m(B_C, Q)' = \# \{ C_j^T \mid C_j^T \text{ は } p\text{-正則類で} \\ D(C_j^T) \cong Q \}$$

とおく。これらの非負整数は $\mathcal{C}(G)$ の block 分割の
 仕方によらず B_C と Q だけで決まる。 $m(B_C, Q) \neq 0$
 のとき、 Q は B_C の下位不足群とよばれ、又 $m(B_C, Q)$
 は B_C の下位不足群としての Q の重複度とよばれる。
 $m(B_C, Q)$ に関する基本的性質を挙げておく (詳細につ
 いては 永尾・津島 [9] 参照)

$$(1) \quad l(B_C) = \# \{ C_j^T \mid C_j^T \text{ は } p\text{-正則類} \}$$

$$(2) \quad Q \text{ が } B_C \text{ の下位不足群ならば } Q \leq D(B_C).$$

$$m(B_C, D(B_C))' = 1$$

$$(3) \quad B_C \text{ の Cartan 行列の単因子としての } p^m \text{ の重複}$$

度 $= \sum_Q m(B_\pi, Q)'$, 但し Q は位数 p^m の G の p -部分群の全体の共役に関するある代表系と渡る。

$$(4) \quad m(B_\pi, Q) = \sum_{\bar{b}} m(\bar{b}, Q),$$

$$m(B_\pi, Q)' = \sum_{\bar{b}} m(\bar{b}, Q)',$$

但し \bar{b} は $\bar{b}^G = B_\pi$ なる $N_G(Q)$ の p -block の全体と渡る。

§1 の記号の下で, $D = D(B)$ とおき, D は可換群とする。又 B_0 は $N_G(D)$ の p -block とし, $b \in C_G(D)$ における B の root, すなわち b は $b^G = B$ となる $C_G(D)$ の p -block とする。得られた結果は次の通りである。

定理 G は p -可解群とする。 D の p -部分群 P に対して次のこと成立する。

$$m(b^{N_G(P)}, P) = m(b^{N_G(D) \cap N_G(P)}, P),$$

$$m(b^{N_G(P)}, P)' = m(b^{N_G(D) \cap N_G(P)}, P)'.$$

系 定理の条件の下で, G の p -部分群 Q に対して次のこと成立する。

$$m(B, Q) = \sum_R m(B_0, R),$$

$$m(B, Q)' = \sum_R m(B_0, R)',$$

ここで, R は Q と G -共役な $N_G(D)$ の p -部分群全体の $N_G(D)$ -共役に関する代表系と取る。

§3 定理の証明のための準備

H と G の正規部分群, ζ と G -不変な H の (通常) 既約指標と取る. $\bar{G} = G/H$, $\bar{x} = xH \in \bar{G}$ ($x \in G$) とおく.

\bar{x} は $[x, y] \in H$ なる任意の元 $y \in G$ に対して ζ の $\langle H, x, y \rangle$ へ拡張される時, ζ -special とよばれる. \bar{x} を含む \bar{G} の共役類も ζ -special とよばれる.

Gallagher [6, Theorem] により ζ^G の既約成分の個数は \bar{G} の ζ -special な共役類の個数に等しい.

補題 上の記号の下で, $\chi_1, \chi_2, \dots, \chi_n$ と ζ^G の既約成分の全体とする. このとき次のことが成立する.

(i) $x \in G$ に対して, \bar{x} が ζ -special であることと どれかの χ_i が xH 上で vanish (零) することは同値である.

(ii) C_1, C_2, \dots, C_n と $\{C_1 e_\zeta, C_2 e_\zeta, \dots, C_n e_\zeta\}$ が $(KG) e_\zeta$ の K -基底であるような G の共役類と取る, 但し e_ζ は ζ に対応する KH の中心原始中等

元, \hat{C}_j は C_j の KG における類和である。このとき $\{\bar{x}_j \mid j = 1, 2, \dots, s\}$ ($x_j \in C_j$) は \bar{G} の ζ -special な共役類の完全代表系となる。

証明は Watanabe [12] 参照。なお (1) の十分条件は Isaacs [7, chap. 11, problem 11.15] でおおむね得られる。

命題 1 H と G の正規 p' -部分群, ζ と G -不変な H の既約指標, $\bar{C}_1, \bar{C}_2, \dots, \bar{C}_s \in \bar{G}$ の ζ -special な共役類の全体とする。もし $B \in \{S\}$ を cover する G の唯一つの p -block であるならば, G の p -部分群 Q に対し

$$m(B, Q) = \#\{\bar{C}_j \mid D(\bar{C}_j) =_{\bar{G}} \bar{Q}\},$$

$$m(B, Q)' = \#\{\bar{C}_j \mid \bar{C}_j \text{ は } p\text{-正則類で} \\ D(\bar{C}_j) =_{\bar{G}} \bar{Q}\},$$

$$\text{但し } \bar{Q} = QH/H.$$

証明は Hong の second reduction の議論を用いて H が central の場合に帰着させ, そこにおい

ては補題を用いるが、くわしくは [12] 参照。なお命題において $\{G\}$ を cover する G の p -block $\alpha \rightarrow \beta$ は限らないとは、 $\{G\}$ を cover するすべての p -block の和集合に対して同様のことが成り立つ。

§4 定理の証明 (概略)

明らかに $P \triangleleft G$ としてよい。故に

$$(5) \quad m(B, P) = m(B_0, P), \quad m(B, P)' = m(B_0, P)'$$

を示せばよい。このことと Hong の reduction を用いて示す。又 $|G|$ に関する帰納法を用いる。 $H = O_p(G)$, ζ と B によって cover される H の既約指標 (正確には $\{G\}$ が B によって cover される), $T(\zeta)$ と ζ の inertial group とする。

$T(\zeta) < G$ の場合

B_1 と $\{G\}$ を cover しかつ $B = B_1^{G/T(\zeta)}$ となる $T(\zeta)$ の p -block とする。 B_1 と B の既約指標の全体は "誘導" により一対一に対応する。又、必要ならば ζ とその G -共役でおきかえることにより B_1 の不足群は D としてよい。 θ と ζ の Glauberman 対応子とする、つまり θ は $\zeta_{G(D)}$ の重複度が p で割れない唯一の既約成分で

ある。このとき $T(\theta) = T(\zeta) \cap N_G(D)$ 。 B_2 と $B_1 = \beta_2^{T(\zeta)}$ なる $T(\theta)$ の p -blocks とする。 B_2 は B_1 の Brauer 対応子で $B_0 = \beta_2^{N_G(D)}$ 。 さて $m(B, P) = m(B_1, P)$, $m(B, P) = m(B_1, P)$ 及び $m(B_0, P) = m(B_2, P)$, $m(B_0, P) = m(B_2, P)$ は容易に示せる。一方 B_2 と B_1 は帰納法の仮定が適用できるので (5) が成立する。

* $T(\zeta) = G$ の場合

G が p -可解群であることから, $G = HN_G(D)$, $O_p(N_G(D)) = C_H(D)$ が得られる。さらし B と B_0 はそれぞれ $\{1\}$, $\{0\}$ と cover する唯一の p -block である。

$\bar{G} = G/H$, $\bar{P} = PH/H$, $\bar{x} = xH$ ($x \in G$), $\bar{G} = N_G(D)/C_H(D)$, $\bar{P} = PC_H(D)/C_H(D)$, $\bar{x} = xC_H(D)$ ($x \in N_G(D)$) とおく。

[9, Theorem 2, (3)] より $x \in N_G(D)$ に対して, \bar{x} が ζ -special であることと \bar{x} が θ -special であることとは同値であることを示せる。従って \bar{G} と \bar{G} との自然な同型対応と命題から (5) が得られる。

系の証明 D が可換であるから $B = \beta^G$ となる $N_G(Q)$ の p -block β に対して D の部分群 P が $T(\theta)$ -共役と無視して一意的に存在して $[Q, \beta]$ と $[P, \beta^{N_G(P)}]$

は G -共役となる: $Q = P^x$, $B = (b^{N_G(P)})^x$ ($x \in G$),
 但し $T(b)$ は b の $N_G(D)$ における inertial group である。
 このとき $m(B, Q) = m(b^{N_G(P)}, P)$, $m(B, Q)' =$
 $m(b^{N_G(P)}, P)'$ であるから (4) と定理より系は得ら
 れる。

系と下位不足群の性質から $m(B, Q)$, $m(B, Q)'$ を求
 めるには $m(b^{T(b)}, R)'$ の値がわかることが必要となる
 が、これについて次のことが成立する。

命題 2 $D \in G$ の正規可換 p -部分群, $B \in D(B) =$
 D なる G の p -block, $b \in B$ によって cover される $C_G(D)$
 の p -block とする。 $T(b) = G$ と仮定し, $\zeta \in D$ 上
 自明なる通常既約指標とする。 $\{\chi_j C_G(D) \mid 1 \leq j \leq r\}$ が
 $G/C_G(D)$ の ζ -special な共役類の完全代表系ならば, G
 の p -部分群 R に対して

$$m(B, R)' = \#\{\chi_j C_G(D) \mid C_D(\chi_j) \stackrel{\#}{=} R\}.$$

証明は [12] 参照。

文 献

- [1] R. Brauer: On blocks and sections in finite groups II, *Amer. J. Math.*, 90 (1968), 895-925.
- [2] M. Broué: Isométries parfaites, types de blocs, catégories dérivées, *Rapport de Recherche du LMENS*, 89-3 (1989), 1-30.
- [3] M. Broué-L. Puig: A Frobenius theorem for blocks, *Invent. Math.*, 56 (1980), 117-128.
- [4] E. C. Dade: Blocks with cyclic defect groups, *Ann. Math.*, (2) 84 (1966), 20-48.
- [5] E. C. Dade: A correspondence of characters, *Proc. Symp. Pure Math.*, 37 (1980), 401-403.
- [6] P. X. Gallagher: The number of conjugacy classes in a finite group, *Math. Z.*, 118 (1970), 175-179.
- [7] I. M. Isaacs: *Character theory in finite groups*, Academic Press, New York, 1976.
- [8] M. Kiyota: On 3-blocks with an elementary abelian defect group of order 9, *J. Fac. Sci. Univ. Tokyo*, 31 (1984), 33-58.

- [9] 永尾汎・津島行男：有限群の表現，裳華房
- [10] T. Okuyama - M. Wajima: Character correspondence and p -blocks of p -solvable groups, Osaka J. Math., 17 (1980), 801-806.
- [11] Y. Usami: On p -blocks with abelian defect groups and inertial index 2 or 3, I, J. Alg. 119 (1988), 123-146.
- [12] A. Watanabe: Note on a p -block of a finite group with abelian defect group II, to appear in Osaka J. Math. 28 (1991).