

第 21 回代数的組合せ論シンポジウム 報告集

2004 年 6 月 28 日 ~ 30 日
於 信州大学 理学部大会議室

平成 16 年度文部科学省科学研究費基盤研究 (B)(1)
課題番号 16340010 研究代表者 坂内英一

まえがき

この報告集は 2004 年 6 月 28 日から 6 月 30 日にわたり、信州大学理学部大会議室で行われた「第 21 回代数的組合せ論シンポジウム」の講演記録です。講演は 19 名の講演者によって行われ、約 80 名の参加者があり盛会でした。

この報告集の作成、および数名の講演者の旅費は

平成 16 年度文部科学省科学研究費基盤研究 (B)(1)

研究代表者 坂内英一教授 (課題番号 16340010)

より援助を受けています。また参加者への会場である松本周辺の案内などについては松本コンベンションビューローに協力して頂きました。講演者の方々、参加者の方々、また会場準備などを手伝ってくれた信州大学の学生達、この研究集会に関係するすべての方々にお礼を申し上げます。

2004 年 10 月
信州大学理学部
花本章秀

第 21 回代数的組合せ論シンポジウム

日時：平成 16 年 6 月 28 日 (月) ~ 30 日 (水)

場所：信州大学 (松本キャンパス) 理学部大会議室

世話人：花木章秀 (信州大学理学部, e-mail : hanaki@math.shinshu-u.ac.jp)

6 月 28 日 (月)

10:00-10:30 田辺 顕一郎 (筑波大学数学系)

Zhu 代数の商加群から誘導される頂点作用素代数の加群について

10:40-11:40 宮本 雅彦 (筑波大学数学系)

サッカーボールとサッカーゴールを使つてのゴレイコード、マジュー群構成

11:50-12:20 小竹 悟 (信州大学理学部)

Ruijsenaars 模型の古典平衡点と変形された直交多項式

14:00-14:30 大野 泰生 (近畿大学理工学部)

多重ゼータ値の和公式について

14:40-15:10 平峰 豊 (熊本大学教育学部)

A_5 における相対差集合の分類

15:20-16:00 中川 暢夫 (近畿大学理工学部)

On the 2-dimensinal dual hyper oval in the polar space $PG(5, 4)$ and its automorphism groups

16:10-17:10 吉荒 聡 (東京女子大学文理学部)

極空間中の双対弧 (Dimensional dual arcs of polar type)

6 月 29 日 (火)

09:30-10:30 島田 伊知朗 (北海道大学大学院理学研究科)

符号と超特異 $K3$ 曲面のモジュライ

10:40-11:40 北詰 正頭 (千葉大学理学部)

長さ 72 の extremal doubly-even self-dual code に関係した 5-design について

11:50-12:20 城本 啓介 (愛知県立大学情報科学部)

Bounds for binary matroids

14:00-14:30 細谷 利恵 (国際基督教大学理学科)

A characterization of tight graphs

14:40-15:10 田上 真 (九州大学数理学研究院)

On graph spectra of finite upper half planes over Galois rings

15:20-16:00 谷口 哲至 (九州大学数理学研究院)

On graphs with the smallest eigenvalue at least $-1 - \sqrt{2}$

16:10-16:40 奥山 京 (大分大学工学部)

極小な直和因子をもつ部分群について

18:00-20:00 懇親会

6月30日(水)

- 09:30-10:30 吉田 知行 (北海道大学理学部)
局所有限トポス上の離散数学の構築を目指して—Burnside 環のベキ等元公式
- 10:40-11:10 宮本 泉 (山梨大学工学部)
置換群の可移拡大の組合せ論的計算法
- 11:20-11:50 石川 賢太 (千葉大学理学部)
Finite groups with a small number of conjugacy lengths
- 13:30-14:00 吉田 憲秀 (千葉大学大学院自然科学研究科)
The W -graphs of the Hecke algebra of type E_7
- 14:10-14:40 二宮 晏 (信州大学理学部), 夫馬 道卓 (信州大学大学院工学系研究科)
Commutativity of Hecke algebras associated with p -nilpotent groups and their Sylow p -subgroups

懇親会

日時：平成 16 年 6 月 29 日 (火) 18:00 ~ 20:00

場所：信州大学旭会館 ライジングサン

会費：4000 円 (学生 2000 円)

懇親会出席予定の方は 6 月 18 日 (金) までに花木までお知らせください。

〒390-8621 松本市旭 3-1-1 信州大学理学部 花木章秀

e-mail : hanaki@math.shinshu-u.ac.jp

Tel : 0263-37-2453 (研究室)

1. 田辺 顕一郎 (筑波大学数学系)	1
Zhu 代数の商加群から誘導される頂点作用素代数の加群について	
2. 宮本 雅彦 (筑波大学数学系)	7
マシュー群の中の 2A-involution - サッカーボールと一緒に	
3. 小竹 悟 (信州大学理学部)	16
Ruijsenaars 模型の古典平衡点と変形された直交多項式	
4. 大野 泰生 (近畿大学理工学部), 若林 徳子 (近畿大学総合理工学研究科)	26
Multiple zeta-star values の巡回和公式	
5. 平峰 豊 (熊本大学教育学部)	32
Relative difference sets in $\text{Alt}(5)$	
6. 中川 暢夫 (近畿大学理工学部)	45
On the 2-dimensinal dual hyper oval in the polar space $PG(5, 4)$ and its automorphism groups	
7. 吉荒 聡 (東京女子大学文理学部)	57
極空間中の双対弧 (Dimensional dual arcs of polar type)	
8. 島田 伊知朗 (北海道大学大学院理学研究科)	69
符号と超特異 $K3$ 曲面のモジュライ	
9. 原田 昌晃 (山形大), 北詰 正顕 (千葉大学理学部), 宗政 昭弘 (東北大)	88
長さ 72 の extremal doubly-even self-dual code に関係した 5-design について	
10. 城本 啓介 (愛知県立大学情報科学部)	95
Bounds for binary matroids	
11. 細谷 利恵 (国際基督教大学理学科)	102
A characterization of tight graphs	
12. 田上 真 (九州大学数理学研究院)	109
Galois 環上の有限上半平面に対する固有値について	
13. 谷口 哲至 (九州大学数理学研究院)	120
On graphs with the smallest eigenvalue at least $-1 - \sqrt{2}$	
14. 奥山 京 (大分大学工学部)	135
Minimal direct summands	
15. 吉田 知行 (北海道大学理学部)	140
局所有限トポス上の Burnside 環のベキ等元公式 (The idempotent formula of the Burnside ring of a locally finite topos)	

16. 宮本 泉 (山梨大学工学部) 置換群の可移拡大の組合せ論的計算法	149
17. 石川 賢太 (千葉大学理学部) Finite groups with small number of conjugacy lengths	156
18. 吉田 憲秀 (千葉大学大学院自然科学研究科) The W -graphs of the Hecke algebra of type E_7	162
19. 二宮 晏 (信州大学理学部), 夫馬 道卓 (信州大学大学院工学系研究科) Commutativity of Hecke algebras associated with p -nilpotent groups and their Sylow p -subgroups	169

100

101

102

103

The first part of the document is a list of names and titles, including "The Hon. Mr. Justice" and "The Hon. Mr. Justice". The text is very faint and difficult to read, but it appears to be a list of names and titles, possibly a list of judges or officials.

Zhu 代数の商加群から誘導される 頂点作用素代数の加群について

田辺顕一郎

筑波大学大学院数理物質科学研究科

1 動機と準備

頂点作用素代数に対して Zhu 代数と呼ばれる結合代数が定義される。Zhu 代数の左加群から頂点作用素代数の加群が構成できることが知られている。Zhu 代数自体の商加群から構成される頂点作用素代数の加群の構造に関して結果を得たので報告する。

まず頂点作用素代数の定義を紹介する。

定義 1. $(V, Y, 1, \omega)$ が頂点作用素代数であるとは次が成り立つ時にいう:

- (1) $V = \bigoplus_{n=0}^{\infty} V_n$ は \mathbb{C} 上の次数付きベクトル空間。各斉次空間 V_n は有限次元。 $v \in V_n$ の時、 n を v のウェイトといい wtv で表す。
- (2) z を変数として $Y(\cdot, z)$ は V から $(\text{End}_{\mathbb{C}} V)[[z, z^{-1}]]$ への写像。 $v \in V$ に対して $Y(v, z) = \sum_{n \in \mathbb{Z}} v_n z^{-n-1}$ と表示する ($v_n \in (\text{End}_{\mathbb{C}} V)$)。
- (3) $1 \in V_0$ で $\omega \in V_2$ である。
- (4) 任意の $u, v \in V$ に対して、 $u_n v = 0$ ($n \gg 0$)。
- (5) $Y(1, z) = \text{id}_V$. $a_{-1}1 = a$, $a_n 1 = 0$ ($n \geq 0$)。
- (6) ある c_V が存在してヴィラソロ代数の関係式 $[\omega_{m+1}, \omega_{n+1}] = (m-n)\omega_{m+n+1} + \frac{m^3-m}{12}\delta_{m+n,0}c_V$ が成り立つ。
- (7) $v \in V_n$ に対して $\omega_1 v = nv$ 。
- (8) $v \in V$ に対して $Y(\omega_0 v, z) = \frac{d}{dz} Y(v, z)$ 。
- (9) (Borcherds 恒等式) $u, v \in V$, $l, m, n \in \mathbb{Z}$ に対して

$$\sum_{i=0}^{\infty} \binom{m}{i} (u_{l+i}v)_{m+n-i} = \sum_{i=0}^{\infty} (-1)^i \binom{l}{i} (u_{m+l-i}v_{n+i} + (-1)^{l+1}v_{n+l-i}u_{m+i}).$$

次に頂点作用素代数の加群の定義をする。

定義 2. V を頂点作用素代数とする。 (M, Y) が弱 V 加群であるとは次が成り立つ時にいう:

- (1) z を変数として $Y(\cdot, z)$ は V から $(\text{End}_{\mathbb{C}} M)[[z, z^{-1}]]$ への写像。 $v \in V$ に対して $Y(v, z) = \sum_{n \in \mathbb{Z}} v_n z^{-n-1}$ と表示する。
- (2) 任意の $u \in V, v \in M$ に対して、 $u_n v = 0$ ($n \gg 0$)。
- (3) $Y(1, z) = \text{id}_M$ 。
- (4) (Borcherds 恒等式) $u, v \in V, l, m, n \in \mathbb{Z}$ に対して

$$\sum_{i=0}^{\infty} \binom{m}{i} (u_{l+i} v)_{m+n-i} = \sum_{i=0}^{\infty} (-1)^i \binom{l}{i} (u_{m+l-i} v_{n+i} + (-1)^{l+1} v_{n+l-i} u_{m+i}).$$

$\mathbb{N} := \{0, 1, 2, \dots\}$ とする。

定義 3. V を頂点作用素代数とする。 (M, Y) が弱 V 加群とする。 (M, Y) が \mathbb{N} -graded 弱 V 加群であるとは次が成り立つ時にいう:

- (1) M は整数による次数付け $M = \bigoplus_{n \in \mathbb{Z}} M(n)$ を持つ。
- (2) 任意の斉次元 $u \in V$ と $n, m \in \mathbb{Z}$ に対して $u_m M(n) \subset M(n + wt_u - m - 1)$ となる。
- (3) $M(n) = 0$ ($n \ll 0$)。

$M = \bigoplus_{n \in \mathbb{Z}} M(n)$ が \mathbb{N} -graded 弱 V 加群である時、任意の $a \in \mathbb{Z}$ に対して $M[n] := M(n + a)$ とおいて新しい次数付け $M = \bigoplus_{n \in \mathbb{Z}} M[n]$ を考えても上記の条件は満たされる。したがって今後、零でない \mathbb{N} -graded 弱 V 加群 $M = \bigoplus_{n \in \mathbb{Z}} M(n)$ に対しては $M(0) \neq 0, M(n) = 0$ ($n < 0$) となっているとする。

V を頂点作用素代数、 M を弱 V 加群とする。 $v \in V, i \in \mathbb{Z}$ に対して新しい記号 $o_i(v) := v_{wt_v - 1 - i}$ を定める。 $M = \bigoplus_{n=0}^{\infty} M(n)$ が \mathbb{N} -graded 弱 V 加群である場合には $o_i(v) M(n) \subset M(i+n)$ となっていて添字の動きが見やすい記号である。また $n \in \mathbb{Z}$ に対して $\Omega_n(M) := \{u \in M \mid o_j(u)w = 0, \forall j < -n\}$ とおく。 M が \mathbb{N} -graded である場合には $M = \bigoplus_{i=0}^{\infty} M(i)$ と書いたときに $M(n) \subset \Omega_n(M)$ となっている。

次に Zhu 代数の定義を紹介する。[2] において、頂点作用素代数の色々な例に対して観察されていたモジュラー不変性に統一的な証明が与えられたのであるが、そこで導入された Zhu 代数はその証明に本質的な役割

を果たした。その過程で頂点作用素代数の表現と Zhu 代数の表現とに密接な関係がある事が示された。例えば頂点作用素代数の既約加群は Zhu 代数の既約加群と一対一に対応していることが示された。Zhu 代数はその後 [1] で拡張され類似の関係が得られている。ここでその頂点作用素代数の表現と Zhu 代数の表現との関係の必要なところだけを紹介する。

$(V, Y, 1, \omega)$ を頂点作用素代数とする。斉次元 $u \in V, v \in V, n = 0, 1, \dots$ に対して積

$$u *_n v := \sum_{i=0}^n \binom{-n-1}{i} \operatorname{Res}_z Y(u, z) v \frac{(1+z)^{wt_u+n}}{z^{n+i+1}},$$

$$u \circ_n v := \operatorname{Res}_z Y(u, z) v \frac{(1+z)^{wt_u+n}}{z^{2n+2}}.$$

を定義する。ここで $\operatorname{Res}_z f(z)$ は $f(z)$ を z に関してローラン級数に展開した時の z^{-1} の係数を取る操作を表している。 $O_n(V) = \operatorname{Span}_{\mathbb{C}}\{u \circ_n v, (\omega_1 + \omega_0)u \mid u, v \in V\}$ とおく。また $O_{-1}(V) := V$ とおく。

Zhu と Dong-Li-Mason は次を示した:

事実 1. ([2],[1])

- (1) $O_n(V) \supset O_{n+1}(V)$ ($n = 0, 1, \dots$)
- (2) $O_n(V)$ は $(V, *_n)$ の両側イデアル。
- (3) $A_n(V) := V/O_n(V)$ とおくと、 $(A_n(V), *_n)$ は 1 を単位元を持つ結合代数になる。 $A_n(V)$ を第 n 次 Zhu 代数という。
- (4) 写像 $A_{n+1}(V) \rightarrow A_n(V)$ ($u + O_{n+1}(V) \mapsto u + O_n(V)$) は \mathbb{C} 代数としての準同型写像となる。
- (5) $W = \bigoplus_{n=0}^{\infty} W(n)$ を \mathbb{N} -graded 弱 V 加群とする。

$$\begin{aligned} V \times W(n) &\rightarrow W(n), \quad \forall n \in \mathbb{Z}_{\geq 0} \\ (v, w) &\mapsto o_0(v)w \end{aligned}$$

は $W(n)$ 上に左 $A_n(V)$ 加群の構造を誘導する。

- (6) $N \in \mathbb{Z}_{\geq 0}$ とする。 U を左 $A_N(V)$ 加群で $O_{N-1}(V) \cdot U \neq 0$ となるものとする。この時、 \mathbb{N} -graded 弱 V 加群 $W = \bigoplus_{n=0}^{\infty} W(n)$ で次を満たすものが存在する:

- ・ $W(0) \neq 0$. 左 $A_N(V)$ 加群として $W(N) \simeq U$. 以降 $U = W(N)$ とみなす。
- ・ W は V 加群として U から生成される。

- M を任意の弱 V 加群、 $\phi: U \rightarrow \Omega_N(M)$ を $A_N(V)$ 加群としての任意の準同型とする。この時、次の図式が可換となる V 加群としての準同型写像 $\bar{\phi}: W \rightarrow M$ が一意的に存在する:

$$\begin{array}{ccc} W & \xrightarrow{\exists! \bar{\phi}} & M \\ \uparrow & & \uparrow \\ U & \xrightarrow{\phi} & \Omega_N(M) \end{array}$$

W を U から誘導された V 加群という。 U_1, U_2 を左 $A_N(V)$ 加群とする。上記の普遍性は $A_N(V)$ 加群としての任意の準同型写像 $\psi: U_1 \rightarrow U_2$ に対して、 U_i から誘導された V 加群 W_i ($i = 1, 2$) 上の V 加群としての準同型写像 $\bar{\psi}: W_1 \rightarrow W_2$ で $\bar{\psi}|_{U_1} = \psi$ となるものを一意的に誘導する。

最後に出てきた誘導加群の構成をみていく。 t を変数とするローラン多項式環 $\mathbb{C}[t, t^{-1}]$ と V とのテンソル積 $\mathbb{C}[t, t^{-1}] \otimes V$ を考える。 $D := \frac{d}{dt} \otimes 1 + 1 \otimes \omega_0$ として商空間 $\hat{V} := \mathbb{C}[t, t^{-1}] \otimes V / D(\mathbb{C}[t, t^{-1}] \otimes V)$ を考える。 $t^m \otimes v$ ($v \in V, m \in \mathbb{Z}$) を $v(m)$ で表す事にする。また v が斉次元の時 $v(m)$ のウェイトを $\text{wt}v - m - 1$ と定義して $\text{wt}(v(m))$ で表す事にする。 $\hat{V}(m) := \{x \in \hat{V} \mid \text{wt}x = m\}$ とおくと、 $\hat{V} = \bigoplus_{m \in \mathbb{Z}} \hat{V}(m)$ となる。 $u(m), v(n) \in \hat{V}$ に対して

$$[u(m), v(n)] := \sum_{i=0}^{\infty} \binom{m}{i} (u_i v)(m+n-i).$$

とおくと、 $(\hat{V}, [\cdot, \cdot])$ は \mathbb{Z} -graded Lie 環となる。 $\hat{V}(0)$ は \hat{V} の部分リー環となる。また任意の $n \in \mathbb{N}$ に対して $P_n := \bigoplus_{p > n} \hat{V}(-p) \oplus \hat{V}(0)$ は \hat{V} の部分リー環となる。 \hat{V} の包絡環を $U(\hat{V})$, P_n の包絡環を $U(P_n)$ と表す。

U を左 $A_N(V)$ 加群とする。 U を写像 $\hat{V}(0) \rightarrow A_N(V)$ ($v \mapsto v(\text{wt}v - 1)$) を用いて $\hat{V}(0)$ 加群とみなす。さらに $\hat{V}(-p)$ ($p > N$) の U への作用を 0 と定めることによって U を P_N 加群とみなす。 \hat{V} 加群 $U(\hat{V}) \otimes_{U(P_N)} U$ を \hat{V} の作用が Borchers 恒等式を満たすように最小のイデアル I で割った空間 $U(\hat{V}) \otimes_{U(P_N)} U/I$ が誘導加群 W である。

W が U から生成される N -graded V 加群になっていることを見るのは簡単であるが、 $W = \bigoplus_{n=0}^{\infty} W(n)$ と表した時、 $W(0) \neq 0$ と $A_N(V)$ 加群として $U \simeq W(N)$ を示す為には面倒な計算が必要である。

事実 1. から各 $W(n)$ は $A_n(V)$ 加群となっていて U から一意的に決まっている。 $W(n)$ が U の影響をどのように受けた $A_n(V)$ 加群となっているかを調べる事は頂点作用素代数の表現を研究する上で重要であると思われる。しかし、それは誘導加群の構成からは分かりづらい。 $A_n(V)$ 加群としての $W(n)$ の構造を捉える事が研究の動機である。

$N = 0$ で U が $A_0(V)$ 自身の商加群の場合にはその誘導加群 $W = \bigoplus_{n=0}^{\infty} W(n)$ に対して $W(n)$ の $A_n(V)$ 加群としての情報を得る事が出来た事を次で記す。

2 結果

$N = 0$ の時、 U が $A_0(V)$ 自身の商加群の場合に対してその誘導加群 $W = \bigoplus_{n=0}^{\infty} W(n)$ を考える。 $A_0(V) = V/O_0(V)$ であったから適当な $(V, *_0)$ の左イデアル $I \supset O_0(V)$ が存在して $U = V/I$ と書ける。各 $n \in \mathbb{N}$ に対して $O_{0,n}(V, I)$ を次の元達で張られる V の部分空間とする：

$$\begin{aligned} & \cdot \operatorname{Res}_z Y(u, z) v \frac{(1+z)^{wtu}}{z^{n+1}}, \quad u \in V, v \in I, \\ & \cdot (\omega_1 + \omega_0 - n)u, \quad u \in V. \end{aligned}$$

定理 1. $n \in \mathbb{N}$ とする。

- (1) $O_{0,n}(V, I)$ は $(V, *_n)$ の左イデアルである。さらに $V \times V/O_{0,n}(V, I) \rightarrow V/O_{0,n}(V, I)$ は $V/O_{0,n}(V, I)$ 上に左 $A_n(V)$ 加群としての構造を誘導する。
- (2) $W = \bigoplus_{n=0}^{\infty} W(n)$ を $U = V/I$ から誘導された V 加群とする。

$$\begin{aligned} V/O_{0,n}(V, I) & \rightarrow W(n). \\ v & \mapsto o_n(v)[1]. \quad [1] \in W(0) = U = V/I. \end{aligned}$$

は $A_n(V)$ 加群としての全射準同型となる。

(2) において $O_{0,n}(V, I)$ が Kernel に入っている事は直ぐにわかる。(1),(2) とも条件を地道な計算で確認するだけなので証明は省略する。

また研究集会後、(2) の Kernel を完全に決定する事が出来た。それを用いて U が $A_0(V)$ 自身の商加群の場合に、Zhu 代数の加群達の直和を取る事による誘導加群の別構成が得られた。

参考文献

- [1] C. Dong, H. Li, and G. Mason, Vertex operator algebras and associative algebras, *J. Algebra* **206** (1998), 67–96.
- [2] Y. Zhu, Modular invariance of characters of vertex operator algebras, *J. Amer. Math. Soc.* **9** (1996), 237–302.

マッシュー群の中の 2A-involutions

サッカーボールと一緒に

宮本雅彦

筑波大学 数理物質科学研究科数学専攻

1 序文

興味の対象はモンスター単純群 M とそれを自己同型群としてもつランク 24 のムーンシャイン頂点作用素代数 V^{\natural} です。特に、ランク 1/2 の頂点作用素部分代数 (Ising model) によって定義される M の位数 2 の元 (2A-inv.) は興味ある性質 (e.g. 6-transposition i.e. $|gh| \leq 6 \quad \forall g, h \in 2A$ 、や拡大 E_8 -Dynkin diagram に対する McKay's observation など) を示しており、頂点作用素代数の立場からの解析を行いたいと思っています。特に、モンスター単純群を生成している 21 個の invs. との関係を調べる事は大きな目標の一つです。単独の 2A-inv. や可換な 2 つの 2A-invs. に対してはこれまでの研究で、ほぼ満足のいく結果を得ており、頂点作用素代数による説明が元の性質を明快に表しています。しかし、非可換な 2 つの 2A-invs. の関係を説明する頂点作用素代数の関係は未だはっきりせず、新しい考察を必要としているが、ムーンシャイン頂点作用素代数の構造自体はモンスター単純群以上に分からない点が多い。最終目標である 21 個の invs. をすべて調べるためには当然 ムーンシャイン頂点作用素代数 V^{\natural} 自体を扱わなければなりません、数個の 2A-invs. だけを考えるのであれば、 M や V^{\natural} をすべて扱う必要はないというのが、この研究の動機です。

モンスター単純群の中で 2 つの 2A-invs. の積は 9 種類あり、

$$1A, 2A, 3A, 4A, 5A, 6A, 4B, 2B, 3C$$

となっています。これらの共役類の位数全体の集合は拡大 E_8 -Dynkin diagram における isotropic 元を表す基本ルートの重複度と一致しています。(McKay's E_8 -observation)

これらの関係は、モンスター単純群のような大きな群を見なくても、マッシュー群 M_{24} の内部において、上の 9 種類をすべて観察出来ることが群論の知識から分かります。実際には、より小さい部分群である $2^4 A_8$ においても観察できます。それゆえ、頂点作用素代数の立場からみてわかり易い方法でマッシュー群の中の部分群を観察してみようというのが本講演の趣旨であり、そのためにサッカーボールを使おうというわけです。

(I-1) 理由

(1) サッカーボールの自己同型群は交代群 A_5 ですが、同型 $A_5 \cong SL(2, 4)$ により、 \mathbb{F}_4^2 (加法群として \mathbb{F}_2^4 と同型) への作用が分かります。それを使って、同型 $GL(4, 2) \cong A_8$ のことが良く分かります。

(2) A_8 の作用する 8 点と、 $GL(4, 2)$ が作用する \mathbb{F}_2^4 の 16 ベクトルを合わせた 24 点集合の上に、群の同型 $GL(4, 2) \cong A_8$ からゴーレイコードなどが構成できます。それゆえ、サッカーボールを使ってゴーレイコードの元をすべて記述することが出来、その自己同型群 (マシュー群 M_{24}) の一部が良く分かります。

ゴーレイコードとは

長さ 24 の self-dual code で minimal weight は 8。このような線形コードは同型を除いて一意的に存在する。minimal weight 8 であるコードワード (8 点集合) (octad と呼ぶ) 全体は (5, 8, 24) スタイナーシステムをなす。即ち、任意の 5 点集合を含む 8 点集合 (octad) は一意的に決まる。

2 A toy version of V^h

位数 2 の自己同型 2A-inv. は Ising model によって与えられますが、2 つの Ising model の関係は良くわかっていません。しかし、これらを格子の自己同型として考えることには次の 2 つの利点があります。

(2.a) 格子頂点作用素代数の構造がわかり易い。

(2.b) semi self-dual である $\sqrt{2}E_8$ -格子によって与えられる高次元鏡映は 2A-inv. と同じ性質を示します。即ち、もし整数格子 $L \supseteq H \cong \sqrt{2}E_8$ なら、

$$-1 \text{ on } \mathbb{Q}H, \quad 1 \text{ on } \mathbb{Q}H^\perp$$

は L の自己同型 ([Griess]) となっており、2A-inv. です。

実際、コンウェイ群の中の 2A-inv. はこの高次元鏡映で与えられるものであり、モンスター単純群の中に出て来る 9 種類の積はすべて現れます。

(2) 今回は、より小さく置換の範囲 (マシュー群 M_{24} の部分群 2^4A_8) で考察し、9 種類の 2A-inv. の組に対して $\sqrt{2}E_8$ -格子の組を構成します。

マシュー群 M_{24} の invs (位数 2 の元) の共役類はモンスター単純群と同様に、2 種類しかありません。24 点上の置換と考えると、

$$\left\{ \begin{array}{l} 2A\text{-inv. : タイプ } 1^8 2^8 \text{ (互換 8 つの積) の巡回型、と} \\ 2B\text{-inv. : タイプ } 2^{12} \text{ (互換 12 個の積) で、固定点を持たないもの} \end{array} \right.$$

となっています。

2A-inv. τ の固定点は 8 点であり、後で示すように Golay code の octad となっています。格子の自己同型としては、 τ を 8 個の互換 $\tau = (x_9, x_{17})(x_{10}, x_{18}) \cdots (x_{16}, x_{24})$ で表すと、

$$\langle v_1 = x_9 - x_{17}, \quad v_2 = x_{10} - x_{18}, \quad \cdots \quad v_8 = x_{16} - x_{24} \rangle$$

上で -1 倍として作用しています。すなわち、この中に τ を定義する semi self-dual 部分格子 $\sqrt{2}E_8$ が含まれているわけです。この $\sqrt{2}E_8$ 格子は後で示すように、16 点が \mathbb{F}_2^4 構造を持つことを使って構成できます。

3 サッカーボールと 4 次元ベクトル空間

(II-1) サッカーボール、正 20 面体や正 12 面体の自己同型群は交代群 A_5 です。この自己同型群の動きを見るために、20 面(サッカーボールの正六角形)に $\{1, 2, 3, 4, 5\}$ の順序付き組 (i, j) ($i \neq j$) を次のように対応させます。

- (a) (i, j) 面と (s, t) 面が隣接しているなら、 $\{i, j, s, t\}$ は異なる 4 文字となっており、
 - (b) 各正五角形での回転は A_5 の中の位数 5 の置換に対応しています。
- すなわち、一つの正五角形に隣接している 5 つの正六角形が順に、 $(i_1, j_1), (i_2, j_2), (i_3, j_3), (i_4, j_4), (i_5, j_5)$ なら、置換として、位数 5 の巡回置換 $(i_1, i_2, i_3, i_4, i_5)$ と $(j_1, j_2, j_3, j_4, j_5)$ は同じものというわけです。

注意することは、このような割り当ては、2 通りあります。実際、 $(1, 2), (3, 4)$ を隣接 2 面とすると、この 2 面が共有する辺の頂点に付属する 2 つの正五角形での回転は、すでに $1 \rightarrow 3, 2 \rightarrow 4$ が決められているので、可能性は 2 通り

$$1 \rightarrow 3 \rightarrow 2 \rightarrow 4 \rightarrow 5 \rightarrow 1, \quad 1 \rightarrow 3 \rightarrow 5 \rightarrow 2 \rightarrow 4 \rightarrow 1$$

だけになります。これらを $(1, 2)$ 面、 $(3, 4)$ 面の両方に隣接している正五角形のどちらかに割り付けるかで、2 通り出て来ます。それ以降は、自動的に番号付けが決まります。

サッカーボールを利用する理由は、群論的に面白い同型

$$A_5 \cong PSL(2, 5) \cong PGL(2, 4) \cong SL(2, 4)$$

が、正 20 面体および正 12 面体 (それゆえサッカーボール) によって表示できるからです。

(II-2) \mathbb{Z}_2^4 との関係 $SL(2, 4) \cong A_5$

辺に注目しましょう。辺は全部で 30 個あり、向かい合った辺を同一視し、これを対辺と呼ぶことにします。すると 15 対辺があり、 A_5 はこの 15 対辺に可移に作用しています。1 点の固定部分群の位数は $60/15 = 4$ なので、固定部分群はシロー 2 部分群。一方、 $SL(2, 4)$ は $\mathbb{F}_4^2 - \{(0, 0)\}$ に可移に作用しており、その 1 点固定部分群もシロー 2 部分群です。それゆえ、 $A_5 \cong SL(2, 4)$ より、上の 2 つの置換は同一のものと考えることが出来ます。

この事実より、15 対辺に parity check 用の形式的な 0 対辺を加えた 16 対辺には \mathbb{F}_2 上 4 次元ベクトル空間の構造が入ることが分かります。すなわち、この 16 対辺に次のように加法が定義できます。

加法: 加法は位数3の自己同型 (正3角形) で与えます。即ち、異なるベクトル (対辺) v, u に対して $\sigma(v) = u$ となる位数3の自己同型 σ を持ってきて、

$$v + u = \sigma(u) \quad v + v = 0$$

と定義します。

(II-3) 部分空間

正20面体 (サッカーボール) は \mathbb{F}_2^4 を上手く表していることを紹介しましょう。

例えば、3次元部分空間は次のようになります。

3次元空間は15個あり、その平行移動した超空間も15個あります。一つの対辺 $-$ に隣接する対辺は8本あります。すなわち、 $X-X$ の形を作る8対辺ですが、この8対辺が超平面を形成します。各対辺に対して、この隣接8対辺が決まりますので、これで15個の超空間が表示できました。その8対辺の補集合が3次元空間に対応しています。

また、2次元の部分空間 (のゼロ以外の3辺) は上で定義した加法によって与えられたり、上の超空間の共通部分として与えられます。サッカーボールの自己同型群は交代群 A_5 で、作用する空間を $\mathbb{F}_4 \oplus \mathbb{F}_4$ と見ることができるので、形状として4種類

{ 正3角形, 互いに直交した3辺, 正3角形から伸びる放射状3辺, 蛇型の3辺 }

に分かれます。

このように、4次元空間の中の3次元部分空間、2次元部分空間は正12面体 (正20面体、サッカーボール) を使って完全に表示することができるので、それらから定義される Reed Muller codes も表示できます。

(II-4) Reed Muller code $RM(r, 4)$ ($r = 1, 2$)

\mathbb{Z}_2^4 の16 vectors を座標とみて、次のようなコードを定義します。

Reed Muller code $RM(1, 4)$ とは、 \mathbb{Z}_2^4 中の3次元空間 (15個) と超平面全体 (15個)、およびゼロと全体の合計32個のコードワードからなるコードです。これは5次元部分空間をなしています。

また、2次元ベクトル空間とその平行移動したものの全体から生成される線形コードを $RM(2, 4)$ で表します。

$RM(2, 4) = RM(1, 4)^\perp$ となっており、これは11次元コードです。

4 自己同型群 A_8

各面 (サッカーボールの正六角形) に $\{1, 2, \dots, 5\}$ の順序付き組 (a, b) が対応しているので、各辺に対しては、 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ の形の行列が対応しています。

同値ルール 置換 $\{(1), (ab)(cd), (ac)(bd), (ad)(bc)\}$ に対しては不変とする。即ち、

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix} \text{ とする.}$$

加法の定義

(1) 2つの元に出てくる数字の種類が4点の場合

同値ルールを利用して、左上の成分が同一としてよい。このとき、加法は

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 3 \\ 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}$$

のようになります。これにより定義される octad は加法に出てくる3点、およびゼロ（合わせて2次元部分空間）と表示に出てきている4数字を合わせた8点集合です。

$$\left\{ \begin{pmatrix} 00 \\ 00 \end{pmatrix}, \begin{pmatrix} 12 \\ 34 \end{pmatrix}, \begin{pmatrix} 13 \\ 42 \end{pmatrix}, \begin{pmatrix} 14 \\ 23 \end{pmatrix} \right\} \cup \{1234\}$$

(2) 次に、2つの元に $\{1, 2, 3, 4, 5\}$ のすべてが出てくる場合

同値ルールを使うと、Horizontal「水平」、Vertical「垂直」、X-crossing（対角、逆対角）のどれかは一貫します。たとえば、下の例のように、水平が一貫したとします。このとき、加法は、残りの水平部分で位数3の巡回を起こして定義します。

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix}$$

定義される octad はこの加法で定義される2次元部分空間と、一致した $\{H, V, X\}$ の一つ、それに位数3で巡回した3数字の8点です。

$$\left\{ \begin{pmatrix} 00 \\ 00 \end{pmatrix}, \begin{pmatrix} 12 \\ 34 \end{pmatrix}, \begin{pmatrix} 12 \\ 45 \end{pmatrix}, \begin{pmatrix} 12 \\ 53 \end{pmatrix} \right\} \cup \{H345\}$$

4.1 $2^4 A_8$ の24点集合への置換を目で見るために

マシュー群 M_{24} 全体の動きを見る方法としては、通常 MOG による表示がよく使われます。しかし、今回の我々の目的の為には、 M_{24} 全体は必要ありません。特に、 $2^4 A_8$ の動きだけを見るなら、サッカーボールから作った16対辺と8点を加えた次のような見方が簡単です。

Partition (MOG の配置にあわせた)

1	2	$\begin{pmatrix} 00 \\ 00 \end{pmatrix}$	$\begin{pmatrix} 13 \\ 42 \end{pmatrix}$	$\begin{pmatrix} 12 \\ 53 \end{pmatrix}$	$\begin{pmatrix} 25 \\ 34 \end{pmatrix}$
3	4	$\begin{pmatrix} 12 \\ 34 \end{pmatrix}$	$\begin{pmatrix} 41 \\ 32 \end{pmatrix}$	$\begin{pmatrix} 12 \\ 45 \end{pmatrix}$	$\begin{pmatrix} 51 \\ 34 \end{pmatrix}$
X	5	$\begin{pmatrix} 14 \\ 35 \end{pmatrix}$	$\begin{pmatrix} 54 \\ 32 \end{pmatrix}$	$\begin{pmatrix} 42 \\ 35 \end{pmatrix}$	$\begin{pmatrix} 51 \\ 42 \end{pmatrix}$
H	V	$\begin{pmatrix} 15 \\ 32 \end{pmatrix}$	$\begin{pmatrix} 14 \\ 52 \end{pmatrix}$	$\begin{pmatrix} 13 \\ 25 \end{pmatrix}$	$\begin{pmatrix} 45 \\ 31 \end{pmatrix}$

作用（置換）の規則: S_8 の置換作用は次のように与えられます。

(1) S_5 の作用は、 $\{1, 2, 3, 4, 5\}$ に対する作用としてすべての部分に作用します。

(2) S_8 中の A_5 と可換な S_3 の動きは、 $\{H, V, X\}$ に対して与えられ、それぞれ配置を換えます。

例えば、互換 (V, X) は垂直と対角を交換し、水平がそのままであるような配置の置換です。

すなわち、 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} a & b \\ d & c \end{pmatrix}$ に移します。

(3) 次に、 $\{1, 2, 3, 4, 5\}$ と $\{H, V, X\}$ の間の置換を互換を使って説明します。互換 $(1, H)$ の作用は、

(3.1) 1 が存在する場合、例えば、 $\begin{pmatrix} 1 & a \\ b & c \end{pmatrix}$ のとき、 d として表示に出て来ていない $\{1, 2, 3, 4, 5\}$ の残りの数字とします。作用は、1 と H (水平) の関係にある a を d に交換し、のこりの b, c は不変のままです。 $\begin{pmatrix} 1 & a \\ b & c \end{pmatrix} \rightarrow \begin{pmatrix} 1 & d \\ b & c \end{pmatrix}$

(3.2) 1 が表示に出て来ていない場合、 H (水平)を保ち、 $\{V, X\}$ を交換します。すなわち、 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} a & b \\ d & c \end{pmatrix}$ となります。

5 ゴーレイコード（蛇足）

次に、群の同型 $A_8 \cong GL(4, 2)$ と Reed Muller code を使って、ゴーレイコード G_{24} が記述できることを紹介します。

16対辺の集合 S に8点集合 $C = \{H, V, X, 1, 2, 3, 4, 5\}$ を加えて24点集合

$$\Omega = C \cup S$$

を考えます。 $\alpha \subseteq \Omega$ を $\alpha_l \subseteq C$, と $\alpha_r \subseteq S$ を使って

$$\alpha = \alpha_l \cup \alpha_r$$

と表示します。

構成には必要ありませんが、群論としての事実を一応説明しておきましょう。 S 中の2次元ベクトル空間(35個)と8点集合 C の4点ずつへの分割(35通り)の間に1対1の関係があることを説明しましょう。8点集合の4点ずつへの分割に対して、その4点ずつの分割を不変にする位数2の偶置換達は A_8 の位数16の可換2群を作り、これに対応する $GL(4, 2)$ の部分群はある2次元部分空間を固定する可換2群です。この対応を使って、2次元部分空間 α_r と4点ずつへの分割の4点 α_l をあわせたもの $\{\alpha_l \cup \alpha_r \mid \alpha_r \text{ 2次元部分空間}\}$ を考えます。さらに、 $\{0 \cup \alpha_r \mid \alpha_r \in RM(1, 4)\}$ を加え、これら全体によって張られる空間を G_{24} とおきます。構成から容易に、 G_{24} の次元は、 $\dim RM(2, 4) + 1 = 12$ であり、 G_{24} が自己直交コードであることが分かります。

この G_{24} がゴーレイコードです。 S への射影 $G_{24} \ni \alpha_l \cup \alpha_r \rightarrow \alpha_r \in S$ の核は $\langle C \rangle$ だけであり、 G_{24} の最小ウエイトが 8 であることも容易に分かります。

このゴーレイコードの元をすべてサッカーボールを使って表してみましょう。必要ありませんが、16点集合の中の $RM(1,4)$, すなわち、超平面 (3次元平面) に対応するものはすべて G_{24} の元で、これは、 $\alpha_l = 0$ となる G_{24} の元全体と一致することを考えると、見やすくなるかもしれません。

サッカーボールによるゴーレイコードワード α の表示の仕方

- (a) $C + \alpha$, α のどちらかを構成すればよいので、 $H \notin \alpha$ となるものを構成します。
- (b) X は parity check 用で α_l は常に偶集合とします。

これからも目標は、 S の $RM(2,4)$ の各元に対して、 C の (H を含まない) 偶部分集合を決めるわけです。

では、16対辺から適当に幾つか選び、それを \mathcal{P} で表すことにします。

0対辺 (parity check) を使って、 \mathcal{P} は偶数個とします。

(c) \mathcal{P} が $RM(2,4)$ の元であることの確認

ボールの正五角形に、隣接する \mathcal{P} の辺の数を偶奇で記入します。

(c1) $\mathcal{P} = \alpha_r$ となる $\alpha \in G_{24}$ が存在する必要十分条件 (i.e. $\mathcal{P} \in RM(2,4)$) はすべての頂点 (6対) での値が等しいことです。

(d) α_l の決定

適当な正五角形とその周りの5つの正六角形をとり、

番号は自分の内部に隣接する番号以外を割り当てます。

$$(d2) \left\{ \begin{array}{l} \text{放射5線 (+ 偶奇)} \Rightarrow \alpha_l \text{ 中の } V \text{ の存在を意味する} \\ \text{5辺台形 (+ 偶奇)} \Rightarrow \alpha_l \text{ 中の } 1, 2, 3, 4, 5 \text{ の存在を意味する} \\ X \text{ は parity check として利用し、} \alpha_l \text{ が偶集合となるようにする。} \end{array} \right.$$

これにより、 α_l が決まります。この時、 $\alpha_l \cup \alpha_r \in G_{24}$ であり、これで G_{24} の $H \notin \alpha$ となるコードワードすべてを表示出来ます。

容易に、次のことが分かります。

(i) α_r が4点なら、 α_l も4点集合であり、 $\alpha_l + \alpha_r$ と $C + \alpha_l + \alpha_r$ は octads となっています。(この4点ずつへの分割は C を含む sextet 全体と一致しています。)

(ii) α_r が6点なら、 $\alpha_l + \alpha_r$ か $C + \alpha_l + \alpha_r$ のどちらかが octad です。

6点集合 α_r が 0 を含む場合には、4次元空間の基底 $\{x_1, x_2, x_3, x_4\}$ が存在して、 $\alpha_r = \{0, x_1, x_2, x_3, x_4, x_1+x_2+x_3+x_4\}$ となることと同値です。

それ以外としては、

$\alpha_r \in RM(1,4) - \{(0^{16}), (1^{16})\}$ が octad であり、これらに、 C を加えると、すべての octads

の集合になります。

Observation

一つ $2A$ -inv. が固定する octads の個数は 71 (モンスター単純群の位数を割る最大の素数) です。何か関係があるのでしょうか？

6 マッシュー群 M_{24} の中の $2A$ -involutions

マッシュー群の中の $2A$ -inv. は一つの octad C とそれと共通部分を持たない 3 つの octads C_1, C_2, C_3 で $|C_i \cap C_j| = 4$ ($i \neq j$), $|C_1 \cap C_2 \cap C_3| = 2$ を満たすものによって定義されています。すなわち、 C_1, C_2, C_3 によって、16 点集合 $\Omega - C$ が 8 つの 2 個ずつの組 $\{i_1, j_1\}, \dots, \{i_8, j_8\}$ に分割され、互換の積 $\tau = (i_1, j_1) \cdots (i_8, j_8)$ が $2A$ -inv. を与えらわけてす。

この位数 2 の自己同型 τ を $\sqrt{2}E_8$ 部分格子による自己同型として理解するためには、 $2A$ -自己同型 τ に対して、2 つの octads $C_1 = \{x_9, \dots, x_{16}\}, C_2 = \{x_{17}, \dots, x_{24}\}$ で τ が 8 個の互換の積 $(x_9, x_{17})(x_{10}, x_{18}) \cdots (x_{16}, x_{24})$ となるようなものを見つける必要があります。そうすれば、 C_1, C_2 と共通部分を持つ各 octad $D = \{x_9, x_{10}, x_{11}, x_{12}, x_{17}, x_{18}, x_{19}, x_{20}\}$ に対して、

$$y_D = \frac{x_9 + x_{10} + x_{11} + x_{12} - x_{17} - x_{18} - x_{19} - x_{20}}{2}$$

と定義し、そのような y_D 全体が張る格子を考えると、 $\sqrt{2}E_8$ と同型な部分格子となっています。この時、 τ はその上に -1 倍として作用しています。

次に、モンスター単純群の $2A$ -involutions の 2 つの積として現れる 9 種類のタイプはすべて M_{24} の中で実現でき、特に (2^4A_8) の中で可能です。これを紹介しましょう。

まず、事実として、 A_8 の中の inv. はすべて $\begin{pmatrix} 00 \\ 00 \end{pmatrix}$ を固定するので、両方とも M_{24} の中で $2A$ -invs. です。

即ち、 A_8 に制限してみると 2 種類の位数 2 のタイプ $\{(12)(34)(X5)(HV), (12)(34)\}$ があるのですが、両方とも $2A$ -inv. となっているということです。それゆえ、この 2 種類のタイプのどちらかによって invert される元を探してみると、

- (2A) $(12)(34), (12)(5X)$ の積は $(34)(5X)$ であり、 $2A$ -inv となっています。
- (3A) (123) は $(13)(24)$ で invert されます。これは $3A$ -triality です。
 $(123)(XHV)$ 型の元も同じ共役類となっています。(固定点を持つ)
- (5A) (12345) も $(15)(24)$ によって invert されています。これは $5A$ -元です。
- (4B) $(1234)(5X)$ は $(23)(HV)$ で invert されています。これは $4B$ -元です。
- (4A,2B) $(1234)(5XHV)(+ \binom{13}{42})$ とその2乗は $(14)(23)(5V)(XH)$ で invert されています。それぞれ、 $4A$ と $2B$ です。
- (6A) $(123)(45)(XV)$ は $(13)(45)$ で invert されており、 $6A$ -元です。
 $(12345X)(HV)$ も同じ $6A$ -元の形になっています。

$3C$ は後半2列の octad を利用して定義しました。すなわち、自己同型 g を 1列 \leftrightarrow 3列, 2列 \leftrightarrow 4列, 5、6列の点はすべて固定で定義し、自己同型 h を加法 $h : + \binom{12}{53}$ で定義されるものとします。この時、積 hg が位数3の自己同型 $\{1, 2列\} \rightarrow \{3, 4列\} \rightarrow \{5, 6列\} \rightarrow \{1, 2列\}$ を与えます。これが $3C$ -元です。

7 最後

最後に正12面体の面を2つにわけ、24面を作って、ゴーレイコードを構成する方法が次の Web site に載っています。

Decoding the Golay code by hand

Joe Fields (University of Illinois at Chicago)

これも非常に面白い方法で、正12面体の incident matrix A を使って、

$$(I_{12}, F + A)$$

と書くと、これがゴーレイコードの生成行列になっているわけです。(ここで、 F は成分がすべて1である行列を表しています。)

配置さえ決めると、ゴーレイコードは左側だけで一意的に決まるので、解読は簡単です。しかし、群の作用を考えると、 A_5 以外の作用は見えません。

Ruijsenaars 模型の古典平衡点と変形された直交多項式

信州大学理学部 小竹 悟

1 序論

(y_1, \dots, y_r) に対する連立方程式

$$\sum_{\substack{k=1 \\ k \neq j}}^r \frac{1}{y_j - y_k} = y_j, \quad (j = 1, \dots, r) \quad (1.1)$$

の解を御存じであろうか。この問題は 19 世紀に Stieltjes によって既に調べられており、その答えは Hermite の多項式 $H_r(x)$ の r 個の零点で与えられる。それではこの方程式を (1 パラメータ) 変形した次の方程式 (パラメータ $\delta \rightarrow 0$ の極限で上の方程式に帰着する)

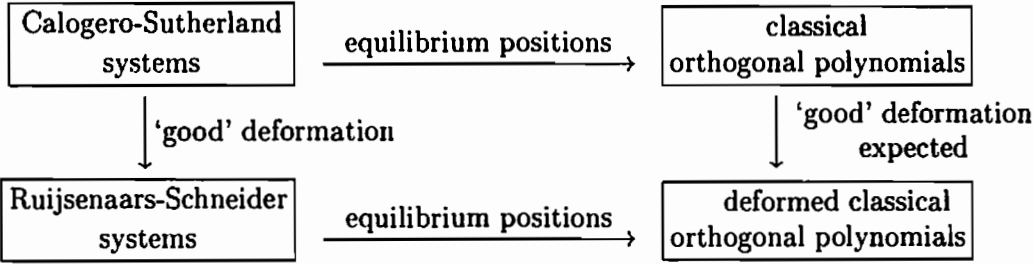
$$\prod_{\substack{k=1 \\ k \neq j}}^r \frac{y_j - y_k - i\sqrt{\delta}}{y_j - y_k + i\sqrt{\delta}} = \frac{1 - i\sqrt{\delta} y_j}{1 + i\sqrt{\delta} y_j}, \quad (j = 1, \dots, r) \quad (1.2)$$

の解はどうなるであろうか。(1.1) の解が Hermite 多項式の零点であり、(1.2) が (1.1) の変形である事から、(1.2) の解は '変形された Hermite 多項式' の零点で与えられると考えるのは自然である。そして (1.1) \rightarrow (1.2) が '良い変形' であるならば、この変形された Hermite 多項式は '性質良く変形されている' と期待できる。何故物理屋の私がこの様な方程式を考えてみるかと言うと、(1.1), (1.2) はそれぞれ Calogero-Sutherland-Moser 模型, Ruijsenaars-Schneider 模型と呼ばれる力学系の古典平衡点の式だからである。

Calogero-Sutherland-Moser 模型とは、長距離相互作用 (ポテンシャルは $\frac{1}{r^2}, \frac{1}{\sin^2 r}, \rho(r)$ など、近距離では $\frac{1}{r}$) を持つ、1 次元 (量子) 可積分多体系である。この Calogero-Sutherland-Moser 模型はルート系に付随する模型で、ハミルトニアンはルート系の Coxeter 群の作用の下で不変になっている。Ruijsenaars-Schneider 模型とは、この Calogero-Sutherland-Moser 模型の '変形版' ('相対論版', '離散化版') である。ハミルトニアンの運動項は p_j^2 の代わりに $\sim \cosh p_j$ となっている。あるパラメータを特別な値に近づけると (例えば '光速' を無限大にすると), Ruijsenaars-Schneider 模型は Calogero-Sutherland-Moser 模型に帰着する。これらの模型と (数理) 物理学との関係は、例えば、分数排他統計、量子 Hall 効果との関連などの元々の物性理論との関係の他に、超対称ゲージ理論の厳密解を与える Seiberg-Witten 理論との関連、2 次元共形場理論で重要な役割を果たす (変形) Virasoro 代数や (変形) W_N 代数との関連など、多岐にわたっており、古典論・量子論共に大変興味深い模型となっている。

本講演では、古典ルート系 (A, B, C, D, BC) に付随する、有理関数または三角関数のポテンシャルを持つ、Ruijsenaars-Schneider 模型の古典平衡点についての研究結果を報告す

る。古典ルート系に付随する Calogero 模型 (有理関数ポテンシャル)・Sutherland 模型 (三角関数ポテンシャル) の古典平衡点は, Hermite, Laguerre, Chebyshev, Legendre, Gegenbauer, Jacobi の多項式の零点になっている。Calogero-Sutherland 模型・Ruijsenaars-Schneider 模型と (変形)Virasoro 代数・(変形) W_N 代数との関係を見出した時の経験などから, Ruijsenaars-Schneider 模型は Calogero-Sutherland 模型の '良い' 変形になっている事を知っているので, Ruijsenaars-Schneider 模型の古典平衡点は Hermite, Laguerre, Jacobi 等の多項式を '性質良く' 変形した多項式の零点になっている事が期待される。



例えば, Hermite, Laguerre, Jacobi 等の多項式は古典直交多項式として知られているが, この直交性という性質は変形後も保持される事が期待され, 実際その様になっている。

紙面の都合で省略した部分も多々あるが, 詳細については文献 [1] を参照して頂きたい。

2 ポテンシャルと平衡点

先ず, 模型の定義と古典平衡点の式を与えておく。

古典ハミルトニアン $H(p, q)$ で定まる古典力学を考える。 $\{q_j | j = 1, \dots, r\}$ は座標で, $\{p_j | j = 1, \dots, r\}$ は共役運動量である。これらを \mathbb{R}^r のベクトル $q = {}^t(q_1, \dots, q_r)$, $p = {}^t(p_1, \dots, p_r)$ として表しておく。 r は粒子数である (A 型を除き, ルート系 Δ のランクでもある)。時間発展を表す正準運動方程式は

$$\dot{q}_j = \frac{\partial H(p, q)}{\partial p_j}, \quad \dot{p}_j = -\frac{\partial H(p, q)}{\partial q_j} \tag{2.1}$$

で, 古典平衡点はその停留解である:

$$p = 0, \quad q = \bar{q}, \quad \text{s.t.} \quad \left. \frac{\partial H(0, q)}{\partial q_j} \right|_{q=\bar{q}} = 0, \quad (j = 1, \dots, r). \tag{2.2}$$

2.1 Calogero 系と Sutherland 系

古典ルート系に付随する Calogero 系, Sutherland 系の古典ハミルトニアンは

$$H_{CS}(p, q) = \frac{1}{2} \sum_{j=1}^r p_j^2 + V_C(q), \quad V_C(q) = \frac{1}{2} \sum_{j=1}^r \left(\frac{\partial W(q)}{\partial q_j} \right)^2 \tag{2.3}$$

という形をしており、古典平衡点の式 (2.2) は

$$\left. \frac{\partial W(q)}{\partial q_j} \right|_{q=\bar{q}} = 0, \quad (j = 1, \dots, r) \quad (2.4)$$

と簡単化される。‘prepotential’ $W(q)$ の具体形は

$$\text{Calogero 系} : W(q) = -\frac{\omega}{2} \sum_{j=1}^r q_j^2 + \sum_{\rho \in \Delta_+} g_\rho \log |(\rho \cdot q)|, \quad (2.5)$$

$$\text{Sutherland 系} : W(q) = \sum_{\rho \in \Delta_+} g_\rho \log |\sin(\rho \cdot q)| \quad (2.6)$$

で、 Δ_+ は正ルートの集合である。結合定数 ω 及び g_ρ は正の実数で、 g_ρ はルートの長さで決まっている： A_{r-1} , D_r の時は全てのルートに対して g ； B_r , C_r の時は long ルートに対しては g_L , short ルートに対しては g_S ； BC_r の時は long ルートに対しては g_L , middle ルートに対しては g_M , short ルートに対しては g_S 。

平衡点の式 (2.4) は

$$\text{Calogero } A_{r-1} : \sum_{\substack{k=1 \\ k \neq j}}^r \frac{1}{\bar{q}_j - \bar{q}_k} = \frac{\omega}{g} \bar{q}_j, \quad (2.7)$$

$$\text{Calogero } C_r : \sum_{\substack{k=1 \\ k \neq j}}^r \frac{2\bar{q}_j}{\bar{q}_j^2 - \bar{q}_k^2} = \frac{\omega}{g_S} \bar{q}_j - \frac{g_L}{g_S} \frac{1}{\bar{q}_j}, \quad (2.8)$$

$$\text{Sutherland } A_{r-1} : \sum_{\substack{k=1 \\ k \neq j}}^r \cot(\bar{q}_j - \bar{q}_k) = 0, \quad (2.9)$$

$$\text{Sutherland } BC_r : \sum_{\substack{k=1 \\ k \neq j}}^r \left(\cot(\bar{q}_j - \bar{q}_k) + \cot(\bar{q}_j + \bar{q}_k) \right) = -\frac{g_S}{g_M} \cot \bar{q}_j - 2 \frac{g_L}{g_M} \cot 2\bar{q}_j \quad (2.10)$$

である。(2.7) の解に対して、 $\bar{q}_j = \sqrt{\frac{2}{\omega}} y_j$ とおくと、 $\{y_j\}$ を零点として持つ多項式は Hermite の多項式 $H_r(x)$ である：

$$2^r \prod_{j=1}^r (x - y_j) = r! \sum_{j=0}^{\lfloor \frac{r}{2} \rfloor} \frac{(-1)^j (2x)^{r-2j}}{j!(r-2j)!} \stackrel{\text{def}}{=} H_r(x). \quad (2.11)$$

(2.8) の解に対して、 $\bar{q}_j = \sqrt{\frac{2}{\omega}} y_j$, $\alpha = \frac{g_L}{g_S} - 1$ とおくと、 $\{y_j^2\}$ を零点として持つ多項式は Laguerre の多項式 $L_r^{(\alpha)}(x)$ である：

$$\frac{(-1)^r}{r!} \prod_{j=1}^r (x - y_j^2) = \sum_{j=0}^r \binom{r+\alpha}{r-j} \frac{(-x)^j}{r!} \stackrel{\text{def}}{=} L_r^{(\alpha)}(x). \quad (2.12)$$

(2.9) の解は並進不変で、重心座標が 0 になるように $\bar{q}_j = \frac{\pi}{2} - \frac{\pi(2j-1)}{2r}$ と選ぶと、 $\{\sin \bar{q}_j\}$ を零点として持つ多項式は第 1 種の Chebyshev の多項式 $T_n(x)$ である：

$$2^{r-1} \prod_{j=1}^r (x - \sin \bar{q}_j) = 2^{r-1} \prod_{j=1}^r \left(x - \cos \frac{\pi(2j-1)}{2r} \right) \stackrel{\text{def}}{=} T_r(x). \quad (2.13)$$

(2.10) の解に対して、 $\alpha = \frac{g_S}{g_M} + \frac{g_L}{g_M} - 1$, $\beta = \frac{g_L}{g_M} - 1$ とおくと、 $\cos 2\bar{q}_j$ を零点として持つ多項式は Jacobi の多項式 $P_r^{(\alpha, \beta)}(x)$ である：

$$2^{-r} \binom{\alpha+\beta+2r}{r} \prod_{j=1}^r (x - \cos 2\bar{q}_j) = \sum_{j=0}^r \binom{\alpha+r}{r-j} \binom{\alpha+\beta+r+j}{j} 2^{-j} (x-1)^j \stackrel{\text{def}}{=} P_r^{(\alpha, \beta)}(x). \quad (2.14)$$

2.2 Ruijsenaars 系

古典ルート系に付随する Ruijsenaars 系の古典ハミルトニアンは

$$H(p, q) = \sum_{j=1}^r \left(\cosh p_j \sqrt{V_j(q) V_j^*(q)} - \frac{1}{2} (V_j(q) + V_j^*(q)) \right) \quad (2.15)$$

で、関数 $V_j = V_j(q)$ とその複素共役 V_j^* の形はルート系 Δ によって決まっている：

$$A_{r-1} : V_j(q) = w(q_j) \prod_{\substack{k=1 \\ k \neq j}}^r v(q_j - q_k), \quad (j = 1, \dots, r), \quad (2.16)$$

$$B_r, C_r, D_r, BC_r : V_j(q) = w(q_j) \prod_{\substack{k=1 \\ k \neq j}}^r v(q_j - q_k) v(q_j + q_k), \quad (j = 1, \dots, r). \quad (2.17)$$

関数 v と w の具体形は下で与える。ハミルトニアンを平衡点の回りで展開して考察する事により、古典平衡点の式 (2.2) が次の様に簡単化される：

$$V_j(\bar{q}) = V_j^*(\bar{q}) > 0, \quad (j = 1, 2, \dots, r). \quad (2.18)$$

2.2.1 Ruijsenaars-Calogero 系

極限で Calogero 系に帰着する模型を Ruijsenaars-Calogero 系と呼ぶ事にする。これには閉じ込めのポテンシャルが 1 次で増大するものと、2 次で増大するものがある。

Linear Confining Potential Case

関数 v と w は

$$A, D : v(x) = 1 - i \frac{g}{x}, \quad w(x) = 1 + i \frac{x}{a}, \quad (2.19)$$

$$B : v(x) = 1 - i \frac{gL}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 - i \frac{gS}{2x}\right)^2, \quad (2.20)$$

$$C : v(x) = 1 - i \frac{gS}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 - i \frac{gL}{x}\right), \quad (2.21)$$

$$\widetilde{BC} : v(x) = 1 - i \frac{g_0}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 - i \frac{g_1}{x}\right) \left(1 - i \frac{g_2}{x}\right) \quad (2.22)$$

で与えられる. 結合定数 $a, g, g_L, g_S, g_0, g_1, g_2$ は正の実数である. 平衡点の式 (2.18) は Bethe 仮設方程式に似た形に書き表される (B, C, D は \widetilde{BC} から得られる):

$$A_{r-1} : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\bar{q}_j - \bar{q}_k - ig}{\bar{q}_j - \bar{q}_k + ig} = \frac{a - i\bar{q}_j}{a + i\bar{q}_j}, \quad (2.23)$$

$$\widetilde{BC}_r : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\bar{q}_j - \bar{q}_k - ig_0}{\bar{q}_j - \bar{q}_k + ig_0} \frac{\bar{q}_j + \bar{q}_k - ig_0}{\bar{q}_j + \bar{q}_k + ig_0} = \frac{a - i\bar{q}_j}{a + i\bar{q}_j} \frac{\bar{q}_j + ig_1}{\bar{q}_j - ig_1} \frac{\bar{q}_j + ig_2}{\bar{q}_j - ig_2}. \quad (2.24)$$

Quadratic Confining Potential Case

関数 v は前と同じだが, 関数 w には一つ因子が掛かって,

$$A, D : v(x) = 1 - i \frac{g}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 + i \frac{x}{b}\right), \quad (2.25)$$

$$B : v(x) = 1 - i \frac{gL}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 + i \frac{x}{b}\right) \left(1 - i \frac{gS}{2x}\right)^2, \quad (2.26)$$

$$C : v(x) = 1 - i \frac{gS}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 + i \frac{x}{b}\right) \left(1 - i \frac{gL}{x}\right), \quad (2.27)$$

$$\widetilde{BC} : v(x) = 1 - i \frac{g_0}{x}, \quad w(x) = \left(1 + i \frac{x}{a}\right) \left(1 + i \frac{x}{b}\right) \left(1 - i \frac{g_1}{x}\right) \left(1 - i \frac{g_2}{x}\right) \quad (2.28)$$

で与えられる. 結合定数 $a, b, g, g_L, g_S, g_0, g_1, g_2$ は正の実数である. 平衡点の式 (2.18) は Bethe 仮設方程式に似た形に書き表される (B, C, D は \widetilde{BC} から得られる):

$$A_{r-1} : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\bar{q}_j - \bar{q}_k - ig}{\bar{q}_j - \bar{q}_k + ig} = \frac{a - i\bar{q}_j}{a + i\bar{q}_j} \frac{b - i\bar{q}_j}{b + i\bar{q}_j}, \quad (2.29)$$

$$\widetilde{BC}_r : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\bar{q}_j - \bar{q}_k - ig_0}{\bar{q}_j - \bar{q}_k + ig_0} \frac{\bar{q}_j + \bar{q}_k - ig_0}{\bar{q}_j + \bar{q}_k + ig_0} = \frac{a - i\bar{q}_j}{a + i\bar{q}_j} \frac{b - i\bar{q}_j}{b + i\bar{q}_j} \frac{\bar{q}_j + ig_1}{\bar{q}_j - ig_1} \frac{\bar{q}_j + ig_2}{\bar{q}_j - ig_2}. \quad (2.30)$$

2.2.2 Ruijsenaars-Sutherland 系

極限で Sutherland 系に帰着する模型を Ruijsenaars-Sutherland 系と呼ぶ事にする. 関数 v と w は

$$A, D : v(x) = 1 - i \tanh g \cot x, \quad w(x) = 1, \quad (2.31)$$

$$B : v(x) = 1 - i \tanh g_L \cot x, \quad w(x) = (1 - i \tanh \frac{g_S}{2} \cot x)^2, \quad (2.32)$$

$$B' : v(x) = 1 - i \tanh g_L \cot x, \quad w(x) = 1 - i \tanh g_S \cot x, \quad (2.33)$$

$$C : v(x) = 1 - i \tanh g_S \cot x, \quad w(x) = 1 - i \tanh 2g_L \cot 2x, \quad (2.34)$$

$$C' : v(x) = 1 - i \tanh g_S \cot x, \quad w(x) = (1 - i \tanh g_L \cot 2x)^2, \quad (2.35)$$

$$B'C : v(x) = 1 - i \tanh g_M \cot x, \\ w(x) = (1 - i \tanh g_S \cot x)(1 - i \tanh 2g_L \cot 2x) \quad (2.36)$$

で与えられる。結合定数 g, g_L, g_M, g_S は正の実数である。平衡点の式 (2.18) は Bethe 仮設方程式に似た形に書き表される (B', C は $B'C$ から, D は B から得られる) :

$$A_{r-1} : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\tan(\bar{q}_j - \bar{q}_k) - i \tanh g}{\tan(\bar{q}_j - \bar{q}_k) + i \tanh g} = 1, \quad (2.37)$$

$$B_r : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\tan(\bar{q}_j - \bar{q}_k) - i \tanh g_L}{\tan(\bar{q}_j - \bar{q}_k) + i \tanh g_L} \frac{\tan(\bar{q}_j + \bar{q}_k) - i \tanh g_L}{\tan(\bar{q}_j + \bar{q}_k) + i \tanh g_L} = \left(\frac{\tan \bar{q}_j + i \tanh \frac{g_S}{2}}{\tan \bar{q}_j - i \tanh \frac{g_S}{2}} \right)^2, \quad (2.38)$$

$$C'_r : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\tan(\bar{q}_j - \bar{q}_k) - i \tanh g_S}{\tan(\bar{q}_j - \bar{q}_k) + i \tanh g_S} \frac{\tan(\bar{q}_j + \bar{q}_k) - i \tanh g_S}{\tan(\bar{q}_j + \bar{q}_k) + i \tanh g_S} = \left(\frac{\tan 2\bar{q}_j + i \tanh g_L}{\tan 2\bar{q}_j - i \tanh g_L} \right)^2, \quad (2.39)$$

$$B'C_r : \prod_{\substack{k=1 \\ k \neq j}}^r \frac{\tan(\bar{q}_j - \bar{q}_k) - i \tanh g_M}{\tan(\bar{q}_j - \bar{q}_k) + i \tanh g_M} \frac{\tan(\bar{q}_j + \bar{q}_k) - i \tanh g_M}{\tan(\bar{q}_j + \bar{q}_k) + i \tanh g_M} \\ = \frac{\tan \bar{q}_j + i \tanh g_S}{\tan \bar{q}_j - i \tanh g_S} \frac{\tan 2\bar{q}_j + i \tanh 2g_L}{\tan 2\bar{q}_j - i \tanh 2g_L}. \quad (2.40)$$

2.3 直交多項式と三項関係式

ここで直交多項式と三項関係式についての基礎事実を思い出しておく。

$\{f_n(x)\}_{n=0}^{\infty}$ を実係数の直交多項式の系列とする。 $f_n(x)$ は次数 n の x の多項式で (正定値) 内積 $(f, g) = \int f(x)g(x)w(x)dx$ ($w(x)$ は重み関数) に関して直交している, $(f_n, f_m) = h_n \delta_{n,m}$ ($h_n > 0$). $f_n^{\text{monic}}(x)$ をモノック多項式 $f_n(x) = c_n f_n^{\text{monic}}(x) = c_n(x^n + \dots)$ とする。すると, $f_n^{\text{monic}}(x)$ は次の三項関係式を満足する ($f_1^{\text{monic}}(x) = 0$ とおく) :

$$f_{n+1}^{\text{monic}}(x) - (x - a_n)f_n^{\text{monic}}(x) + b_n f_{n-1}^{\text{monic}}(x) = 0, \quad (n \geq 0). \quad (2.41)$$

a_n ($n \geq 0$) と b_n ($n \geq 1, b_0$ は不要, $b_n > 0$) は実数である。

面白いのはこの逆が成立する事である。 $\{f_n(x)\}$ を三項関係式 (2.41) (つまり, 実数 a_n ($n \geq 0$), b_n ($n \geq 1, b_n > 0$), c_n ($n \geq 0, c_n \neq 0$) を与える) で定義された多項式とすると, $\{f_n(x)\}$ は何らかの (正定値) 内積に関する直交多項式である。

3 Ruijsenaars 模型の古典平衡点を零点とする多項式

最初は、古典平衡点の式 (2.23)-(2.24), (2.29)-(2.30), (2.38)-(2.40) を数值的に解いて、その古典平衡点を零点とする多項式を計算する作業を繰り返し、それらを眺めて多項式が満たしている三項関係式を見出したのであるが、古典平衡点の式と(ほぼ)等価な関数方程式を考えればよい事が分かったので、多項式に対する関数方程式を解く事によって、変形された Hermite, Laguerre, Jacobi の直交多項式的具体形を決定した。以下では多項式の定義と(あまり長くない場合に)三項関係式の係数を具体的に与える。

3.1 Hermite の多項式の変形

3.1.1 Linear Confining Potential Case

方程式 (2.23) の解 $\{\bar{q}_j\}$ に対して

$$\bar{q}_j = \sqrt{ag} y_j, \quad \delta = \frac{g}{a} \quad (3.1)$$

と定義し、 $\{y_j\}$ を零点として持つ次数 r の x の多項式を導入する：

$$H_r(x, \delta) \stackrel{\text{def}}{=} 2^r \prod_{j=1}^r (x - y_j). \quad (3.2)$$

これは Hermite の多項式 (2.11) を変形したもので、 $\lim_{\delta \rightarrow 0} H_r(x, \delta) = H_r(x)$ である。 $H_r(x, \delta)$ が満たす三項関係式 (2.41) の係数は

$$a_n = 0, \quad b_n = \frac{n}{2} \left(1 + \frac{n-1}{2} \delta \right). \quad (3.3)$$

3.1.2 Quadratic Confining Potential Case

方程式 (2.29) の解 $\{\bar{q}_j\}$ に対して

$$\bar{q}_j = \sqrt{ag} y_j, \quad \delta = \frac{g}{a}, \quad \varepsilon = \frac{a}{b} \quad (3.4)$$

と定義し、 $\{y_j\}$ を零点として持つ次数 r の x の多項式を導入する：

$$H_r(x, \delta, \varepsilon) \stackrel{\text{def}}{=} 2^r \prod_{j=1}^r (x - y_j). \quad (3.5)$$

これは上の変形 Hermite 多項式を更に変形したもので、 $\lim_{\varepsilon \rightarrow 0} H_r(x, \delta, \varepsilon) = H_r(x, \delta)$ である。 $H_n(x, \delta, \varepsilon)$ が満たす三項関係式 (2.41) の係数は

$$a_n = 0, \quad b_n = \frac{n}{2} \left(1 + \frac{n-1}{2} \delta \right) \left(1 + \frac{n-1}{2} \delta \varepsilon \right) \frac{d_n}{d_{2n-1} d_{2n+1}}, \quad d_m = 1 + \left(1 + \frac{m-2}{2} \delta \right) \varepsilon. \quad (3.6)$$

3.2 Laguerre の多項式の変形

3.2.1 Linear Confining Potential Case

方程式 (2.24) の解 $\{\bar{q}_j\}$ に対して

$$\bar{q}_j = \sqrt{ag_0} y_j, \quad \delta = \frac{g_0}{a}, \quad \alpha = \frac{g_1 + g_2}{g_0} - 1, \quad \gamma = \frac{g_1 g_2}{g_0^2} \quad (3.7)$$

と定義し, $\{y_j^2\}$ を零点として持つ次数 r の x の多項式を導入する:

$$L_r^{(\alpha)}(x, \gamma, \delta) \stackrel{\text{def}}{=} \frac{(-1)^r}{r!} \prod_{j=1}^r (x - y_j^2). \quad (3.8)$$

これは Laguerre の多項式の 2 パラメータ変形で, $\lim_{\delta \rightarrow 0} L_r^{(\alpha)}(x, \gamma, \delta) = L_r^{(\alpha)}(x)$ である. $L_n^{(\alpha)}(x, \gamma, \delta)$ が満たす三項関係式 (2.41) の係数は

$$a_n = 2n + \alpha + 1 + (n(2n + 1) + 2n\alpha + \gamma)\delta, \quad (3.9)$$

$$b_n = n(n + \alpha) \left(1 + (2n + \alpha - 1)\delta + ((n - 1)(n + \alpha) + \gamma)\delta^2 \right). \quad (3.10)$$

3.2.2 Quadratic Confining Potential Case

方程式 (2.30) の解 $\{\bar{q}_j\}$ に対して

$$\bar{q}_j = \sqrt{ag_0} y_j, \quad \delta = \frac{g_0}{a}, \quad \varepsilon = \frac{b}{a}, \quad \alpha = \frac{g_1 + g_2}{g_0} - 1, \quad \gamma = \frac{g_1 g_2}{g_0^2} \quad (3.11)$$

と定義し, $\{y_j^2\}$ を零点として持つ次数 r の x の多項式を導入する:

$$L_r^{(\alpha)}(x, \gamma, \delta, \varepsilon) \stackrel{\text{def}}{=} \frac{(-1)^r}{r!} \prod_{j=1}^r (x - y_j^2). \quad (3.12)$$

これは上の変形 Laguerre 多項式を更に変形したもので, $\lim_{\varepsilon \rightarrow 0} L_r^{(\alpha)}(x, \gamma, \delta, \varepsilon) = L_r^{(\alpha)}(x, \gamma, \delta)$ である. $L_n^{(\alpha)}(x, \gamma, \delta, \varepsilon)$ が満たす三項関係式 (2.41) の係数は少し長いので省略する.

3.3 Jacobi の多項式の変形

A_{r-1} : 方程式 (2.37) の解は, 変形前の方程式 (2.9) と同じである. よって第 1 種の Chebyshev の多項式 $T_r(x)$ (2.13) は, ここでの問題設定では, 変形を受けない.

$B'C_r$: 方程式 (2.40) の解 $\{\bar{q}_j\}$ に対して

$$\delta = \tanh^2 g_M, \quad \alpha = \frac{\tanh g_S}{\tanh g_M} + \frac{\tanh 2g_L}{2 \tanh g_M} - 1, \quad \beta = \frac{\tanh 2g_L}{2 \tanh g_M} - 1 \quad (3.13)$$

と定義し, $\{\cos 2\bar{q}_j\}$ を零点とする次数 r の x の多項式を導入する:

$$P_r^{(\alpha, \beta)}(x, \delta) \stackrel{\text{def}}{=} 2^{-r} \binom{\alpha + \beta + 2r}{r} \prod_{j=1}^r (x - \cos 2\bar{q}_j). \quad (3.14)$$

これは Jacobi の多項式 (2.14) の変形で, $\lim_{\delta \rightarrow 0} P_r^{(\alpha, \beta)}(x, \delta) = P_r^{(\alpha, \beta)}(x)$ である. $P_n^{(\alpha, \beta)}(x, \delta)$ が満たす三項関係式 (2.41) の係数は少し長いので省略する.

C'_r : 方程式 (2.39) の解 $\{\bar{q}_j\}$ に対して

$$\delta = \tanh^2 g_S, \quad \alpha = \frac{\tanh g_L}{\tanh g_S} - 1 \quad (3.15)$$

と定義し, $\{\cos 2\bar{q}_j\}$ を零点とする次数 r の x の多項式を導入する:

$$\tilde{C}_r^{(\alpha + \frac{1}{2})}(x, \delta) \stackrel{\text{def}}{=} 2^r \binom{\alpha - \frac{1}{2} + r}{r} \prod_{j=1}^r (x - \cos 2\bar{q}_j). \quad (3.16)$$

これは Gegenbauer の多項式 (Jacobi の特別な場合) の変形で, $\lim_{\delta \rightarrow 0} \tilde{C}_r^{(\alpha + \frac{1}{2})}(x, \delta) = C_r^{(\alpha + \frac{1}{2})}(x)$ である. $\tilde{C}_n^{(\alpha + \frac{1}{2})}(x, \delta)$ が満たす三項関係式 (2.41) の係数は少し長いので省略する.

B_r : 方程式 (2.38) の解 $\{\bar{q}_j\}$ に対して

$$\delta = \tanh^2 g_L, \quad \alpha = \frac{2 \tanh \frac{g_S}{2}}{\tanh g_L} - 1 \quad (3.17)$$

と定義し, $\{\cos 2\bar{q}_j\}$ を零点とする次数 r の x の多項式を導入する:

$$\hat{P}_r^{(\alpha)}(x, \delta) \stackrel{\text{def}}{=} 2^{-r} \binom{\alpha - 1 + 2r}{r} \prod_{j=1}^r (x - \cos 2\bar{q}_j). \quad (3.18)$$

これは Jacobi の多項式 (2.14) の変形で, $\lim_{\delta \rightarrow 0} \hat{P}_r^{(\alpha)}(x, \delta) = P_r^{(\alpha, -1)}(x)$ である. $\hat{P}_n^{(\alpha)}(x, \delta)$ が満たす三項関係式 (2.41) の係数は少し長いので省略する.

4 コメント

Ruijsenaars 模型の古典平衡点を零点として持つ多項式として, 変形 Hermite, Laguerre, Jacobi 多項式を定義しその具体形を求めたが, これらは Askey-scheme として知られる超幾何直交多項式 [2] のメンバーになっている事が文献を調べているうちに明らかになった. 最後にその対応を挙げておく.

$H_n(x, \delta)$ (3.2) は Meixner-Pollaczek 多項式 $P_n^{(\lambda)}(x; \phi)$ ([2] の §1.7) の特別な場合 :

$$H_n(x, \delta) = n! \sqrt{\delta}^n P_n^{(\frac{1}{2})} \left(\frac{x}{\sqrt{\delta}}; \frac{\pi}{2} \right). \quad (4.1)$$

$H_n(x, \delta, \varepsilon)$ (3.5) は連続 Hahn 多項式 $p_n(x; a, b, c, d)$ ([2] の §1.4) の特別な場合 :

$$H_n(x, \delta, \varepsilon) = \frac{2^n n! \sqrt{\delta}^n}{(n-1 + \frac{2}{\delta} + \frac{2}{\delta\varepsilon})_n} P_n \left(\frac{x}{\sqrt{\delta}}; \frac{1}{\delta}, \frac{1}{\delta\varepsilon}, \frac{1}{\delta}, \frac{1}{\delta\varepsilon} \right), \quad (4.2)$$

$L_n^{(\alpha)}(x, \gamma, \delta)$ (3.8) は連続双対 Hahn 多項式 $S_n(x^2; a, b, c, d)$ ([2] の §1.3) をリスケールしたものの (α_1 と α_2 は $x^2 - (\alpha - 1)x + \gamma - \alpha = 0$ の 2 根) :

$$L_n^{(\alpha)}(y^2, \gamma, \delta) = \frac{\delta^n}{n!} S_n \left(\frac{y^2}{\delta}; \frac{1}{\delta}, \alpha_1 + 1, \alpha_2 + 1 \right). \quad (4.3)$$

$L_n^{(\alpha)}(x, \gamma, \delta, \varepsilon)$ (3.12) は Wilson 多項式 $W(x^2; a, b, c, d)$ ([2] の §1.1) をリスケールしたもの :

$$L_n^{(\alpha)}(y^2, \gamma, \delta, \varepsilon) = \frac{\delta^n}{n! (n + \alpha + \frac{1}{\delta} + \frac{1}{\delta\varepsilon})_n} W_n \left(\frac{y^2}{\delta}; \frac{1}{\delta}, \frac{1}{\delta\varepsilon}, \alpha_1 + 1, \alpha_2 + 1 \right). \quad (4.4)$$

$P_n^{(\alpha, \beta)}(x, \delta)$ (3.14) は Askey-Wilson 多項式 $p_n(x; a, b, c, d|q)$ ([2] の §3.1) の特別な場合 :

$$P_n^{(\alpha, \beta)}(x, \delta) = 2^{-2n} (a^{\alpha+\beta+2n}) (ab^2 q^{n-1}; q)_n^{-1} p_n(x; a, b, -b, -1|q), \quad (4.5)$$

$$q = \frac{1 - \sqrt{\delta}}{1 + \sqrt{\delta}} = e^{-2g_M}, \quad a = \frac{1 - (\alpha - \beta)\sqrt{\delta}}{1 + (\alpha - \beta)\sqrt{\delta}} = e^{-2g_S}, \quad b^2 = \frac{1 - 2(\beta + 1)\sqrt{\delta}}{1 + 2(\beta + 1)\sqrt{\delta}} = e^{-4g_L}. \quad (4.6)$$

$\tilde{C}_n^{(\alpha+\frac{1}{2})}(x, \delta)$ (3.16) も Askey-Wilson 多項式の特別な場合 :

$$\tilde{C}_n^{(\alpha+\frac{1}{2})}(x, \delta) = (a^{-\frac{1}{2}+n}) (a^4 q^{n-1}; q)_n^{-1} p_n(x; a, a, -a, -a|q), \quad (4.7)$$

$$q = \frac{1 - \sqrt{\delta}}{1 + \sqrt{\delta}} = e^{-2g_S}, \quad a^2 = \frac{1 - (\alpha + 1)\sqrt{\delta}}{1 + (\alpha + 1)\sqrt{\delta}} = e^{-2g_L}. \quad (4.8)$$

$\hat{P}_n^{(\alpha)}(x, \delta)$ (3.18) も Askey-Wilson 多項式の特別な場合 :

$$\hat{P}_n^{(\alpha)}(x, \delta) = 2^{-2n} (a^{-1+2n}) (a^2 q^{n-1}; q)_n^{-1} p_n(x; a, a, -1, -1|q), \quad (4.9)$$

$$q = \frac{1 - \sqrt{\delta}}{1 + \sqrt{\delta}} = e^{-2g_L}, \quad a = \frac{1 - \frac{1}{2}(\alpha + 1)\sqrt{\delta}}{1 + \frac{1}{2}(\alpha + 1)\sqrt{\delta}} = e^{-g_S}. \quad (4.10)$$

References

- [1] S. Odake and R. Sasaki, "Equilibria of 'Discrete' Integrable Systems and Deformations of Classical Polynomials", hep-th/0407155.
- [2] R. Koekoek and R. F. Swarttouw, "The Askey-scheme of hypergeometric orthogonal polynomials and its q -analogue", math.CA/9602214.

Multiple zeta-star values の巡回和公式

大野 泰生* 近畿大学理工学部

若林 徳子 近畿大学総合理工学研究科

Abstract

多重ゼータ値 (MZV, MZSV) のなす \mathbb{Q} -代数の構造を把握する上で重要とされる和公式の均等な細分化について述べる.

1 Introduction

多重ゼータ値とその与える \mathbb{Q} -代数 (およびその類似物) は, 数論をはじめとして, トポロジー・量子物理学におよぶ様々な分野に現れ研究されている. 近年では研究手法も多様となり, 数論・組合せ論・微分方程式・超幾何関数など様々な分野の研究者の交流点ともなっている. これら研究者の主な目標のひとつは, まず多重ゼータ値のなす \mathbb{Q} -代数の構造を詳しく理解することであり, 我々は多重ゼータ値の間の \mathbb{Q} -線形関係式の全体像を把握することを試みている. すでに多くの関係式が証明され, その全体像も解明されてきているが, まだ未解明の謎が多く存在している.

多重ゼータ値には2つの種類がある. 歴史上, 多重ゼータ値を最初に扱ったとされる Euler([6]) は, 我々が MZSVs (multiple zeta-star values ; 等号付き多重ゼータ値) と呼んでいるものを主体に扱っていたようである. 一方, 近年の研究の主流は MZVs (multiple zeta values) であり, 通常こちらが多重ゼータ値と呼ばれている. MZSV も MZV も (各重さ毎に) 互いに他の線形結合で書き下せることから, 上述の \mathbb{Q} -代数は同一のものである.

MZSVs と MZVs の定義は以下の通りである: 許容的多重インデックス $\mathbf{k} = (k_1, k_2, \dots, k_n)$ (即ち $k_i \in \mathbb{Z}, k_1 > 1, k_i > 0$) に対して,

$$\zeta^*(\mathbf{k}) = \zeta^*(k_1, k_2, \dots, k_n) = \sum_{m_1 \geq m_2 \geq \dots \geq m_n \geq 1} \frac{1}{m_1^{k_1} m_2^{k_2} \dots m_n^{k_n}},$$

*Supported in part by JSPS Grant-in-Aid No. 15740025 and No. 15540190 and by Kinki University Grant No. 2003-GS02.

$$\zeta(\mathbf{k}) = \zeta(k_1, k_2, \dots, k_n) = \sum_{m_1 > m_2 > \dots > m_n > 0} \frac{1}{m_1^{k_1} m_2^{k_2} \dots m_n^{k_n}}.$$

多重インデックス $\mathbf{k} = (k_1, k_2, \dots, k_n)$ ($k_i \in \mathbb{Z}, k_i > 0$) に対して, \mathbf{k} の重さ $\text{wt}(\mathbf{k})$, 深さ $\text{dep}(\mathbf{k})$, 高さ $\text{ht}(\mathbf{k})$ とは, それぞれ $k = k_1 + k_2 + \dots + k_n$, n , $s = \#\{i | k_i > 1\}$ で決まる整数のこととする. 記号 $I(k, n, s)$ で重さ k , 深さ n , 高さ s の多重インデックス \mathbf{k} の全体集合を表し, $I_0(k, n, s)$ で許容的すなわち $k_1 > 1$ を満たす元による部分集合を記し, 更に $I(k, n) = \bigcup_{s=1}^{\min(n, k-n)} I(k, n, s)$ と定める.

試しに MZSV の値を 2 つほど, なるべく depth の小さい MZVs を使って書き下してみると,

$$\zeta^*(3, 2, 2) = \frac{-291}{16} \zeta(7) + \frac{21}{10} \zeta(2)^2 \zeta(3) + \frac{15}{2} \zeta(2) \zeta(5),$$

$$\zeta^*(3, 3, 2) = \frac{1151}{350} \zeta(2)^4 + \frac{9}{2} \zeta(2) \zeta(3)^2 - 27 \zeta(3) \zeta(5) + \frac{27}{4} \zeta(6, 2),$$

というような式で, 総じて重さを増すにつれて煩雑な表記になる.

本題に入る前に和公式の復習をしておく. 和公式は多重ゼータ値のなす Q -代数の構造を把握する上で最も重要な関係式のひとつであると目されている. 次節で述べる巡回和公式はこの公式の精密化である.

Theorem 1 (和公式; Granville[7], Zagier[17]) 任意の整数 $k > n > 0$ に対して以下が成立.

$$\sum_{(k_1, k_2, \dots, k_{n+1}) \in I(k, n+1)} \zeta(k_1 + 1, k_2, \dots, k_{n+1}) = \zeta(k + 1),$$

$$\sum_{(k_1, k_2, \dots, k_{n+1}) \in I(k, n+1)} \zeta^*(k_1 + 1, k_2, \dots, k_{n+1}) = \binom{k}{n} \zeta(k + 1).$$

本稿では, MZSVs についての巡回和公式を述べる. 他方の MZVs に対する巡回和公式は Hoffman と第一筆者の共同研究により既に得られている ([10]) が, 次節に記すように両辺とも MZVs の和となるやや複雑な関係式族である. 本稿で与える MZSVs の巡回和公式は MZSVs の和をリーマンゼータ値の整数倍として記述するものであり, 上述の和公式の均等な細分化になっており, 巡回和の標準的な理解を示唆しているように思われる.

2 MZSVsの巡回和公式

本節では巡回和の定義, 主定理 (MZSVsの巡回和公式) を述べ, 重さの小さい部分での具体的な表を与える.

σ を長さ n (位数 n) の巡回置換とし, $\sigma^j = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau_j(1) & \tau_j(2) & \cdots & \tau_j(n) \end{pmatrix}$ と書くとき, 多重インデックス $(k_1, k_2, \dots, k_n), (h_1, h_2, \dots, h_n) \in I(k, n)$ が巡回同値であるとは,

$$(h_1, h_2, \dots, h_n) = (k_{\tau_j(1)}, k_{\tau_j(2)}, \dots, k_{\tau_j(n)})$$

を満たす整数 j が存在することと定義する. 記号 $\Pi(k, n)$ で $I(k, n)$ における巡回同値類の全体を記す.

筆者が今回得た結果は以下のものである.

Theorem 2 $\Pi(k, n)$ ($k > n > 0$) の任意の元 α に対して以下が成り立つ.

$$\sum_{(k_1, k_2, \dots, k_n) \in \alpha} \sum_{i=0}^{k_1-2} \zeta^*(k_1 - i, k_2, \dots, k_n, i + 1) = \frac{k|\alpha|}{n} \zeta(k + 1).$$

ここで左辺の第 2 の和について, $k_1 = 1$ のときは 0 とする.

比較のために MZVs に対する巡回和公式を再掲しておく.

Theorem 3 ([10]) $\Pi(k, n)$ ($k > n > 0$) の任意の元 α に対して以下が成り立つ.

$$\sum_{(k_1, k_2, \dots, k_n) \in \alpha} \zeta(k_1 + 1, k_2, \dots, k_n) = \sum_{(k_1, k_2, \dots, k_n) \in \alpha} \sum_{i=0}^{k_n-2} \zeta(k_1 - i, \dots, k_n, i + 1).$$

ここで右辺の第 2 の和について, $k_1 = 1$ のときは 0 とする.

比較して明らかなように, 定理 3 の公式は両辺とも MZVs の線形和になっており, やや複雑である. 定理 2 の公式では右辺がリーマンゼータ値の定数倍になっており, 和公式の均等な分割 (位数分の重み付きで) になることも容易に確認できる.

重さ 8 未満の MZSVs について, 各巡回同値類の元とその値の総和は次頁の表の通りである.

wt.	dep.	$k \in \alpha$	MZSVs	和	$\frac{n}{ \alpha }$
3	2	(2)	$\zeta^*(2, 1)$	$2\zeta(3)$	1
4	2	(3)	$\zeta^*(3, 1), \zeta^*(2, 2)$	$3\zeta(4)$	1
	3	(2, 1)	$\zeta^*(2, 1, 1)$	$3\zeta(4)$	1
5	2	(4)	$\zeta^*(4, 1), \zeta^*(3, 2), \zeta^*(2, 3)$	$4\zeta(5)$	1
	3	(3, 1)	$\zeta^*(3, 1, 1), \zeta^*(2, 1, 2)$	$4\zeta(5)$	1
	3	(2, 2)	$\zeta^*(2, 2, 1)$	$2\zeta(5)$	2
	4	(2, 1, 1)	$\zeta^*(2, 1, 1, 1)$	$4\zeta(5)$	1
6	2	(5)	$\zeta^*(5, 1), \zeta^*(4, 2), \zeta^*(3, 3), \zeta^*(2, 4)$	$5\zeta(6)$	1
	3	(4, 1)	$\zeta^*(4, 1, 1), \zeta^*(3, 1, 2), \zeta^*(2, 1, 3)$	$5\zeta(6)$	1
	3	(3, 2)	$\zeta^*(3, 2, 1), \zeta^*(2, 2, 2), \zeta^*(2, 3, 1)$	$5\zeta(6)$	1
	4	(3, 1, 1)	$\zeta^*(3, 1, 1, 1), \zeta^*(2, 1, 1, 2)$	$5\zeta(6)$	1
	4	(2, 2, 1)	$\zeta^*(2, 2, 1, 1), \zeta^*(2, 1, 2, 1)$	$5\zeta(6)$	1
	5	(2, 1, 1, 1)	$\zeta^*(2, 1, 1, 1, 1)$	$5\zeta(6)$	1
7	2	(6)	$\zeta^*(6, 1), \zeta^*(5, 2), \zeta^*(4, 3), \zeta^*(3, 4), \zeta^*(2, 5)$	$6\zeta(7)$	1
	3	(5, 1)	$\zeta^*(5, 1, 1), \zeta^*(4, 1, 2), \zeta^*(3, 1, 3), \zeta^*(2, 1, 4)$	$6\zeta(7)$	1
	3	(4, 2)	$\zeta^*(4, 2, 1), \zeta^*(3, 2, 2), \zeta^*(2, 2, 3), \zeta^*(2, 4, 1)$	$6\zeta(7)$	1
	3	(3, 3)	$\zeta^*(3, 3, 1), \zeta^*(2, 3, 2)$	$3\zeta(7)$	2
	4	(4, 1, 1)	$\zeta^*(4, 1, 1, 1), \zeta^*(3, 1, 1, 2), \zeta^*(2, 1, 1, 3)$	$6\zeta(7)$	1
	4	(3, 2, 1)	$\zeta^*(3, 2, 1, 1), \zeta^*(2, 2, 1, 2), \zeta^*(2, 1, 3, 1)$	$6\zeta(7)$	1
	4	(3, 1, 2)	$\zeta^*(3, 1, 2, 1), \zeta^*(2, 1, 2, 2), \zeta^*(2, 3, 1, 2)$	$6\zeta(7)$	1
	4	(2, 2, 2)	$\zeta^*(2, 2, 2, 1)$	$2\zeta(7)$	3
	5	(3, 1, 1, 1)	$\zeta^*(3, 1, 1, 1, 1), \zeta^*(2, 1, 1, 1, 2)$	$6\zeta(7)$	1
	5	(2, 2, 1, 1)	$\zeta^*(2, 2, 1, 1, 1), \zeta^*(2, 1, 1, 2, 1)$	$6\zeta(7)$	1
	5	(2, 1, 2, 1)	$\zeta^*(2, 1, 2, 1, 1)$	$3\zeta(7)$	2
	6	(2, 1, 1, 1, 1)	$\zeta^*(2, 1, 1, 1, 1, 1)$	$6\zeta(7)$	1

3 補足

証明の詳細は論文 [14] を見ていただきたいが、収束級数

$$C(k_1, k_2, \dots, k_n) = \sum_{\substack{a_1 \geq a_2 \geq \dots \geq a_n \geq a_{n+1} \geq 1 \\ a_1 \neq a_{n+1}}} \frac{1}{a_1^{k_1} a_2^{k_2} \dots a_n^{k_n} (a_1 - a_{n+1})}$$

に対して、次の命題を証明することにより定理 2 が従う。証明全体は比較的初等的な分数の計算であり、大筋において MZVs の巡回和公式の証明と類似

である.

Proposition 1 任意の自然数 n, k_1, \dots, k_n (ただし $k = k_1 + k_2 + \dots + k_n > n$) に対して次が成立する.

$$\begin{aligned} & C(k_1, k_2, \dots, k_n) - C(k_2, k_3, \dots, k_n, k_1) \\ &= k_1 \zeta(k+1) - \sum_{i=0}^{k_1-2} \zeta^*(k_1-i, k_2, k_3, \dots, k_n, i+1). \end{aligned}$$

定理 2 と定理 3 それぞれが, 各重さの MZVs の張る \mathbb{Q} -ベクトル空間の次元の上限にもたらず寄与は同等であるが, 今後定理 3 の一般化を目指すよりもむしろ, 値の均一性を伴っている定理 2 の一般化を目指す方が順当であろうという推測は真っ当に感じられる.

References

- [1] T. Aoki and Y. Ohno, Sum relations for multiple zeta values and connection formulas for the Gauss hypergeometric functions, to appear in *Publ. Res. Inst. Math. Sci.*
- [2] T. Arakawa and M. Kaneko, Multiple zeta values, poly-Bernoulli numbers, and related zeta functions, *Nagoya Math. J.*, **153** (1999), 191-216.
- [3] J. M. Borwein, D. H. Bailey, and R. Girgensohn, Experimentation in mathematics, A. K. Peters, 2004.
- [4] J. M. Borwein, D. M. Bradley, D. J. Broadhurst and P. Lisoněk, Special values of multiple polylogarithms, *Trans. Amer. Math. Soc.*, **353** (2000), 907-941.
- [5] D. Bowman and D. M. Bradley, Resolution of some open problems concerning multiple zeta evaluations of arbitrary depth, *Compositio Math.*, **139** (2003), 85-100.
- [6] L. Euler, Meditationes circa singulare serierum genus, *Novi Comm. Acad. Sci. Petropol.*, **20** (1775), 140-186, reprinted in *Opera Omnia ser. I*, vol. 15, B. G. Teubner, Berlin (1927), 217-267.
- [7] A. Granville, A decomposition of Riemann's zeta-function, in *London Math. Soc. Lecture Note Ser.* 247, Cambridge, 1997, pp. 95-101.

- [8] M. Hoffman, Multiple harmonic series, *Pacific J. Math.*, **152** (1992), 275-290.
- [9] M. E. Hoffman, The algebra of multiple harmonic series, *J. Algebra*, **194** (1997), 477-495.
- [10] M. Hoffman and Y. Ohno, Relations of multiple zeta values and their algebraic expression, *J. Algebra*, **262** (2003), 332-347.
- [11] K. Ihara, M. Kaneko and D. Zagier, Multiple zeta values, Derivation relations and regularized double shuffle relations of multiple zeta values, in preparation.
- [12] Y. Ohno, A generalization of the duality and sum formulas on the multiple zeta values, *J. Number Theory*, **74** (1999), 39-43.
- [13] Y. Ohno, Sum relations for multiple zeta values, in *Proceedings of Symposium of Zeta functions, Topology, and Quantum physics 2003*. to appear.
- [14] Y. Ohno and N. Wakabayashi, Cyclic sum of multiple zeta values, in preparation.
- [15] Y. Ohno and D. Zagier, Multiple zeta values of fixed weight, depth, and height, *Indag. Math.*, **12** (2001), 483-487.
- [16] D. Zagier, Values of zeta functions and their applications, in Proceedings of ECM 1992, *Progress in Math.*, **120** (1994), 497-512.
- [17] D. Zagier, Multiple zeta values, Unpublished preprint, Bonn, 1995.

Department of Mathematics
Kinki University
Higashi-Osaka, 577-8502 Japan
ohno@math.kindai.ac.jp
noriko@math.kindai.ac.jp

Relative difference sets in $\text{Alt}(5)$

Yutaka Hiramine

Department of Mathematics, Faculty of Education, Kumamoto University

Kurokami, Kumamoto, Japan

E-mail: hiramine@gpo.kumamoto-u.ac.jp

Abstract

This paper is motivated by N. Ito's paper [3], in which he constructed a $(60, 2, 60, 30)$ -relative difference sets in $\text{SL}(2, 5)$. This is the only example of a nontrivial relative difference set in a non-solvable group known to the author. As its homomorphic image, another relative difference set is obtained in a simple group $\text{Alt}(5)$. However, this is a trivial difference set. In this paper we study relative difference sets in $\text{Alt}(5)$ and show that there exist exactly two nontrivial relative difference sets in $\text{Alt}(5)$ up to equivalence.

1 Introduction

Let G be a group of order mu and U a subgroup of G of order u . A k -subset D of G is called a (m, u, k, λ) -difference set in G with respect to U if $DD^{(-1)} = k + \lambda(G - U)$. Here we identify a subset X of G with an element $\sum_{x \in X} x \in \mathbb{C}[G]$

and set $X^{(-1)} = \sum_{x \in X} x^{-1}$. D is also called a relative difference set relative to U and U is called a forbidden subgroup. If $U = 1$, then D is an ordinary (m, k, λ) -difference set. We say that D is trivial if $k = 1$ or $(u, k) \in \{(1, m), (1, m - 1)\}$. Two relative difference sets D_1 and D_2 in G are equivalent if $D_1 = (D_2)^\theta g$ for an element $g \in G$ and an automorphism θ of G .

In this paper we give a classification of relative difference sets in $\text{Alt}(5)$.

Theorem. *Let D be a nontrivial (m, u, k, λ) -difference set in $\text{Alt}(5)$ relative to its subgroup U . Then D is equivalent to one of the following.*

- (i) $(m, u, k, \lambda) = (12, 5, 11, 2)$, $U = \langle (1, 2, 3, 4, 5) \rangle$ and $D = D_1 \cup D_1^{(-1)} \cup D_2$, where $D_1 = \{(1, 2, 5), (1, 3, 5), (1, 2, 4, 3, 5), (1, 2, 4, 5, 3)\}$ and $D_2 = \{(1, 2)(4, 5), (2, 4)(3, 5), (2, 5)(3, 4)\}$.
- (ii) $(m, u, k, \lambda) = (30, 2, 29, 14)$, $U = \langle (2, 3)(4, 5) \rangle$ and $D = D_1 \cup D_1^{(-1)} \cup D_2$, where $D_1 = \{(1, 2, 4), (1, 3, 5), (1, 4, 5), (2, 4, 5), (3, 4, 5), (1, 2, 3, 5, 4), (1, 2, 5, 3, 4), (1, 2, 5, 4, 3), (1, 3, 2, 4, 5), (1, 3, 4, 2, 5), (1, 4, 2, 3, 5)\}$ and

$$D_2 = \{(1, 3)(4, 5), (1, 3)(2, 5), (1, 2)(4, 5), (1, 2)(3, 4), (1, 5)(2, 4), (1, 4)(3, 5), (2, 4)(3, 5)\}.$$

2 Relative difference sets in $Alt(5)$ obtained from affine difference sets

Let D be a nontrivial (m, u, k, λ) -difference set in $G (= Alt(5))$ relative to a subgroup U of G . Then, as $DD^{(-1)} = k + \lambda(G - U)$, we have $k^2 = k + \lambda(60 - u)$, $k \leq m (= |G : U|)$ and $u|60$. On the other hand, if λ is odd, then all involutions of G are contained in U , as otherwise an involution outside U , say x , is represented an even number of times as a difference $d_1 d_2^{-1} (= d_2 d_1^{-1})$ with $d_1, d_2 \in D$. Hence we can easily check that there are exactly three types of possible parameters (m, u, k, λ) as follows :

$$(i) (12, 5, 11, 2), \quad (ii) (30, 2, 29, 14), \quad (iii) (20, 3, 19, 6) \quad (1)$$

In this section we construct relative difference sets of type (i) and (ii). The method is to use the following lemma.

Lemma 2.1 (Elliot Butson [1]) *Let D be an (m, u, k, λ) -difference set in G relative to U . If N is a normal subgroup of G of order n contained in U , and if φ denotes the canonical epimorphism $G \rightarrow G/N$, then $\varphi(D)$ is an $(m, u/n, k, \lambda n)$ -difference set in G/N relative to U/N .*

First we construct a $(m+1, m-1, m, 1)$ -difference set in a group G which involves $Alt(5)$ for $m = 11, 29$. A relative difference set with such parameters is called an *affine difference set* of order m (See [4]). Then, setting a natural homomorphism $\varphi : G \rightarrow G/Z(G)$ and applying Lemma 2.1, we obtain a nontrivial relative difference set in $Alt(5)$.

Let $K \times K$ be a 2-dimensional vector space over $K = GF(p^e)$, where p is a prime. We can regard $K \times K$ as a desarguesian affine plane of order p^e . Let $\mathbb{P} = K \times K \setminus \{O\}$, where $O = (0, 0)$ and let $\mathbb{L} = \{\ell_{a,b} \mid a, b \in K, b \neq 0\} \cup \{\ell_c \mid c \in K, c \neq 0\}$ be the set of lines of $K \times K$ not through O , where $\ell_{a,b} = \{(x, ax + b) \mid x \in K\}$, $\ell_c = \{(c, y) \mid y \in K\}$. Clearly $GL(2, p^e)$ leaves \mathbb{P} and \mathbb{L} invariant and $|\mathbb{P}| = |\mathbb{L}| = p^{2e} - 1$.

Lemma 2.2 *Let G be a subgroup of $GL(2, p^e)$ isomorphic to $SL(2, 5)$. If $p > 5$, then every nonidentity element of G fixes no element of \mathbb{P} and \mathbb{L} .*

Proof. Let g be a nonidentity element of G and set $g = \begin{bmatrix} s & t \\ u & v \end{bmatrix}$, where $s, t, u, v \in K$. If g fixes an element of \mathbb{P} . Then one of the eigenvalues of g is 1.

Since $g \in G = [G, G] \subset SL(2, p^e)$, g is similar to $\begin{bmatrix} 1 & 0 \\ k & 1 \end{bmatrix}$ for some $k \in K$. By assumption $p \nmid |G|$, hence $g = 1$, a contradiction.

We can check the following :

$$(\ell_{a,b})g = \begin{cases} \ell_{\frac{ua+t}{ua+s}, \frac{b}{ua+s}} & \text{if } ua + s \neq 0 \\ \ell_{ub} & \text{if } ua + s = 0 \end{cases}, \quad (\ell_c)g = \begin{cases} \ell_{\frac{u}{v}, \frac{-t}{v}} & \text{if } u \neq 0 \\ \ell_{sc} & \text{if } u = 0 \end{cases}$$

Assume g fixes an element $\ell_{a,b} \in \mathbb{L}$. Then $ua + s \neq 0$ and $a = \frac{ua+t}{ua+s}$, $b = \frac{b}{ua+s}$. Hence $au + s = 1$, $av + t = a$. If $u = 0$ or $v = 1$, then $g = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}$, respectively. This implies that g is an element of order p , contrary to the assumption that $p > 5$. Thus $\frac{1-s}{u} = \frac{t}{1-v}$. From this, $\text{tr}(g) = s + v = 2$ and so g is similar to $\begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$ for some $k \in K$, a contradiction. Similarly we can show that $(\ell_c)g \neq \ell_c$.

(I) A construction of a $(12, 5, 11, 2)$ -difference set in $Alt(5)$:

Let $K = GF(11)$ and set $x_1 = \begin{bmatrix} 7 & 2 \\ 6 & 5 \end{bmatrix}$, $x_2 = \begin{bmatrix} 1 & 7 \\ 6 & 10 \end{bmatrix}$, $x_3 = \begin{bmatrix} 10 & 1 \\ 9 & 1 \end{bmatrix}$ and $Z = \langle -I_2 \rangle$. Here I_n is the identity matrix of size n . Then $x_1^3 \equiv x_2^2 \equiv x_3^2 \equiv (x_1x_2)^3 \equiv (x_2x_3)^3 \equiv (x_1x_3)^2 \equiv 1 \pmod{Z}$. Set $G = \langle x_1, x_2, x_3 \rangle$ and $H = \langle x_1, x_2 \rangle$. Then G and H are subgroups of $SL(2, 11)$. On the other hand, setting $y_1 = (2, 5, 4)$, $y_2 = (1, 4)(2, 5)$ and $y_3 = (1, 3)(2, 5)$, we have $y_1^3 = y_2^2 = y_3^2 = (y_1y_2)^3 = (y_2y_3)^3 = (y_1y_3)^2 = 1$. Hence a mapping μ from G to $Alt(5)$ defined by $\mu(x_i) = y_i$ for $i \in \{1, 2, 3\}$ is a homomorphism. By Example 19.8 of [2] and the simplicity of $Alt(5)$, we have $G/Z \simeq Alt(5) \supset H/Z \simeq Alt(4)$ and so $G \simeq SL(2, 5)$. We note that $\langle y_1 \rangle \simeq \mathbb{Z}_3$, $\langle y_1 \rangle \langle y_2, y_2^{y_1} \rangle \simeq Alt(4) \subset Alt(5) = \langle y_1 \rangle \langle y_2, y_2^{y_1} \rangle \langle y_4 \rangle$, where $y_2^{y_1} = y_1^{-1}y_2y_1$ and $y_4 = y_1y_2y_3 = (1, 4, 2, 5, 3)$. Set $x_4 = x_1x_2x_3$. Then, as μ is a homomorphism, we have the following.

$$G = \pm \{1, x_1, x_1^2\} \{1, x_2, x_2^{x_1}, x_2^{x_1^2}\} \{1, x_4, x_4^2, x_4^3, x_4^4\} \quad (2)$$

Let \mathbb{P} and \mathbb{L} be as before. Then $|\mathbb{P}| = |\mathbb{L}| = |G| = 120$. It follows from Lemma 2.2 that G acts regularly on \mathbb{P} and \mathbb{L} . For a point $(1, 0) \in \mathbb{P}$ and a line $\ell = \{1\} \times K$, we set $D = \{g \in G \mid (1, 0)g \in \ell\}$. Then $D = \{g \in G \mid (g)_{1,1} = 1\}$, where $(g)_{ij}$ is the (i, j) -entry of g . Therefore we have the following.

Lemma 2.3 *The following hold.*

- (i) $|D| = 11$.
- (ii) Let U be the set of diagonal matrices in G . Then $Z(G) \leq U = \langle x_4 \rangle \simeq \mathbb{Z}_{10}$, where $x_4 = x_1x_2x_3 = \begin{bmatrix} 8 & 0 \\ 0 & 7 \end{bmatrix}$.
- (iii) Let $d_1, d_2 \in D$ and assume that $d_1d_2^{-1} \in U$. Then $d_1 = d_2$.

(iv) Let $d_1, d_2, d_3, d_4 \in D$. If $d_1 d_2^{-1} = d_3 d_4^{-1}$, then either (1) $d_1 = d_2$ and $d_3 = d_4$ or (2) $d_1 = d_3$ and $d_2 = d_4$.

Proof. (i) follows immediately from the regularity of G on \mathbb{P} . Clearly $|U| \leq 10$ and as $x_1 x_2 x_3 = \begin{bmatrix} 8 & 0 \\ 0 & 7 \end{bmatrix} \in G$, we have (ii). Since $(d_1)_{1,1} = (d_2)_{1,1} = 1$, we can verify (iii).

Assume $d_1 d_2^{-1} = d_3 d_4^{-1}$ and $d_1 \neq d_2$. Then $(1,0)d_1 d_2^{-1} = (1,0)d_3 d_4^{-1} = (u, v)$ for some $(u, v) \in \mathbb{P}$, $(u, v) \neq (1,0)$. Set $d_i = \begin{bmatrix} 1 & a_i \\ b_i & c_i \end{bmatrix}$ for $i \in \{1, 2, 3, 4\}$. Then $(1,0) \begin{bmatrix} 1 & a_1 \\ b_1 & c_1 \end{bmatrix} = (u, v) \begin{bmatrix} 1 & a_2 \\ b_2 & c_2 \end{bmatrix}$ and $(1,0) \begin{bmatrix} 1 & a_3 \\ b_3 & c_3 \end{bmatrix} = (u, v) \begin{bmatrix} 1 & a_4 \\ b_4 & c_4 \end{bmatrix}$. Hence $u + v b_2 = u + v b_4 = 1$ and $a_1 = a_2 u + c_2 v$, $a_3 = a_4 u + c_4 v$. By the first equation, $v \neq 0$ as $(u, v) \neq (1,0)$. From this, $b_2 = b_4$, which implies that $d_2^{-1} d_4 (\in G)$ is a triangular matrix. As $|G|$ is not divisible by 11, $d_2^{-1} d_4$ is a diagonal matrix. (iv) follows at once from (iii).

Applying (iii) and (iv) of Lemma 2.3, we have the following.

Proposition 2.4 Let G, D and U be as in Lemma 2.3. Then D is an affine difference set of order 11 in $G (= SL(2, 5))$ relative to U .

Using (2), we can verify the following :

$$D = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 7 \\ 6 & 10 \end{bmatrix} (= x_2), \begin{bmatrix} 1 & 4 \\ 3 & 2 \end{bmatrix} (= -x_2^{x_1} x_4^4), \right. \\ \left. \begin{bmatrix} 1 & 3 \\ 4 & 2 \end{bmatrix} (= x_1 x_4), \begin{bmatrix} 1 & 2 \\ 10 & 10 \end{bmatrix} (= -x_1 x_2 x_4^4), \begin{bmatrix} 1 & 9 \\ 5 & 2 \end{bmatrix} (= x_1 x_2^{x_1} x_4^2), \right. \\ \left. \begin{bmatrix} 1 & 8 \\ 8 & 10 \end{bmatrix} (= -x_1 x_2 x_2^{x_1} x_4^4), \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} (= -x_1^2 x_4^4), \begin{bmatrix} 1 & 5 \\ 9 & 2 \end{bmatrix} (= x_1^2 x_2 x_4), \right. \\ \left. \begin{bmatrix} 1 & 6 \\ 7 & 10 \end{bmatrix} (= -x_1^2 x_2^{x_1} x_4^4), \begin{bmatrix} 1 & 10 \\ 2 & 10 \end{bmatrix} (= -x_1^2 x_2 x_2^{x_1} x_4^4) \right\}.$$

As a corollary, we have

Proposition 2.5 Set $\bar{D} = \{(2, 5)(3, 4), (1, 3, 4), (1, 3, 2, 4, 5), (1, 3)(2, 4), (2, 3)(4, 5), (1, 4, 5), (1, 4, 5, 2, 3), (1, 5, 4), (1, 5, 4, 2, 3), (1, 3, 2, 5, 4), (1, 4, 3)\}$. Then \bar{D} is a $(12, 5, 11, 2)$ -difference set in $\text{Alt}(5)$ relative to $\bar{U} = \{(1, 2, 3, 4, 5)\}$.

Proof. Let G, D and U be as in Lemma 2.3 and let μ be as before. By the proof of Lemma 2.3(ii), $\mu(U) = \mu(\langle x_1 x_2 x_3 \rangle) = \langle y_1 y_2 y_3 \rangle = \langle (1, 4, 2, 5, 3) \rangle = \langle (1, 2, 3, 4, 5) \rangle$. It follows from Lemmas 2.1, 2.3(ii) and Proposition 2.4 that $\mu(D)$ is a $(12, 5, 11, 2)$ -difference set in $\mu(G)$ relative to $\langle (1, 2, 3, 4, 5) \rangle$. On the other hand $\mu(D) = \{\mu(1), \mu(x_2), \mu(-x_2^{x_1} x_4^4), \mu(x_1 x_4), \mu(-x_1 x_2 x_4^4), \mu(x_1 x_2^{x_1} x_4^2), \mu(-x_1 x_2 x_2^{x_1} x_4^4), \mu(-x_1^2 x_4^4), \mu(x_1^2 x_2 x_4), \mu(-x_1^2 x_2^{x_1} x_4^4), \mu(x_1^2 x_2 x_2^{x_1} x_4^4)\}$
 $= \{e, y_2, y_2^{y_1} y_4^4, y_1 y_4, y_1 y_2 y_4^4, y_1 y_2^{y_1} y_4^2, y_1 y_2 y_2^{y_1} y_4^4, y_1^2 y_4^2, y_1^2 y_2 y_4, y_1^2 y_2^{y_1} y_4^4, y_1^2 y_2 y_2^{y_1} y_4\}$
 $= \{e, (1, 4)(2, 5), (1, 4, 2, 3, 5), (1, 4, 5, 2, 3), (2, 4)(3, 5), (1, 3, 4, 2, 5), (1, 3)(2, 4),$

$(1, 2, 5, 3, 4), (1, 2, 4, 5, 3), (1, 4)(3, 5), (1, 3)(2, 5)\}$, where e is the identity element of $Alt(5)$. Set $\bar{D} = \mu(D)(2, 5)(3, 4) = \{(2, 5)(3, 4), (1, 3, 4), (1, 3, 2, 4, 5), (1, 3)(2, 4), (2, 3)(4, 5), (1, 4, 5), (1, 4, 5, 2, 3), (1, 5, 4), (1, 5, 4, 2, 3), (1, 3, 2, 5, 4), (1, 4, 3)\}$. Then we have the proposition.

Remark 2.6 We have chosen a translate \bar{D} of $\mu(D)$ so that $\bar{D} \cap \bar{U} = \phi$. Therefore $Alt(5) = \bar{U}\bar{D} \cup \bar{U}$ and we can verify that $\bar{D} = \bar{D}^{(-1)}$.

(II) A construction of a $(30, 2, 29, 14)$ -difference set in $Alt(5)$:

Let $K = GF(29)$ and set $x_1 = \begin{bmatrix} 20 & 3 \\ 18 & 10 \end{bmatrix}, x_2 = \begin{bmatrix} 20 & 1 \\ 5 & 9 \end{bmatrix},$
 $x_3 = \begin{bmatrix} 2 & 26 \\ 21 & 27 \end{bmatrix}$ and $G_0 = \langle x_1, x_2, x_3 \rangle \leq SL(2, 29), Z_0 = \langle -I_2 \rangle$. Let y_1, y_2 and y_3 be as in the case (I). Since $x_1^3 \equiv x_2^2 \equiv x_3^2 \equiv (x_1x_2)^3 \equiv (x_2x_3)^3 \equiv (x_1x_3)^2 \equiv 1 \pmod{Z_0}$, we can define a homomorphism μ from G_0 to $\langle y_1, y_2, y_3 \rangle (= Alt(5))$ in a similar way as in (I). Then it follows that $G_0 = \pm \langle x_1 \rangle \langle x_2, x_2^{x_1} \rangle \langle x_4 \rangle \simeq SL(2, 5), \mu^{-1}(e) = Z_0$ and $G_0/Z_0 \simeq Alt(5)$. Set $G = G_0Z (\subset GL(2, 29))$, where $Z = \langle \begin{bmatrix} 7 & 0 \\ 0 & 7 \end{bmatrix} \rangle \simeq \mathbb{Z}_7$. We can check that G acts regularly on \mathbb{P} and \mathbb{L} . For a point $(1, 0) \in \mathbb{P}$ and a line $\ell = \{1\} \times K$, we set $D = \{g \in G \mid (1, 0)g \in \ell\}$. Then $D = \{g \in G \mid (g)_{1,1} = 1\}$.

Let U_0 and U be the set of lower triangular matrices in G_0 and G , respectively. Since $K^* \simeq \mathbb{Z}_{28}$ and $7, 29 \nmid |G_0|$, we have $|U_0| \leq 4$. On the other hand, $x_3^{x_2x_1} = \begin{bmatrix} 17 & 0 \\ 21 & 12 \end{bmatrix} \in G_0$, hence $U_0 = \langle \begin{bmatrix} 17 & 0 \\ 21 & 12 \end{bmatrix} \rangle \simeq \mathbb{Z}_4$. Therefore $U = U_0Z \simeq \mathbb{Z}_{28}$. By a similar argument as in the case (I), we have the following.

Proposition 2.7 Let $G (\simeq SL(2, 5) \times \mathbb{Z}_7), U (\simeq \mathbb{Z}_{28})$ and $D (|D| = 29)$ be as above. Then D is an affine difference set of order 29 in G relative to U .

Set $M_k = \{g \in G_0 \mid (g)_{1,1} = k\}$ for $k \in K$. Then, as $7^7 \equiv 1 \pmod{29}$, $D = M_1 \cup 7^6M_7 \cup 7^5M_{7^2} \cup 7^4M_{7^3} \cup 7^3M_{7^4} \cup 7^2M_{7^5} \cup 7M_{7^6} (\subset GL(2, 29))$. We can check that

$$M_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 8 \\ 7 & 28 \end{bmatrix}, \begin{bmatrix} 1 & 6 \\ 20 & 5 \end{bmatrix}, \begin{bmatrix} 1 & 5 \\ 17 & 28 \end{bmatrix}, \begin{bmatrix} 1 & 27 \\ 13 & 4 \end{bmatrix} \right\}$$

$$= \{1, x_4^2, x_2^{x_1}, x_1x_2x_2^{x_1}x_4^3, -x_2x_2^{x_1}x_4^4, -x_1^2x_4^2\},$$

$$M_7 = \left\{ \begin{bmatrix} 7 & 3 \\ 10 & 21 \end{bmatrix}, \begin{bmatrix} 7 & 10 \\ 14 & 16 \end{bmatrix} \right\} = \{x_1x_2x_2^{x_1}x_4^2, -x_1^2x_2x_2^{x_1}x_4^3\},$$

$$M_{7^2} (= M_{20}) = \left\{ \begin{bmatrix} 20 & 1 \\ 5 & 9 \end{bmatrix}, \begin{bmatrix} 20 & 3 \\ 18 & 10 \end{bmatrix}, \begin{bmatrix} 20 & 22 \\ 27 & 8 \end{bmatrix}, \begin{bmatrix} 20 & 11 \\ 25 & 8 \end{bmatrix}, \begin{bmatrix} 20 & 17 \\ 10 & 10 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 20 & 16 \\ 13 & 9 \end{bmatrix} \right\} = \{x_2, x_1, -x_2^{x_1}x_4^3, -x_1x_4^4, -x_1x_2, -x_1^2x_4^3\},$$

$$M_{7^3} (= M_{24}) = \left\{ \begin{bmatrix} 24 & 6 \\ 20 & 28 \end{bmatrix}, \begin{bmatrix} 24 & 22 \\ 25 & 0 \end{bmatrix} \right\} = \{-x_1x_2x_4^2, -x_1^2x_4^4\},$$

$$\begin{aligned}
\mathbb{M}_{7^4} (= \mathbb{M}_{23}) &= \left\{ \begin{bmatrix} 23 & 24 \\ 3 & 12 \end{bmatrix}, \begin{bmatrix} 23 & 27 \\ 22 & 12 \end{bmatrix} \right\} = \{x_2x_4^2, x_1^2x_2^x x_4^2\}, \\
\mathbb{M}_{7^5} (= \mathbb{M}_{16}) &= \left\{ \begin{bmatrix} 16 & 28 \\ 18 & 8 \end{bmatrix}, \begin{bmatrix} 16 & 10 \\ 12 & 13 \end{bmatrix}, \begin{bmatrix} 16 & 19 \\ 15 & 7 \end{bmatrix}, \begin{bmatrix} 16 & 21 \\ 14 & 13 \end{bmatrix}, \begin{bmatrix} 16 & 17 \\ 16 & 8 \end{bmatrix} \right\} \\
&= \{x_1x_4, x_1x_2x_4^4, x_1x_2x_2^{x_1}x_4^4, -x_2x_2^{x_1}x_4, -x_1x_4^3\}, \\
\mathbb{M}_{7^6} (= \mathbb{M}_{25}) &= \left\{ \begin{bmatrix} 25 & 4 \\ 4 & 3 \end{bmatrix}, \begin{bmatrix} 25 & 27 \\ 13 & 28 \end{bmatrix}, \begin{bmatrix} 25 & 7 \\ 23 & 3 \end{bmatrix}, \begin{bmatrix} 25 & 1 \\ 3 & 28 \end{bmatrix}, \begin{bmatrix} 25 & 24 \\ 14 & 10 \end{bmatrix}, \right. \\
&\quad \left. \begin{bmatrix} 25 & 10 \\ 22 & 10 \end{bmatrix} \right\} = \{x_2^{x_1}x_4^2, x_1x_2^{x_1}x_4^4, x_1^2x_2x_2^{x_1}x_4^2, -x_4^3, -x_4^4, -x_1^2x_2^{x_1}x_4\}.
\end{aligned}$$

Set $D_1 = \bigcup_{0 \leq i \leq 6} \mathbb{M}_{7^i}$ ($\subset G_0$). Clearly $Z(G) = Z_0 \times Z \subset U$. Since $G/Z(G) = G_0Z(G)/Z(G) \simeq G_0/Z_0 \simeq \text{Alt}(5)$, $\mu(D_1)$ is a $(30, 2, 29, 14)$ -difference set in $\text{Alt}(5)$ relative to $\langle (2, 3)(4, 5) \rangle (= \langle \mu(x_3^{x_2^{x_1}}) \rangle)$ by Lemma 2.1 and Proposition 2.7. Set $\bar{D} = \mu(D_1)(1, 2)(3, 4)$. Then, by a similar way as in the proof of Proposition 2.5, we have the following.

Proposition 2.8 *Set $\bar{D} = \{(1, 2)(3, 4), (2, 4, 5), (3, 4, 5), (1, 3)(2, 5), (3, 5, 4), (2, 5, 4), (1, 2)(4, 5), (1, 3)(4, 5), (1, 3, 4, 2, 5), (1, 2, 5, 3, 4), (1, 2, 5, 4, 3), (1, 4, 3, 5, 2), (1, 3, 4, 5, 2), (1, 5, 2, 4, 3), (1, 5)(2, 4), (1, 4)(3, 5), (1, 5, 4), (1, 4, 5), (1, 3, 2, 4, 5), (1, 2, 3, 5, 4), (2, 4)(3, 5), (1, 4, 5, 3, 2), (1, 5, 4, 2, 3), (1, 4, 2), (1, 3, 5), (1, 2, 4), (1, 5, 3), (1, 4, 2, 3, 5), (1, 5, 3, 2, 4)\}$. Then \bar{D} is a $(30, 2, 29, 14)$ -difference set in $\text{Alt}(5)$ relative to $\bar{U} = \langle (2, 3)(4, 5) \rangle (\simeq \mathbb{Z}_2)$.*

Remark 2.9 *We have chosen a translate \bar{D} of $\mu(D_1)$ so that $\bar{D} \cap \bar{U} = \phi$, $\text{Alt}(5) = \bar{U}\bar{D} \cup \bar{U}$ and $\bar{D} = \bar{D}^{(-1)}$.*

In the rest of this paper we use the following notations.

Notation 2.10 *We assume that D is a (m, u, k, λ) -difference set in $G (= \text{Alt}(5))$ relative to a subgroup U of G , where $(m, u, k, \lambda) \in \{(12, 5, 11, 2), (20, 3, 19, 6), (30, 2, 29, 14)\}$. Exchanging D for Dx if necessary we may assume the following.*

$$U \cap D = \phi, \quad |Ux \cap D| = 1 \quad (\forall x \in G \setminus U) \quad (3)$$

We always regard G as a 3-transitive permutation group on $\Omega = \{1, 2, 3, 4, 5\}$. Let ρ be a natural isomorphism from G to the group of permutation matrices of size 5. Let $A = \sum_{d \in D} \rho(d)$ and set $A = (a_{ij})$. Let $G_{(i,j)}$ the set of elements of G such that $i^g = j$ for $i, j \in \Omega$. Denote by $J_{m,n}$ the $m \times n$ all one matrix. Set $I = I_5$ and $J = J_{5,5}$.

Lemma 2.11 *The following hold.*

- (i) $a_{ij} = |G_{(i,j)} \cap D|$ for $i, j \in \Omega$.
- (ii) $AA^T = kI + 12\lambda J - \lambda \cdot \rho(U)$.

(iii) $AJ = JA = kJ$.

Proof. By definition, (i) and (iii) are obvious. Since $DD^{(-1)} = k + \lambda(G - U)$, $\rho(D)\rho(D^{(-1)}) = kI + \lambda(\rho(G) - \rho(U))$. As $|G_{(i,j)}| = 12$, we have $\rho(G) = 12J$. On the other hand, as $\rho(g)$ is an orthogonal matrix for every $g \in G$, $A^T = \sum_{d \in D} \rho(d^{-1})$. Therefore (ii) holds.

3 Non-Existence of (20, 3, 19, 6)-difference set in $Alt(5)$

In order to prove our theorem, we first show that there is no (20, 3, 19, 6)-difference set in $G(= Alt(5))$. Suppose there exists a difference set D with such parameters relative to a subgroup $U \simeq \mathbb{Z}_3$ of G satisfying (3). We may assume that $U = \langle(3, 4, 5)\rangle$.

Lemma 3.1

$$AA^T = \begin{bmatrix} 73 & 72 & 72 & 72 & 72 \\ 72 & 73 & 72 & 72 & 72 \\ 72 & 72 & 85 & 66 & 66 \\ 72 & 72 & 66 & 85 & 66 \\ 72 & 72 & 66 & 66 & 85 \end{bmatrix}$$

Proof. As $U = \langle(3, 4, 5)\rangle$, $\rho(U) = \begin{bmatrix} 3I_2 & O \\ O & J_{3,3} \end{bmatrix}$. Applying Lemma 2.11(ii), we have the lemma.

Lemma 3.2 Set $A = \begin{bmatrix} P & Q \\ R & B \end{bmatrix}$, where P, Q, R and B are 2 by 2, 2 by 3, 3 by 2 and 3 by 3 matrices, respectively. Then the following hold.

$$(i) \quad P = \begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix}, \quad Q = \begin{bmatrix} 4 & 4 & 4 \\ 4 & 4 & 4 \end{bmatrix} \quad \text{and} \quad R = \begin{bmatrix} 4 & 4 \\ 4 & 4 \\ 4 & 4 \end{bmatrix}.$$

$$(ii) \quad B \text{ has a constant row and column sum of 11 and } BB^T = \begin{bmatrix} 53 & 34 & 34 \\ 34 & 53 & 34 \\ 34 & 34 & 53 \end{bmatrix}.$$

Proof. Set $H = G_1$, the stabilizer of 1. Then U is a subgroup of H . Let $j \in \Omega$ and f_j an element of G such that $1^{f_j} = j$. Then $G_{(1,j)} = Hf_j$. As $H \supset U$, Hf_j is a union of right cosets of U . Hence $a_{1,j} = |Hf_j \cap D| = 3$ or 4 according as $i = 1$ or $i \neq 1$ by (3) and Lemma 2.11(i). Similarly $a_{2,j} = 3$ or 4 according as $i = 2$ or $i \neq 2$. Thus $P = \begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix}$ and $Q = \begin{bmatrix} 4 & 4 & 4 \\ 4 & 4 & 4 \end{bmatrix}$.

Let $i \in \Omega \setminus \{1, 2\}$. By (3) and Lemma 3.1,

$$a_{i1} + a_{i2} + a_{i3} + a_{i4} + a_{i5} = 19 \quad (4)$$

$$3a_{i1} + 4a_{i2} + 4a_{i3} + 4a_{i4} + 4a_{i5} = 72 \quad (5)$$

$$4a_{i1} + 3a_{i2} + 4a_{i3} + 4a_{i4} + 4a_{i5} = 72 \quad (6)$$

From (5) and (6), $a_{i1} = a_{i2}$. This, together with (4), gives $a_{i1} = a_{i2} = 4$ and $a_{i3} + a_{i4} + a_{i5} = 11$. Applying Lemma 3.1 we have (i) and (ii).

Set $B = (b_{ij})$. By Lemma 3.2, we have $\{b_{i1}, b_{i2}, b_{i3}\} = \{b_{1j}, b_{2j}, b_{3j}\} = \{1, 4, 6\}$. Moreover, exchanging D for Dx for a suitable $x \in U$ if necessary, we may assume that $b_{1,1} = 1$ and that B is one of the following.

$$B_1 = \begin{bmatrix} 1 & 4 & 6 \\ 4 & 6 & 1 \\ 6 & 1 & 4 \end{bmatrix}, B_2 = \begin{bmatrix} 1 & 4 & 6 \\ 6 & 1 & 4 \\ 4 & 6 & 1 \end{bmatrix}, B_3 = \begin{bmatrix} 1 & 6 & 4 \\ 4 & 1 & 6 \\ 6 & 4 & 1 \end{bmatrix}, B_4 = \begin{bmatrix} 1 & 6 & 4 \\ 6 & 4 & 1 \\ 4 & 1 & 6 \end{bmatrix}.$$

Lemma 3.3 . We have either $A = A_1$ or A_2 up to equivalence, where

$$A_1 = \begin{bmatrix} 3 & 4 & 4 & 4 & 4 \\ 4 & 3 & 4 & 4 & 4 \\ 4 & 4 & 1 & 4 & 6 \\ 4 & 4 & 4 & 6 & 1 \\ 4 & 4 & 6 & 1 & 4 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 3 & 4 & 4 & 4 & 4 \\ 4 & 3 & 4 & 4 & 4 \\ 4 & 4 & 1 & 4 & 6 \\ 4 & 4 & 6 & 1 & 4 \\ 4 & 4 & 4 & 6 & 1 \end{bmatrix}$$

Proof. Let B_i ($1 \leq i \leq 4$) be as above. Set $P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$. Then $PB_1P = B_4$ and $PB_2P = B_3$. On the other hand, $Aut(G) = Sym(5) \triangleright G = Alt(5)$ and the normalizer of U in $Sym(5)$ is $\langle (4, 5) \rangle U$. Since $\rho((4, 5)) = \begin{bmatrix} I_2 & \\ & P \end{bmatrix}$, the lemma holds.

By Lemma 2.11(i) and Lemma 3.3, we have one of the following.

(CASE 1) $A = A_1$ and

$$|G_{(3,3)} \cap D| = |G_{(4,5)} \cap D| = |G_{(5,4)} \cap D| = 1 \quad (7)$$

(CASE 2) $A = A_2$ and

$$|G_{(3,3)} \cap D| = |G_{(4,4)} \cap D| = |G_{(5,5)} \cap D| = 1 \quad (8)$$

The steps for a computer search are as follows:

(STEP 1) Select one element from each coset $Ug (\neq U)$ and get a set of right coset representatives $D = \{r_1, r_2, \dots, r_{19}\}$ of size 19 using (7) or (8).

(STEP 2) Compute the summation $M = \sum_{1 \leq i \leq 19} \rho(r_i)$.

(STEP 3) If $M = A_1$ or A_2 , then check $DD^{(-1)} = 19 + 6(G - U)$.

Thus, we can verify the nonexistence of such a difference set D by a computer search.

4 A classification of relative difference sets in $Alt(5)$

In this section we determine all relative difference sets in $Alt(5)$. We use the notations defined in Notation 2.10.

(I) $(12, 5, 11, 2)$ -difference sets in $Alt(5)$:

The right coset decomposition of $Alt(5)$ by $U(= \langle (1, 2, 3, 4, 5) \rangle)$ is as follows:

$$\begin{aligned}
 Alt(5) &= U + U(3, 4, 5)U + U(3, 5, 4) + U(2, 3)(4, 5) + U(2, 3, 4) + U(2, 3, 5) + \\
 &U(2, 4, 3) + U(2, 4, 5) + U(2, 4)(3, 5) + U(2, 5, 3) + U(2, 5, 4) + U(2, 5)(3, 4), \text{ where} \\
 U &= \{e, (1, 2, 3, 4, 5), (1, 3, 5, 2, 4), (1, 4, 2, 5, 3), (1, 5, 4, 3, 2)\}, \\
 U(3, 4, 5) &= \{(3, 4, 5), (1, 2, 4, 3, 5), (1, 3, 2), (1, 4)(2, 5), (1, 5, 4, 2, 3)\} \\
 U(3, 5, 4) &= \{(3, 5, 4), (1, 2, 5), (1, 3)(2, 4), (1, 4, 5, 3, 2), (1, 5, 2, 3, 4)\}, \\
 U(2, 3)(4, 5) &= \{(2, 3)(4, 5), (1, 2, 5, 3, 4), (1, 3, 5), (1, 4, 2), (1, 5, 2, 4, 3)\}, \\
 U(2, 3, 4) &= \{(2, 3, 4), (1, 2, 5, 4, 3), (1, 3, 2, 4, 5), (1, 4)(3, 5), (1, 5, 2)\} \\
 U(2, 3, 5) &= \{(2, 3, 5), (1, 2)(4, 5), (1, 3, 4, 2, 5), (1, 4, 3), (1, 5, 3, 2, 4)\}, \\
 U(2, 4, 3) &= \{(2, 4, 3), (1, 2, 3, 5, 4), (1, 3)(2, 5), (1, 4, 5), (1, 5, 3, 4, 2)\}, \\
 U(2, 4, 5) &= \{(2, 4, 5), (1, 2)(3, 4), (1, 3, 2, 5, 4), (1, 4, 2, 3, 5), (1, 5, 3)\}, \\
 U(2, 4)(3, 5) &= \{(2, 4)(3, 5), (1, 2, 3), (1, 3, 4, 5, 2), (1, 4, 3, 2, 5), (1, 5, 4)\}, \\
 U(2, 5, 3) &= \{(2, 5, 3), (1, 2, 4), (1, 3, 5, 4, 2), (1, 4, 5, 2, 3), (1, 5)(3, 4)\}, \\
 U(2, 5, 4) &= \{(2, 5, 4), (1, 2, 4, 5, 3), (1, 3, 4), (1, 4, 3, 5, 2), (1, 5)(2, 3)\}, \\
 U(2, 5)(3, 4) &= \{(2, 5)(3, 4), (1, 2)(3, 5), (1, 3)(4, 5), (1, 4)(2, 3), (1, 5)(2, 4)\}.
 \end{aligned}$$

By a similar argument as in §3, we have

$$AA^T = \begin{bmatrix} 33 & 22 & 22 & 22 & 22 \\ 22 & 33 & 22 & 22 & 22 \\ 22 & 22 & 33 & 22 & 22 \\ 22 & 22 & 22 & 33 & 22 \\ 22 & 22 & 22 & 22 & 33 \end{bmatrix}.$$

Hence, the set of entries of each row of A is $\{0, 2, 2, 2, 3, 4\}$. Since U is transitive on Ω , we may assume that $a_{1,1} = 0$. It follows that

$$D \cap G_1 = \phi. \quad (9)$$

Using (9), we know that D is one of the following by a computer search.

- (i) $D_1 = \{(1, 2, 3, 4, 5), (1, 5, 4, 2, 3), (1, 4, 5, 3, 2), (1, 5, 2, 4, 3), (1, 2, 5, 4, 3), (1, 5, 3, 2, 4), (1, 5, 3, 4, 2), (1, 3, 2, 5, 4), (1, 4, 3, 2, 5), (1, 3, 5, 4, 2), (1, 4, 3, 5, 2)\}$,
- (ii) $D_2 = \{(1, 3, 5, 2, 4), (1, 5, 4, 2, 3), (1, 4, 5, 3, 2), (1, 2, 5, 3, 4), (1, 2, 5, 4, 3), (1, 3, 4, 2, 5), (1, 5, 3, 4, 2), (1, 4, 2, 3, 5), (1, 4, 3, 2, 5), (1, 4, 5, 2, 3), (1, 2, 4, 5, 3)\}$,
- (iii) $D_3 = \{(1, 4, 2, 5, 3), (1, 2, 4, 3, 5), (1, 5, 2, 3, 4), (1, 5, 2, 4, 3), (1, 3, 2, 4, 5), (1, 5, 3, 2, 4), (1, 2, 3, 5, 4), (1, 3, 2, 5, 4), (1, 3, 4, 5, 2), (1, 3, 5, 4, 2), (1, 4, 3, 5, 2)\}$,

(iv) $D_4 = \{(1, 5, 4, 3, 2), (1, 2, 4, 3, 5), (1, 5, 2, 3, 4), (1, 2, 5, 3, 4), (1, 3, 2, 4, 5), (1, 3, 4, 2, 5), (1, 2, 3, 5, 4), (1, 4, 2, 3, 5), (1, 3, 4, 5, 2), (1, 4, 5, 2, 3), (1, 2, 4, 5, 3)\}$.

Lemma 4.1 Every $(12, 5, 11, 2)$ -difference set in $Alt(5)$ is equivalent to \bar{D} defined in Proposition 2.5.

Proof. As we have shown above, any $(12, 5, 11, 2)$ -difference set in $Alt(5)$ is equivalent to D_i for some $i \in \{1, 2, 3, 4\}$. On the other hand we can verify that $D_1 = (\bar{D}(1, 4)(2, 3))^{(1, 2, 4, 3)}$, $D_2 = \bar{D}(1, 4)(2, 3)$, $D_3 = \bar{D}(1, 4)(2, 3)$, $D_4 = (\bar{D}(1, 4)(2, 3))^{(1, 3, 4, 2)}$. Thus the lemma holds.

(II) $(30, 2, 29, 14)$ -difference sets in $Alt(5)$:

Let D be a $(30, 2, 29, 14)$ -difference sets in $G(= Alt(5))$ relative to U . We may assume that $D \cap U = \phi$ and $U = \langle t \rangle$, where $t = (2, 3)(4, 5)$. Then the following holds.

Lemma 4.2 $a_{11} = 5$ and $a_{1j} = a_{i1} = 6$ for any $i, j \in \{2, 3, 4, 5\}$.

Proof. Set $H = G_1$, the stabilizer of 1. Choose $y_i \in G$ so that $1^{y_i} = i$ for $i \in \Omega \setminus \{1\}$ and set $y_1 = 1$. Then $G = Hy_1 + Hy_2 + Hy_3 + Hy_4 + Hy_5$. We note that Hy_j is the set of elements $x \in G$ such that $1^x = j$. Let $H = Uh_1 + Uh_2 + Uh_3 + Uh_4 + Uh_5 + Uh_6$ be the right coset decomposition of H by U , where $h_1 = 1$. Then $G = \bigcup_{1 \leq j \leq 5} \bigcup_{1 \leq i \leq 6} Uh_i y_j$. Since $|D \cap U| = 0$ and $|D \cap Ug| = 1$ if $Ug \neq U$, it follows that $|\bar{D} \cap Uh_i y_j| = 0$ if $i = j = 1$ and 0 otherwise. Hence

$$a_{1,j} = |D \cap Hy_j| = \begin{cases} 5 & \text{if } j = 1 \\ 6 & \text{if } j \neq 1. \end{cases} \quad (10)$$

By a similar argument as in §3, we have

$$AA^T = 29I + 14(12J - I - \rho(t)) = \begin{bmatrix} a & b & b & b & b \\ b & d & c & b & b \\ b & c & d & b & b \\ b & b & b & d & c \\ b & b & b & c & d \end{bmatrix}, \quad (11)$$

where $a = 169, b = 168, c = 154, d = 183$. Hence $a_{11}a_{i1} + a_{12}a_{i2} + a_{13}a_{i3} + a_{14}a_{i4} + a_{15}a_{i5} = 168$ for $i \neq 1$. Moreover $a_{i1} + a_{i2} + a_{i3} + a_{i4} + a_{i5} = 29$ by Lemma 2.11. By (10), we have $a_{i1} = 6$ for every $i \neq 1$. Thus the lemma holds.

Let $B = (a_{ij})_{2 \leq i, j \leq 5}$ be a 4 by 4 submatrix of A . By (11) and Lemma 4.2, we have

$$BB^T = \begin{bmatrix} 147 & 118 & 132 & 132 \\ 118 & 147 & 132 & 132 \\ 132 & 132 & 147 & 118 \\ 132 & 132 & 118 & 147 \end{bmatrix}. \quad (12)$$

By Lemma 4.2, B has a constant row sum of 23 and column sum of 23. Moreover, by (12) $a_{i2}^2 + a_{i3}^2 + a_{i4}^2 + a_{i5}^2 = 147$. Hence we can check that $\{a_{i2}, a_{i3}, a_{i4}, a_{i5}\} = \{3, 5, 7, 8\}$ or $\{4, 5, 5, 9\}$ for $i \in \{2, 3, 4, 5\}$ by a computer search. Moreover, we can easily check that $4x + 5y + 5z + 9u \notin \{118, 132\}$ when $\{x, y, z, u\} = \{4, 5, 5, 9\}$ or $\{3, 5, 7, 8\}$. Therefore

$$\{a_{i2}, a_{i3}, a_{i4}, a_{i5}\} = \{3, 5, 7, 8\} \quad \forall i \neq 1. \quad (13)$$

Since $G(= Alt(5))$ is 3-transitive on Ω , exchanging D for Dg for a suitable $g \in G$, we may assume that A has the following forms.

$$A = \begin{bmatrix} 5 & 6 & 6 & 6 & 6 \\ 6 & * & * & * & * \\ 6 & * & * & * & * \\ 6 & * & * & 3 & * \\ 6 & * & * & * & 3 \end{bmatrix}. \quad (14)$$

By (12), (13) and (14), B has one of the following form.

$$(i) \begin{bmatrix} * & * & 7 & 5 \\ * & * & 5 & 7 \\ * & * & 3 & 8 \\ * & * & 8 & 3 \end{bmatrix} \quad (ii) \begin{bmatrix} * & * & 5 & 7 \\ * & * & 7 & 5 \\ * & * & 3 & 8 \\ * & * & 8 & 3 \end{bmatrix}. \quad (15)$$

Exchanging D for D^t if necessary, we assume that B is of type (i). Therefore, by (12) and (13), B is one of the following.

$$B_1 = \begin{bmatrix} 8 & 3 & 7 & 5 \\ 3 & 8 & 5 & 7 \\ 7 & 5 & 3 & 8 \\ 5 & 7 & 8 & 3 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 3 & 8 & 7 & 5 \\ 8 & 3 & 5 & 7 \\ 5 & 7 & 3 & 8 \\ 7 & 5 & 8 & 3 \end{bmatrix}$$

Thus A is one of the following.

$$A_1 = \begin{bmatrix} 5 & 6J \\ 6J & B_1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 5 & 6J \\ 6J & B_2 \end{bmatrix} \quad (16)$$

The right coset decomposition of G by $U(= ((2, 3)(4, 5)))$ is as follows:

$$\begin{aligned} Alt(5) = & U + U(3, 4, 5) + U(3, 5, 4) + U(2, 3, 4) + U(2, 3, 5) + U(1, 3, 2) + \\ & U(1, 3, 4, 5, 2) + U(1, 3, 5, 4, 2) + U(1, 3, 4) + U(1, 3, 5) + U(1, 3, 5, 2, 4) + U(1, 2)(4, 5) + \\ & + U(1, 2, 3, 4, 5) + U(1, 2, 3, 5, 4) + U(1, 2)(3, 4) + U(1, 2)(3, 5) + U(1, 2, 4, 3, 5) + \\ & U(1, 5, 4, 3, 2) + U(1, 5, 2) + U(1, 5, 3, 4, 2) + U(1, 5, 4) + U(1, 5)(3, 4) + U(1, 5, 2, 3, 4) + \\ & U(1, 4, 5, 3, 2) + U(1, 4, 5) + U(1, 4)(3, 5) + U(1, 4, 2) + U(1, 4, 3, 5, 2) + U(1, 4, 2, 3, 5) + \\ & U(2, 4)(3, 5). \end{aligned}$$

The procedure of the computer search is as follows:

- (i) Select one element from each coset $Ug (\neq U)$ and get a set of right coset representatives $D = \{r_1, r_2, \dots, r_{29}\}$ of size 29.
- (ii) Compute the summation $M = \sum_{1 \leq i \leq 29} \rho(r_i)$.
- (iii) If $M = A_1$ or A_2 , then check $DD^{(-1)} = 29 + 14(G - U)$.

Thus we obtain the following two $(30, 2, 29, 14)$ -difference sets.

$$D_1 = \{(3, 4, 5), (3, 5, 4), (2, 4, 5), (2, 5, 4), (1, 3)(4, 5), (1, 3, 4, 5, 2), (1, 3)(2, 5), (1, 3, 2, 4, 5), (1, 3, 5), (1, 3, 4, 2, 5), (1, 2)(4, 5), (1, 2, 4), (1, 2, 3, 5, 4), (1, 2)(3, 4), (1, 2, 5, 4, 3), (1, 2, 5, 3, 4), (1, 5, 3), (1, 5, 4, 2, 3), (1, 5, 2, 4, 3), (1, 5, 4), (1, 5, 3, 2, 4), (1, 5)(2, 4), (1, 4, 5, 3, 2), (1, 4, 5), (1, 4)(3, 5), (1, 4, 2), (1, 4, 3, 5, 2), (1, 4, 2, 3, 5), (2, 4)(3, 5)\},$$

$$D_2 = \{(3, 4, 5), (3, 5, 4), (2, 4, 5), (2, 5, 4), (1, 3)(4, 5), (1, 3)(2, 4), (1, 3, 5, 4, 2), (1, 3, 2, 4, 5), (1, 3, 5), (1, 3, 4, 2, 5), (1, 2)(4, 5), (1, 2, 4), (1, 2, 3, 5, 4), (1, 2, 4, 5, 3), (1, 2)(3, 5), (1, 2, 5, 3, 4), (1, 5, 3), (1, 5, 4, 2, 3), (1, 5, 2, 4, 3), (1, 5, 4), (1, 5)(3, 4), (1, 5, 2, 3, 4), (1, 4, 5, 3, 2), (1, 4, 5), (1, 4, 3, 2, 5), (1, 4, 2), (1, 4, 3, 5, 2), (1, 4)(2, 5), (2, 4)(3, 5)\}.$$
 Thus we have

Lemma 4.3 Any $(30, 2, 29, 14)$ -difference set in $Alt(5)$ is equivalent to one of the following.

$$\{(3, 4, 5), (3, 5, 4), (2, 4, 5), (2, 5, 4), (1, 3)(4, 5), (1, 3, 4, 5, 2), (1, 3)(2, 5), (1, 3, 2, 4, 5), (1, 3, 5), (1, 3, 4, 2, 5), (1, 2)(4, 5), (1, 2, 4), (1, 2, 3, 5, 4), (1, 2)(3, 4), (1, 2, 5, 4, 3), (1, 2, 5, 3, 4), (1, 5, 3), (1, 5, 4, 2, 3), (1, 5, 2, 4, 3), (1, 5, 4), (1, 5, 3, 2, 4), (1, 5)(2, 4), (1, 4, 5, 3, 2), (1, 4, 5), (1, 4)(3, 5), (1, 4, 2), (1, 4, 3, 5, 2), (1, 4, 2, 3, 5), (2, 4)(3, 5)\}$$

Proof. Let D_1 and D_2 be as above. Then we can verify that $D_2 = (D_1(2, 3)(4, 5))^{(2, 4, 3, 5)}$. Thus the lemma holds.

We now prove our theorem.

Proof of Theorem

By Lemmas 4.1 and 4.3 we have the theorem.

Acknowledgement

The author thanks Agnes D. Garciano for her helpful comments and suggestions.

References

- [1] J.E.H. Elliot and A.T. Butson, Relative difference sets, *Ill. J. Math.* **10** (1968), 517-531.
- [2] B. Huppert, "Endliche Gruppen I," Springer-Verlag, Berlin, 1967.

- [3] N. Ito, Note on Hadamard groups of quadratic residue type, *Hokkaido Math. Jour.* **22** (1993), 373-378.
- [4] A. Pott, "Finite Geometry and Character Theory," Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995)

On the 2-dimensional dual hyper oval of the polar type in $PG(5, 4)$ and its automorphism group.

近畿大学・理工学部・理学科

中川 暢夫

Section1 序

有限体 $GF(q)$ 上の n 次元射影空間において、 $q^d + q^{d-1} + \dots + q + 2$ 個の d 次元部分空間から族で dual hyper oval と呼ばれるバランスに富んだ部分空間の族があり、近年吉荒、谷口、ヒュウブレヒト、デル・フラ等により盛んに研究されている ([1], [4], [5], [6], [7], [8])。これらの族は有限体の興味ある関数族とも深く関わっている。ここでは非退化計量ベクトル空間からくる射影空間において極大 isotropic space 上で dual hyper oval をなすものに注目し、4 元体上のユニタリー計量空間からくる、5 次元射影空間における dual hyper oval を構成し、その自己同型群を考察する。

この報告文の内容についてであるが、その事実だけはかの有名なアトラス ([2]) に書かれたいるが、構成法と自己同型群の計算はできていないのでそれらを明確にしたのであり、新しい結果が得られた訳ではない。

V を F_q 上の $n+1$ 次元ベクトル空間とし、 $PG(n, q)$ を V から得られる n 次元射影空間とする。

(定義)

$PG(n, q)$ の d 次元部分空間からなる部分空間の集合族 S が次の 4 つの条件を満たすとき、 S を $PG(n, q)$ の d 次元 dual hyper oval (D.H.O.) という。

(1): $\forall A, \forall B \in S$ に対し $A \cap B$ は射影点

(2): $A \cap B \cap C = \emptyset$

(3): $\langle A \mid A \in S \rangle = PG(n, q)$

(4): $|S| = \frac{q^{d+1}-1}{q-1} + 1$

射影平面 $PG(2, q)$ の hyper oval とは、 $q+2$ 個の射影点の集合で、そのうちのどの 3 点も同一直線上にない集合である。

(例)

$GF(4) = \{0, 1, \omega, \omega^2\}$ where $1 + \omega + \omega^2 = 0$

(ω^2 を $\bar{\omega}$ で表す。)

$[1, 0, 0], [0, 1, 0], [0, 0, 1], [1, 1, 1], [1, \omega, \bar{\omega}], [1, \bar{\omega}, \omega]$

は $GP(2, 4)$ における hyper oval である。

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \{[x, y, z] \mid ax + by + cz = 0\}$$

と定義すると、これは $PG(2, 4)$ の直線を表し、

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega \\ \omega^2 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega^2 \\ \omega \end{bmatrix} \right\}$$

は $PG(2, 4)$ における 1 次元 D.H.O である。

即ちこれらのどの 2 直線の共通部分も射影点であり、どの 3 直線の共通部分も空集合となる。

(定義)

$q = 2^e$ とする。 $GF(q)$ 上の permutation polynomial $f(x)$ が $f(0) = 0$ を満たし、

$f_s(x) = (f(x+s) - f(s))/x$ と定めた $f_s(x)$ がまた permutation polynomial になるとき、 $f(x)$ を弱 O-polynomial という。但し、 $f_s(0) = 0$ とする。

弱 O-polynomial $f(x)$ が更に $f(1) = 1$ を満たすとき、 $f(x)$ を O-polynomial と呼ぶ。

[定理 A][3]

$q = 2^e$ とする。 $PG(2, q)$ の中の任意の hyper oval O に対し、弱 O-polynomial $f(x)$ が存在して、

$$O = \{ [1, x, f(x)] \mid x \in GF(q) \} \cup \{ [0, 1, 0], [0, 0, 1] \}$$

が成り立つ。

もちろん、 $PG(2, q)$ の中の任意の dual hyper oval も弱 O-polynomial で表示される。

(例)

$GF(4)$ 上の O-polynomials は $f(x) = x^2$ で、 $GF(4)$ 上の弱 O-polynomials は $f(x) = x^2$, $f(x) = \omega x^2$, $f(x) = \omega^2 x^2$ である。

(弱 O-polynomials はこれらで尽きる。)

前述のように、 $GF(q)$, ($q = 2^e$) 上の hyper ovals は $GF(q)$ 上の O-polynomials で表されるが、 $GF(q)$ 上の O-polynomials はまだ分類されていない。従って、 $GF(q)$, ($q = 2^e$) 上の hyper ovals の分類問題も未解決である。また、regular hyper ovals とよばれる族は、 $GF(q)$ 上の 3 変数非退化 2 次形式から得られる。

(定義)

$V(n+1, q)$ を $GF(q)$ 上の計量空間とする (orthogonal, symplectic or unitary space with the nondegenerate bilinear form)。 $V(n+1, q)$ から得られる射影空間 $PG(n, q)$ において、 d -dimensional D.H.O.S で、 S の

各 member が maximal totally isotropic subspace になるような S を polar type D.H.O. と呼ぶ。

[定理 1](アトラス 39p)

unitary 型 polar space $PG(5, 4)$ において、polar type 2-dimensional D.H.O. S が存在し、 $Aut(S) \cong 3M_{22}$ が成り立つ。

アトラスの 29p には、[定理 1] の事実と S の表示のみが与えてある。ここでは、この S を構成し、 $M_{22} \leq Aut(S)$ であることを述べる。その前に、最近吉荒により明らかにされた、polar type D.H.O. の系列についての定理とこれからの課題を挙げておく。

[定理 2](Yoshiara)([7])

$d \geq 2$ で d は偶数とする。また、 $1 \leq h \leq d$ で、 $\gcd(h, d+1) = 1$ とする。 $PG(2d+1, 2)$ を直交プラス型 polar space とすると、 $PG(2d+1, 2)$ に d -dimensional polar type D.H.O. が存在する。

この定理は Yoshiara Families として以前から知られていた D.H.O. が、ある条件下で polar type D.H.O. として捉えられることを示したものである。

課題 1

$PG(2d+1, 2^e)$ において、[定理 1],[定理 2] 以外の polar type D.H.O. を構成せよ。

課題 2

q を奇素数とする。 $PG(2d+1, q)$ には、polar type の d -dimensional D.H.O. は存在しないことを示せ。

Section 2

unitary polar space $PG(5, 4)$ における polar type 2-dimensional D.H.O. S の構成

$PG(5, 4)$ を $V = V(6, 4)$ からくる non-degenerate unitary type polar space とする。 x と y の内積を (x, y) で表す。 S を $PG(5, 4)$ における 2-dimensional polar type D.H.O. とする。($|S| = 4^2 + 4 + 2 = 22$) $A \in S$ を一つ固定し、 $A = \langle e_0, e_1, e_2 \rangle$ とする。 $P \in \{A \text{ の射影点} \}$ に対し、 $A \cap B = \{P\}$ となる唯一つの S の member を $A[P]$ で表す。また、ベクトル v に対し、 $A[\langle v \rangle]$ を単に $A[v]$ とかく。すると、 $\{e_0, e_1, e_2\}$ に加えて、 V の basis $\{e_0, e_1, e_2, e_3, e_4, e_5\}$ が存在して、

$$A[e_0] = \langle e_0, e_3, e_4 \rangle, A[e_1] = \langle e_1, e_3, e_5 \rangle,$$

$$A \cap A[e_0] = \langle e_0 \rangle, A[e_0] \cap A[e_1] = \langle e_3 \rangle$$

が成り立つとしてよい。

また、必要なら、basis $\{e_0, e_1, e_2, e_3, e_4, e_5\}$ をうまく取り替えて、

$$(e_0, e_5) = 1, (e_1, e_4) = 1, (e_2, e_3) = 1, A[e_2] = \langle e_2, e_4, e_5 \rangle$$

が成立するようになれる。このとき、

$$\left(\sum_{i=0}^{i=5} x_i e_i, \sum_{j=0}^{j=5} y_j e_j \right) = \sum_{i=0}^{i=5} x_i \bar{y}_{5-i}$$

(ここで、 $\bar{x} = x^2$)

[補題 3]

A に含まれる projective line ℓ と $P \in \ell$ なる projective point P に対して、

$$\lambda(P) := \ell^\perp \cap A[P]$$

は projective line で、

$$\pi(\ell) := \langle \lambda(P) \mid P \in \ell \rangle$$

は projective plane である。更に、

$$O(\ell) := \{ \lambda(P) \mid P \in \ell \} \cup \{ \ell \}$$

は projective plane $\pi(\ell) (\cong PG(2, 4))$ の dual hyper oval をなす。

ここで以下で使用する記号の説明をする。 A の射影点 $P = [a_0 e_0 + a_1 e_1 + a_2 e_2]$ に対し、

$$\ell[a_0, a_1, a_2] := \{ x_0 e_0 + x_1 e_1 + x_2 e_2 \mid x_i \in \mathbb{F}_4, a_0 x_0 + a_1 x_1 + a_2 x_2 = 0 \}$$

と定め、 $\ell[a_0, a_1, a_2]$ を P の dual line と呼ぶ。

さて、 $\ell[0, 0, 1] = \langle e_0, e_1 \rangle$ について、[補題 3] を適用すると、 $\pi(\ell[0, 0, 1]) = \langle e_1, e_0, e_3 \rangle$ で、

$$O(\ell[0, 0, 1]) = \{ \ell[0, 0, 1]^\perp \cap A[P] \mid P \in \ell[0, 0, 1] \} \cup \{ \ell[0, 0, 1] \}$$

は $\langle e_1, e_0, e_3 \rangle$ において、dual hyper oval をなす。故に、[定理 A] により、 $f(t) = t^2$ について、

$$O(\ell[0, 0, 1]) = \{ L[1, t, f(t)] \mid t \in \mathbb{F}_4 \} \cup \{ L[0, 1, 0], L[0, 0, 1] \}$$

となる。ここで、 $L[0, 1, 0] = \langle e_1, e_3 \rangle$, $L[0, 0, 1] = \langle e_1, e_0 \rangle$ 。また、

$$L[1, t, f(t)] := \langle x_1 e_1 + x_0 e_0 + x_3 e_3 \mid x_1 + t x_0 + f(t) x_3 = 0 \rangle$$

である。

今、 $t = 1, \omega, \bar{\omega}$ の各々に対し、projective point $[t e_1 + e_0] \in \ell[0, 0, 1]$ に注目すると、 $[t e_1 + e_0] \in L[1, t, f(t)]$ より、

$$L[1, t, f(t)] = \ell[0, 0, 1]^\perp \cap A[t e_1 + e_0]$$

であるが、 $[f(t)e_1 + e_3] \in L[1, t, f(t)]$ より、

$$[f(t)e_1 + e_3] \in A[te_1 + e_0] \quad \text{where } t = 1, \omega, \bar{\omega}$$

一方、

$$A[te_1 + e_0] \cap A[e_2] = [te_1 + e_0]^\perp \cap \langle e_2, e_4, e_5 \rangle = \langle e_2, e_4 + \bar{t}e_5 \rangle$$

従って、適当な α に対して、

$$A[te_1 + e_0] = \langle te_1 + e_0, f(t)e_1 + e_3, \alpha e_2 + e_4 + \bar{t}e_5 \rangle.$$

更に、 $(f(t)e_1 + e_3, \alpha e_2 + e_4 + \bar{t}e_5) = 0$ だから、 $\alpha = \bar{f}(t)$ が得られる。このようにして、 $t = 1$ に対し、

$$A[e_1 + e_0] = \langle e_1 + e_0, e_1 + e_3, e_2 + e_4 + e_5 \rangle,$$

$t = \omega$ に対し、

$$A[\omega e_1 + e_0] = \langle \omega e_1 + e_0, \bar{\omega} e_1 + e_3, \omega e_2 + e_4 + \bar{\omega} e_5 \rangle,$$

$t = \bar{\omega}$ に対し、

$$A[\bar{\omega} e_1 + e_0] = \langle \bar{\omega} e_1 + e_0, \omega e_1 + e_3, \bar{\omega} e_2 + e_4 + \omega e_5 \rangle$$

となることがわかる。

ここで、 $(e_0, e_2, e_1)(e_3, e_4, e_5)$ なる置換を施すと、 $\ell[0, 0, 1] \rightarrow \ell[0, 1, 0]$ となり、上と同じ議論を繰り返す。 $g(t) = t^2$ および 射影平面 $\pi(\ell[0, 1, 0]) = \langle e_0, e_2, e_4 \rangle$ における basis $\{e_0, e_2, e_4\}$ に対して、

$$O(\ell[0, 1, 0]) = \{L[1, t, g(t)] \mid t \in \mathbb{F}_4\} \cup \{L[0, 1, 0], L[0, 0, 1]\}.$$

従って、

$$A[te_0 + e_2] = \langle te_0 + e_2, g(t)e_0 + e_4, \bar{g}(t)e_1 + e_5 + \bar{t}e_3 \rangle.$$

故に、 $t = 1$ に対し、

$$A[e_0 + e_2] = \langle e_0 + e_2, e_0 + e_4, e_1 + e_5 + e_3 \rangle,$$

$t = \omega$ に対し、

$$A[\omega e_0 + e_2] = \langle \omega e_0 + e_2, \bar{\omega} e_0 + e_4, \omega e_1 + e_5 + \bar{\omega} e_3 \rangle,$$

$t = \bar{\omega}$ に対し、

$$A[\bar{\omega} e_0 + e_2] = \langle \bar{\omega} e_0 + e_2, \omega e_0 + e_4, \bar{\omega} e_1 + e_5 + \omega e_3 \rangle$$

となることがわかる。

更に、もとの射影空間 V に $(e_0, e_1, e_2)(e_3, e_5, e_4)$ なる置換を施すと、 $\ell[0, 0, 1] \rightarrow \ell[1, 0, 0]$ となり、再び上と同じ議論を繰り返す。 $h(t) = t^2$ および 射影平面 $\pi(\ell[1, 0, 0]) = \langle e_2, e_1, e_5 \rangle$ における basis $\{e_2, e_1, e_5\}$ に対して、

$$O(\ell[1, 0, 0]) = \{L[1, t, h(t)] \mid t \in \mathbb{F}_4\} \cup \{L[0, 1, 0], L[0, 0, 1]\}.$$

従って、

$$A[te_2 + e_1] = \langle te_2 + e_1, h(t)e_2 + e_5, \bar{h}(t)e_0 + e_3 + \bar{t}e_4 \rangle.$$

故に、 $t = 1$ に対し、

$$A[e_2 + e_1] = \langle e_2 + e_1, e_2 + e_5, e_0 + e_3 + e_4 \rangle,$$

$t = \omega$ に対し、

$$A[\omega e_2 + e_1] = \langle \omega e_2 + e_1, \bar{\omega} e_2 + e_5, \omega e_0 + e_3 + \bar{\omega} e_4 \rangle,$$

$t = \bar{\omega}$ に対し、

$$A[\bar{\omega} e_2 + e_1] = \langle \bar{\omega} e_2 + e_1, \omega e_2 + e_5, \bar{\omega} e_0 + e_3 + \omega e_4 \rangle$$

となることがわかる。これで、22個の S の members のうち 13個の members が構成できた。

[コメント]

weakly O -polynomials g, h のとり方として、各々 $g(t) = t^2, h(t) = t^2$ を含め 3通りあり、全部で 9通りの場合が考えられ、 $g(t) = t^2, h(t) = t^2$ の場合はそのうちの一つの場合に過ぎない。しかし、残りの 8通りの場合もこれから構成する S と同型な D.H.O. になるもと予想しているが、これについては現在計算中である。

S の残り 9個の members は次のように定まってくる。

例えば、 $[e_0 + e_1 + e_2]$ について、

$$A[e_0] \cap A[e_0 + e_1 + e_2] = [\alpha e_0 + \beta e_3 + \gamma e_4]$$

と置くと、 $(e_0 + e_1 + e_2, \alpha e_0 + \beta e_3 + \gamma e_4) = 0$ だから、 $\beta = \gamma (\neq 0)$ がでる。更に、

$$A[e_1] \cap A[e_0 + e_1 + e_2] = [a e_1 + b e_3 + c e_5]$$

と置くと、 $(e_0 + e_1 + e_2, a e_1 + b e_3 + c e_5) = 0$ だから、 $b = c (\neq 0)$ がでる。故に、適当な α, a に対し、

$$A[e_0 + e_1 + e_2] = \langle e_0 + e_1 + e_2, \alpha e_0 + e_3 + e_4, a e_1 + e_3 + e_5 \rangle$$

となる。しかも、 $(\alpha e_0 + e_3 + e_4, a e_1 + e_3 + e_5) = 0$ となることより、 $\alpha = \bar{a}$ である。また、 $A[e_2] = \langle e_2, e_4, e_5 \rangle$ であり、

$$A[e_2] \cap A[e_0 + e_1 + e_2] = t(e_0 + e_1 + e_2) + (\bar{a} e_0 + e_3 + e_4) + (a e_1 + e_3 + e_5)$$

とかけることより、 $t = \bar{a}, t = a$ となり、 $a = 0$ または $a = 1$ でなければならない。更に、

$$A[\omega e_1 + e_0] \cap A[e_0 + e_1 + e_2] = \alpha(\omega e_1 + e_0) + \beta(\bar{\omega} e_1 + e_3) + \gamma(\omega e_2 + e_4 + \bar{\omega} e_5) =$$

$$\alpha'(e_0 + e_1 + e_2) + \beta'(a e_0 + e_3 + e_4) + \gamma'(a e_1 + e_3 + e_5)$$

に注意して、各 e_j ($j = 0, 1, 2, 3, 4, 5$) の係数を比較すれば、 $a = 0$ が導かれる。このように、

$$A[e_0 + e_1 + e_2] = \langle e_0 + e_1 + e_2, e_3 + e_4, e_3 + e_5 \rangle$$

であることが示された。

同様な考察を行うことにより、

$$\begin{aligned}
 A[e_0 + e_1 + we_2] &= \langle e_0 + e_1 + we_2, e_0 + we_3 + e_4, e_1 + we_3 + e_5 \rangle, \\
 A[e_0 + e_1 + \bar{w}e_2] &= \langle e_0 + e_1 + \bar{w}e_2, e_0 + \bar{w}e_3 + e_4, e_1 + \bar{w}e_3 + e_5 \rangle, \\
 A[e_0 + we_1 + e_2] &= \langle e_0 + we_1 + e_2, \bar{w}e_0 + \bar{w}e_3 + e_4, we_1 + e_3 + e_5 \rangle, \\
 A[e_0 + we_1 + we_2] &= \langle e_0 + we_1 + we_2, \bar{w}e_0 + e_3 + e_4, we_1 + we_3 + e_5 \rangle, \\
 A[e_0 + we_1 + \bar{w}e_2] &= \langle e_0 + we_1 + \bar{w}e_2, we_3 + e_4, \bar{w}e_3 + e_5 \rangle, \\
 A[e_0 + \bar{w}e_1 + e_2] &= \langle e_0 + \bar{w}e_1 + e_2, we_0 + we_3 + e_4, \bar{w}e_1 + e_3 + e_5 \rangle, \\
 A[e_0 + \bar{w}e_1 + we_2] &= \langle e_0 + \bar{w}e_1 + we_2, \bar{w}e_3 + e_4, we_3 + e_5 \rangle, \\
 A[e_0 + \bar{w}e_1 + \bar{w}e_2] &= \langle e_0 + \bar{w}e_1 + \bar{w}e_2, we_0 + e_3 + e_4, \bar{w}e_1 + \bar{w}e_3 + e_5 \rangle,
 \end{aligned}$$

以上で S の 22 個の members がすべて構成された。

Section 3 D.H.O.S の自己同型群

S の members を次の配列で考え、この配列を固定する。

$$S =$$

x	x	A	$A[e_0 + e_1 + e_2]$	$A[e_0 + we_1 + \bar{w}e_2]$	$A[e_0 + \bar{w}e_1 + we_2]$
$A[\bar{w}e_0 + e_1 + e_2]$	$A[we_0 + e_1 + e_2]$	$A[e_0]$	$A[e_1 + e_2]$	$A[e_1 + we_2]$	$A[e_1 + \bar{w}e_2]$
$A[e_0 + \bar{w}e_1 + e_2]$	$A[e_0 + we_1 + e_2]$	$A[e_1]$	$A[e_0 + e_2]$	$A[we_0 + e_2]$	$A[\bar{w}e_0 + e_2]$
$A[e_0 + e_1 + \bar{w}e_2]$	$A[e_0 + e_1 + we_2]$	$A[e_2]$	$A[e_0 + e_1]$	$A[e_0 + we_1]$	$A[e_0 + \bar{w}e_1]$

$Aut(S)$ の生成元の行列表現および S 上の置換は以下ようになる。

(●がついた元は、考えている S の自己同型 φ で固定される元 (member) である。)

$$\varphi(e_0, e_5, e_1, e_4, e_2, e_3) = (e_0, e_5, e_1, e_4, e_2, e_3)A_\varphi$$

ここで、 A_φ は \mathbb{F}_4 上の 6×6 行列である。

$(e_0, e_2, e_1)(e_3, e_4, e_5)$ を σ とすると、

$$\sigma = \left(\begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \right),$$

x	x	7 ●	11 ●	15 ●	19 ●
1	4	8	12	16	20
2	5	9	13	17	21
3	6	10	14	18	22

$$\sigma = (1,3,2)(4,6,5)(8,10,9)(12,14,13)(16,18,17)(20,22,21)$$

$$\tau_1 = (e_0, e_5)(e_1, e_4),$$

$$\tau_1 = \left(\begin{array}{c} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

x	x	7	11	15	19
1 ●	4 ●	8	12	16	20
2 ●	5 ●	9	13	17	21
3 ●	6 ●	10	14	18	22

$$\tau_1 = (7,10)(8,9)(11,14)(12,13)(15,18)(16,17)(19,22)(20,21)$$

$$\tau_2 = (e_0, e_5)(e_2, e_3),$$

$$\tau_2 = \left(\begin{array}{c} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array} \right),$$

x	x	7	11	15	19
1 ●	4 ●	8	12	16	20
2 ●	5 ●	9	13	17	21
3 ●	6 ●	10	14	18	22

$$\tau_2 = (7,9)(8,10)(11,13)(12,14)(15,17)(16,18)(19,21)(20,22)$$

$$\tau_3 = \left(\begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \end{array} \begin{array}{c} \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

x	x	7	11	15	19
1 ●	4 ●	8	12	16	20
2 ●	5 ●	9	13	17	21
3 ●	6 ●	10	14	18	22

$$\tau_3 = (7,11)(8,12)(9,13)(10,14)(15,19)(16,20)(17,21)(18,22)$$

$$\tau_4 = \left(\begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} \omega & \omega \\ \omega & \omega \end{pmatrix} \\ \begin{pmatrix} \bar{\omega} & \bar{\omega} \\ \bar{\omega} & \bar{\omega} \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} \bar{\omega} & \bar{\omega} \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ \omega & \omega \end{pmatrix} \\ \begin{pmatrix} \omega & \omega \\ \omega & \omega \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} \omega & \omega \\ \bar{\omega} & \bar{\omega} \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} \omega & \omega \\ \bar{\omega} & \bar{\omega} \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} \omega & \omega \\ \bar{\omega} & \bar{\omega} \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

x	x	7	11	15	19
1 ●	4 ●	8	12	16	20
2 ●	5 ●	9	13	17	21
3 ●	6 ●	10	14	18	22

$$\tau_4 = (7, 15)(8, 16)(9, 17)(10, 18)(11, 19)(12, 20)(13, 21)(14, 22)$$

$$P := \langle \tau_1, \tau_2, \tau_3, \tau_4 \rangle \cong (\mathbb{Z}_2)^4$$

$$\rho_1 = (e_1, e_2)(e_3, e_4),$$

$$\rho_1 = \left(\begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \right),$$

x	x	7 ●	11 ●	15	19
1 ●	4 ●	8 ●	12 ●	16	20
2	5	9	13	17	21
3	6	10	14	18	22

$$\rho_1 = (2, 3)(5, 6)(9, 10)(13, 14)(15, 19)(16, 20)(17, 22)(18, 21)$$

$$\rho_2 = \left(\begin{array}{c} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \right),$$

x	x	7 ●	11 ●	15	19
1 ●	4 ●	8 ●	12 ●	16	20
2	5	9	13	17	21
3	6	10	14	18	22

$$\rho_2 = (2, 5)(3, 6)(9, 13)(10, 14)(15, 20)(16, 19)(17, 18)(21, 22)$$

$$\rho_3 = \left(\begin{array}{c} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & \omega \\ 0 & \omega \end{pmatrix} \\ \begin{pmatrix} 0 & \omega \\ 0 & \omega \end{pmatrix} \\ \begin{pmatrix} 0 & \omega \\ 0 & \omega \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} \bar{\omega} & \bar{\omega} \\ \omega & 0 \end{pmatrix} \\ \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix} \\ \begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix} \\ \begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix} \end{array} \right) \left(\begin{array}{c} \begin{pmatrix} \bar{\omega} & \bar{\omega} \\ \omega & 0 \end{pmatrix} \\ \begin{pmatrix} \bar{\omega} & 0 \\ \omega & 0 \end{pmatrix} \\ \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix} \\ \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix} \end{array} \right),$$

x	x	7 ●	11 ●	15	19
1 ●	4 ●	8 ●	12 ●	16	20
2	5	9	13	17	21
3	6	10	14	18	22

$$\rho_3 = (2, 9)(3, 10)(5, 13)(6, 14)(15, 22)(16, 18)(17, 19)(20, 21)$$

$$\rho_4 = \left(\begin{array}{c} \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 0 & \omega \\ 0 & \bar{\omega} \\ 0 & \omega \\ 0 & \bar{\omega} \end{pmatrix} \\ \begin{pmatrix} \omega & \bar{\omega} \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} \omega & \bar{\omega} \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

×	×	7 ●	11 ●	15	19
1 ●	4 ●	8 ●	12 ●	16	20
2	5	9	13	17	21
3	6	10	14	18	22

$$\rho_4 = (2, 15)(3, 19)(5, 20)(6, 16)(9, 22)(10, 17)(13, 21)(14, 18)$$

$$Q := \langle \rho_1, \rho_2, \rho_3, \rho_4 \rangle \cong (\mathbb{Z}_2)^4$$

$$\zeta_1 = (e_0, e_1)(e_5, e_4),$$

$$\zeta_1 = \left(\begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

×	×	7 ●	11 ●	15	19
1	4	8	12	16	20
2	5	9	13	17	21
3 ●	6 ●	10 ●	14 ●	18	22

$$\zeta_1 = (1, 2)(4, 5)(8, 9)(12, 13)(15, 19)(16, 21)(17, 20)(18, 22)$$

$$\zeta_2 = \left(\begin{array}{c} \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

×	×	7 ●	11 ●	15	19
1	4	8	12	16	20
2	5	9	13	17	21
3 ●	6 ●	10 ●	14 ●	18	22

$$\zeta_2 = (1, 4)(2, 5)(8, 12)(9, 13)(15, 22)(16, 17)(18, 19)(20, 21)$$

$$\zeta_3 = \left(\begin{array}{c} \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \\ \bar{\omega} & 0 \\ 0 & \omega \\ \omega & \bar{\omega} \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} \bar{\omega} & 0 \\ \omega & 0 \\ 0 & \bar{\omega} \\ \bar{\omega} & \bar{\omega} \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & \omega \\ 0 & \omega \\ 0 & \omega \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

×	×	7 ●	11 ●	15	19
1	4	8	12	16	20
2	5	9	13	17	21
3 ●	6 ●	10 ●	14 ●	18	22

$$\zeta_3 = (1, 8)(2, 9)(4, 12)(5, 13)(15, 21)(16, 19)(17, 18)(20, 22)$$

$$\zeta_4 = \left(\begin{array}{ccc} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & \omega \\ 0 & \bar{\omega} \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & \omega \\ 0 & \bar{\omega} \end{pmatrix} \\ \begin{pmatrix} \omega & \bar{\omega} \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} \omega & \bar{\omega} \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array} \right),$$

x	x	7 ●	11 ●	15	19
1	4	8	12	16	20
2	5	9	13	17	21
3 ●	6 ●	10 ●	14 ●	18	22

$$\zeta_4 = (1, 15)(2, 19)(4, 22)(5, 18)(8, 21)(9, 16)(12, 20)(13, 17)$$

$$R := \langle \zeta_1, \zeta_2, \zeta_3, \zeta_4 \rangle \cong (\mathbb{Z}_2)^4$$

$$z = \left(\begin{array}{ccc} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} \bar{\omega} & 0 \\ 0 & \bar{\omega} \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array} \right),$$

x	x	7 ●	11	15	19 ●
1 ●	4	8	12	16	20
2	5	9 ●	13	17	21 ●
3	6 ●	10	14	18	22

$$z = (2, 3)(4, 5)(8, 10)(11, 15)(12, 18)(13, 17)(14, 16)(20, 22)$$

$G = \langle P, Q, R, \sigma, z \rangle$ と置くと G は $\text{Aut}(S)$ の部分群で、 G は S 上に 3 重可移に作用することは容易に示される。また、 G の S 上の作用で、3 点の固定群は $3 \cdot (\mathbb{Z}_2)^4$ と同型な群になることより、 G は M_{22} を含むことがわかる。

参考文献

[1] A. Del Fra, On d-dimensional dual hyperovals, *Geom. Dedicata*, 79(2000), 157-178.

[2] J.H. Conway, R. T. Curtis, S.P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of FINITE GROUPS*, Clarendon Press, Oxford, 1985.

- [3] I.W.P.Hirschfeld, *Projective Geometries over Finite Fields*, 2nd edn, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1998.
- [4] H.Taniguchi, A family of dual hyperovals over $GF(q)$ with q even, preprint, 2003.
- [5] H.Taniguchi, A note on the automorphism of $\mathcal{T}_\sigma(V)$, preprint, 2003.
- [6] S.Yoshiara, A remark on 2-dimensional dual hyperovals of polar type, Nov.8, 2003, the talk on Nov.8.2003 at Hitotubashi University.
- [7] S.Yoshiara, Some remarks on dimensional dual hyperovals of polar type, preprint, 2004.
- [8] S.Yoshiara, A family of d -dimensional dual hyperovals in $PG(2d+1, 2)$, *Europ.J.Combin.*, 20(1999), 589-603.

極空間中の双対弧 (Dimensional dual arcs of polar type)

吉荒 聡

Satoshi Yoshiara

東京女子大学 文理学部 数理学科

この原稿は2004年6月28日に信州大学理学部で行われた筆者の講演の大筋を再現し、多少の細部を付加したものです。

1. 「高次元の超卵形」の発生にまつわるお話

まず、高次元の双対弧、超卵形という概念の誕生について簡単に触れたい。¹ 1996年頃、筆者は非古典的な一般四辺形の円周拡大²の純幾何学的な構成を考えていた。5次元の射影空間の平面の族が(射影平面上の超卵形を拡張した)ある交叉性を満たすとき、そのアフィン拡大としてこのような幾何が可能であることに気が付き、このような族(Y-族)を Veronesean map を用いて与えた。一方、類似の交叉性を満たす対象として、マシュー群に関連した22枚の平面が散在型の単純群 J_4 の位数2の元の中心化群の中に存在することを知っていた。当時の私の関心は主に Y-族がこの22枚の平面に拡張できるかという点にあった³が、1996年9月のシエナでの共同研究の相手であった A.Pasini は、後者の交叉性に関する条件が、射影平面中の古典的な(双対)超卵形の高次元版であると見抜いた。彼はもう一人の共同研究の相手である C.Huybrechts と共に、この部分空間族の満たす交叉性を「高次元の双対超卵形」として定式化し、そのアフィン拡大として生じる幾何の特徴付け問題に関する幾つかの結果を得た [HP]。そこにおける高次元の超卵形の定義は、第2章で述べる形とは多少違っている。当時から、私には「高次元の双対弧の最大族」として、高次元の双対超卵形を定義するという方が自然に思っていたが、この考えはかなり後になって Y-族に関する論文の中に発表された [Yo2]。

高次元の双対超卵形という概念はすぐに受け入れられ、1998年頃には B.Cooperstein と J.Thas が、その特別な場合(生成空間の次元が最も小さい場合)に関する一種の特徴付けを与えている [CT]。ほぼ同時期に、私も生成空間の次元がその次に小さく、二重可移な自己同型群を持つような双対超卵形の族の構成法を思いついている [Yo1]。また Pasini から直接多くを学ぶ機会を得た A.Del Fra は高次元の双対超卵形に対する基本的事項に関して2000年に重要な論文を発表した [DF]。ここで提起された生成空間の最大値問題は、2002年に私によってほぼ best possible な形に解決され [Yo3]、その後すぐに、最大値を与える双対

¹ 完全を期したものではないし、私の個人的思いこみによる誤りもあるだろうが、5月のベルギーでの集会において A.Pasini と話した際に、おおむねこのようないきさつであったと確認済みである。

² 点と線と面という三種類の対象を持つ結合幾何で、その一点、一線、一面の剰余構造が、それぞれ一般四辺形、二辺形、円周幾何であるようなもの。

³ その後、拡張できることがわかった。論文 [Yo2, p.109] の定義の後の解説参照。

超卵形はある種の制限の元に Veronesean 曲面に限るという結果 (射影平面中の Segre の定理に相当する特徴付け) が J.Thas と H. van Maldeghem によって得られている [TV1, TV2] が、この結果にはまだ改良の余地があると思われる。標数 $q = 2$ の高次元の双対超卵形から、そのアフィン化として semiplanes という幾何学的対象や、その共線グラフとして距離正則グラフなども得られるが、これらについては論文 [Hu, PY1, PY2] などがある。

本稿では、私が最近提唱している極型の双対超卵形について、幾つかの基本的結果を述べたい。また、一般の双対超卵形の自己同型群に関して非常に重要な観察を与える。

2. 古典的モデルとその高次元への拡張

2.1 射影空間における弧・卵形・超卵形 射影平面 $PG(2, q)$ 上の射影点の集合 A が弧であるとは、どのような射影直線 l に対しても、 l 上にあるような A の点が 2 個以下であることであつた: $|l \cap A| \leq 2$ 。

$|A| = k + 1$ とおき、 A 上の一点 P を固定すると、 $A \setminus \{P\}$ から点 P を通る線の集合 $\mathcal{L}(P)$ 上への写像 ρ が $\rho(Q) := P, Q$ を結ぶ直線 と定義することにより得られる。上の性質から、この写像は単射であるから $|A| - 1 \leq q + 1 = |\mathcal{L}(P)|$, つまり $|A| \leq q + 2$ を得る。ここで等号が成立する場合を考えると、 A 上のどの点 P についても、 P を通る直線は必ず A の他の点と交わることがわかる。すなわち射影直線は A と 0 または 2 点で交わる。弧 A の外にある定定点を通して A と非自明に交わる直線を考えれば、 $q + 2 = |A|$ は 2 の倍数となる。まとめると、

$PG(2, q)$ 中の弧 A に対して、 q が奇数ならば $|A| \leq q + 1$ であり、
 q が偶数ならば $|A| \leq q + 2$ である。

$|A| = q + 1$ (resp. $q + 2$) である弧 A のことを卵形 (oval) (resp. 超卵形 (hyperoval)) と呼んだ。

q が奇数の時、1955年頃セグレによって次の美しい定理が示された。 q が奇数ならば、卵形はある非特異な二次形式の零点集合に一致する。 q が偶数の場合、セグレの定理の類似を求める試行の中から、有限体上の整数論 (0-多項式, clan, herd などの置換多項式論) や組合せ幾何 (ある種の一般四辺形, translation planes など) との強い結びつきが発見されて、今でも多くの研究がなされている。

前節で述べたように、この概念を高次元に拡張する試みを一つの動機として、高次元の双対弧、双対超卵形等の概念が生まれたのである。上の古典的な弧、超卵形そのものよりも、その双対のほうが高次元に拡張しやすい。ここで、射影平面中の双対弧とは、射影直線の集合で、どの相異なる 3 線も一点を共有しないものであることに注意しよう。

2.2 高次元の弧・超卵形 V を有限体 $GF(q)$ 上の $n+1$ 次元ベクトル空間とする。 V に付随する射影空間 $PG(V) \cong PG(n, q)$ の d (射影)次元部分空間の族 \mathcal{A} が $PG(n, q)$ 中の d 次元の双対弧であるとは、次の3つの公理を満たすことである。

- (DA1) \mathcal{A} のどの相異なる二つのメンバーの共通部分も射影点である。
 (DA2) \mathcal{A} のどの相異なる三つのメンバーの共通部分も空な射影集合 (V の部分ベクトル空間としては零空間) である。
 (DA3) \mathcal{A} のメンバーの全体は $PG(n, q)$ を生成する。

$PG(n, q)$ またはそれを与えるベクトル空間 V のことを双対弧の生成空間 (ambient space) と呼ぶことがある。

$PG(n, q)$ 中の d 次元の弧 \mathcal{A} から一つのメンバー X をとる。条件 (DA1) により、集合 $\mathcal{A} \setminus \{X\}$ から X 上の射影点の集合 $PG(X)$ への写像 ρ を $\rho(Y) := X \cap Y$ により定めることが出来て、条件 (DA2) によりこの写像は単射である。従って $|\mathcal{A}| \leq \theta_q(d) + 1$ という評価式を得る。ここで $\theta_q(d) = X$ 上の射影点の数 $= 1 + q + \dots + q^d = (q^{d+1} - 1)/(q - 1)$ 。

$|\mathcal{A}| = \theta_q(d) + 1$ を満たす $PG(n, q)$ 中の d 次元双対弧 \mathcal{A} のことを、 $PG(n, q)$ 中の d 次元双対超卵形と呼ぶ。

2.3 コメント (1) $d = 1$ に対する $PG(n, q)$ 中の1次元双対超卵形という概念は ($n = 2$ となるのがわかるので)、射影平面における双対超卵形という概念に他ならない。特に、このときには q は偶数である。

(2) \mathcal{S} が $PG(n, q)$ 中の d 次元の双対超卵形であれば、どのメンバー上の点も $X \cap Y$ ($X \neq Y \in \mathcal{S}$) の形に書ける。従って $PG(n, q)$ の任意の点は、0個または2個のメンバーに含まれる。Huybrechts と Pasini による双対超卵形の定義は、条件 (DA1), (DA3) とこの条件を仮定するものであった。

2.4 基本的未解決問題 (1) 古典的な場合 ($d = 1$) との類似から、次の予想はもつともらしい。「 $PG(n, q)$ 中の d 次元双対超卵形が存在すれば、 q は偶数である」

次の場合に、この予想は正しいことが示されているが、一般には未解決である。

$d = 2$ または d が奇数のとき (Del Fra [DF])
 $n = 2d$ のとき (Cooperstein-Thas [CT]).

(2) 「 $PG(n, q)$ 中の d 次元超卵形が存在するとき、 n と d の間にどのような関係があるか？」という生成空間の次元問題には、次の結果がある [Yo3]。

$q > 2$ ならば $n \leq d(d+3)/2$,
 $q = 2$ ならば $n \leq d(d+3) + 2$.

すべての2のべき q に対して $n = d(d+3)$ を満たす d 次元双対超卵形が構成できる (次節 3.2 参照)。一方、 $n > d(d+3)/2$ を満たす例の存在は知られていない。 $q=2$ の場合に上の不等式を「 $n \leq d(d+3)/2$ 」と改良する問題には、何人かの挑戦者がいるようだが、今のところ成功したという話を聞かない。

3. 幾つかの実例

この節では、今までに知られている双対超卵形の構成のうち幾つかを紹介する。ここにあげられていない構成は、谷口氏によるもの [Ta1, Ta2] 及び cap と関連した構成 [Hu, BD] である。

3.1 Mathieu DHO 中川氏の講演の主題であった、 $PG(5,4)$ 中の2次元双対超卵形 M は双対超卵形の研究に示唆を与えて続けてきた、重要な存在である。 M のメンバーの生成する $GF(4)$ 上の6次元ベクトル空間上には、ユニタリ形式 f が定義され M のメンバーは f に関して全等方部分空間になっている。(具体的な M のメンバー、 f の形については、中川氏の講演を参照されよ。)次元を見れば、これらは極大全等方部分空間である。この事実が、次節の極型の双対超卵形という概念につながる。

3.2 Veronesean DHO [Yo3], [TV1, TV2] Veronesean map とは $PG(d, q)$ の射影点の集合から $PG(D, q)$ ($D = d(d+3)/2$) の射影点の集合上への、次の式により定義される写像のことであった。

$$[x_0, \dots, x_d] \mapsto \begin{bmatrix} x_0^2 & x_0x_1 & \dots & x_0x_d \\ & x_1^2 & \dots & x_1x_d \\ & & \ddots & \\ & & & x_d^2 \end{bmatrix}.$$

ここで $PG(d, q)$ に付随するベクトル空間 $V(d+1, q)$ における基底 e_0, \dots, e_d に関する同次座標を $[x_0, \dots, x_d] = [\sum_{i=0}^d x_i e_i]$ と書き、 $PG(D, q)$ に付随するベクトル空間 $V(D+1, q)$ における基底 e_{ij} ($0 \leq i, j \leq d$) に関する同次座標を $[x_{00}, \dots, x_{dd}] = [\sum_{ij} x_{ij} e_{ij}]$ と書いている。

さて、 $V(d+1, q)$ (resp. $V(D+1, q)$) の部分集合 X (resp. Y) に対して、その直交空間 X^\perp (resp. Y^\perp) を、自然な内積 $(\sum_{i=0}^d x_i e_i, \sum_{i=0}^d y_i e_i) := \sum_{i=0}^d x_i y_i$ (resp. $(\sum_{ij} x_{ij} e_{ij}, \sum_{ij} y_{ij} e_{ij}) := \sum_{ij} x_{ij} y_{ij}$) に関して X (resp. Y) と直交するような $V(d+1, q)$ (resp. $V(D+1, q)$) のベクトル全体のなす部分空間とする。

このとき、 $PG(d, q)$ の射影点 $P = [\sum_{i=0}^d x_i e_i]$ に対して、その $V(d+1, q)$ における直交空間 P^\perp の Veronesean map による像 $(P^\perp)^\zeta$ を考え、更に $V(D+1, q)$ の中でその直交空間 $X(P) := ((P^\perp)^\zeta)^\perp$ をとる。すると任意の P に対して $X(P)$ は $V(D+1, q)$ 中の $d+1$ 次元部分空間であることがわかる。更に $\mathcal{V}^d(q) := \{X(P) \mid P \in PG(d, q)\}$ は $PG(D, q)$ 中の d

次元双対弧であることがわかる。 $\mathcal{V}^d(q)$ には丁度 $\theta_q(d)$ 個のメンバーが含まれるので、双対超卵形にするためには、もう一枚余分な d 次元部分空間を付け加える必要がある。

q が偶数 (2 のべき) であるときには、一般論によってこのような d 次元部分空間を見つけることが出来る。すなわち、 q が偶数の場合には、 $\mathcal{V}^d(q)$ を $PG(D, q)$ 中の d 次元双対超卵形 $\hat{\mathcal{V}}^d(q)$ に (一意的に) 拡張できる。一方、付け加えるべきベクトルの形は具体的に書き出せるので、これらが部分空間をなすかどうかを直接計算で確かめることが可能である。これを行うと⁴、 q が奇数の時には、双対弧 $\mathcal{V}^d(q)$ を双対超卵形に拡張することは出来ない。

3.3 Construction Y [Yo1] 次節との関係上、ここでは簡単に定義だけを復習しておくが、この双対超卵形は (可解ではあるが) 二重可移に作用する自己同型群を持ち、semiplane や distance regular graphs との関連も深い、興味深い存在である [PY1, PY2]。

d を自然数、 h, m は区間 $[1, \dots, d]$ 中の自然数で $d+1$ と互いに素なものとする。このとき、有限体 $GF(2^{d+1})$ を二元体 $GF(2)$ 上の $d+1$ 次元ベクトル空間と見なし、それぞれの $t \in GF(2^{d+1})$ に対して、直和 $V := GF(2^{d+1}) \oplus GF(2^{d+1})$ に付随する射影空間 $PG(V) \cong PG(2d+1, 2)$ の部分空間 $X(t)$ を次のように定める。

$$X(t) := \{(x, x^{2^m}t + xt^{2^h}) \mid x \in GF(2^{d+1})\}.$$

すると、 $S_{m,h}^{d+1} := \{X(t) \mid t \in GF(2^{d+1})\}$ は $h+m \neq d+1$ であれば、 $PG(2d+1, 2)$ 中の d 次元双対超卵形であることが確かめられる。($h+m = d+1$ の時には埋入空間は $PG(2d, 2)$ である。)

4. 極空間中の高次元双対弧・超卵形

ここでは高次元の双対弧のうち、極空間に埋め込めるようなものについて考える。

4.1 定義 V を有限体 $GF(q)$ 上の $n+1$ 次元ベクトル空間、 f は V 上の非退化な交代形式、エルミート形式 (このとき q は平方数 $q = r^2$ とする)、または非特異な二次形式とする。このとき $PG(V) \cong PG(n, q)$ 中の d 次元双対弧 \mathcal{A} が f に関して極型である (of polar type) とは、 \mathcal{A} のどのメンバーも (V の $d+1$ 次元部分空間として) f に関して極大な全等方 (f が二次形式の時には全特異) 部分空間となっていることである。

4.2 コメント (1) $d+1$ 次元の部分空間が $n+1$ 次元ベクトル空間 V の極大な全等方 (特異) 部分空間になっていることから、 d と n の間には次の関係がある。

- (s) f が非退化な交代形式 (以下シンプレクティック形式という) のとき、
 $n+1$ は偶数で $n+1 = 2(d+1) \Leftrightarrow n = 2d+1$ 。

⁴ 修士1年の学生南部奈緒子さんによる結果である。

(u) f が非退化なエルミート形式 (以下ユニタリ形式という) のとき、

$$n+1 \text{ が偶数ならば } n+1 = 2(d+1) \Leftrightarrow n = 2d+1.$$

$$n+1 \text{ が奇数ならば } n+1 = 2(d+1)+1 \Leftrightarrow n = 2d+2.$$

(o) f が非特異な二次形式 (以下直交形式という) のとき、

$$n+1 \text{ が奇数ならば } n+1 = 2(d+1)+1 \Leftrightarrow n = 2d+2.$$

$$n+1 \text{ が偶数ならば、 } f \text{ がプラス型の時 } n+1 = 2(d+1) \Leftrightarrow n = 2d+1.$$

$$n+1 \text{ が偶数ならば、 } f \text{ がマイナス型の時 } n+1 = 2(d+2) \Leftrightarrow n = 2d+3.$$

(2) 上の定義において \mathcal{A} のメンバーを極大全等方 (特異) 部分空間とする必要はないかもしれないが、こうしておく扱いやすい。

4.3 以下、簡単のため $n = 2d+1$ のみに限って論じる。上のコメント (1) で見たように、このとき f はシンプレクティック形式、偶数次元のベクトル空間上のユニタリ形式、または偶数次元のベクトル空間上のプラス型の直交形式である。他の場合 (奇数次元のベクトル空間上のユニタリ・直交形式並びに偶数次元のベクトル空間上のマイナス型の直交形式) は今のところ殆ど考えていない。

課題 $\dim(V) = n+1$ が奇数で f がユニタリまたは直交形式である場合 ($n = 2d+2$)、 $\dim(V) = n+1$ が偶数で f がマイナス型の直交形式である場合 ($n = 2d+3$) に、 f に関する極型の $PG(2d+1, q)$ 中の d -次元双対弧 (特に双対超卵形) について調べよ。

4.4 実例 (1) 22 次の Mathieu 群が作用する $PG(5, 4)$ 中の 2 次元双対超卵形 M は、ユニタリ形式に関して極型である。この事実が、極型の双対超卵形に関する研究の主たる動機となっている。

(2) ごく最近まで (1) の実例 M とおそらくは $S_{1,1}^3$ (前節 3.3 の記号による) のみが極型の高次元超卵形として知られていた唯一の例であったと思われる。2004年3月頃に次が示された。

Proposition 1 3.3 節における $PG(2d+1, 2)$ 中の d 次元双対超卵形の族 $S_{h,m}^{d+1}$ が、付随するベクトル空間 $V(2d+2, 2)$ 上のある形式 f に関して極型であれば、 d は偶数で $h \equiv -2m \pmod{d+1}$ である。逆にこの条件が満たされるとき、 $S_{h,m}^{d+1}$ はプラス型の直交形式に関して (従って随判するシンプレクティック形式に関して) 極型である。

この事実は、トレース関数の値に関する初等的な議論の積み重ねとして得られる。最近谷口氏により構成された $PG(2d+1, q)$ 中の d -次元双対超卵形 [Ta2] の中で埋入空間が $PG(2d+1, q)$ であることがすぐにわかる場合に関しては、極型のものは存在しないことも、同様の論法により確かめられた [Yo4]。ただし、そこでは埋込空間が $PG(2d+1, q)$ となるような場合をすべて尽くしてはいないので、残された場合の中から面白いものが発見される可能性は捨てきれない。

4.5 コメント (1) 今のところ $q > 2$ に対する高次元の極型の双対超卵形として知られているものは M のみである。他にあるのだろうか？

(2) 「高次元の双対超卵形が存在すれば q は偶数である」という予想が正しいとすれば「奇数 q に対して $PG(2d+1, q)$ 中の極型 d -次元双対超卵形は存在しない」という命題は、比較的たやすく証明できそうである。しかし、私は今のところこれを示せない。

4.6 基本性質と 2・3次元極型双対超卵形の分類 極型の双対超卵形の基本性質のうち、重要なものを挙げる。

Lemma 2 S を $PG(2d+1, q)$ 中の d 次元極型双対超卵形とする。このとき互いに相異なる 3 個のメンバー $X, Y, Z \in S$ に対して

$$\text{proj. dim}((X, Y) \cap Z) = d - 1$$

この事実を用いると、 $d = 2$ の場合の極型の双対超卵形の分類は、Del Fra による幾つかの結果に帰着できる。すなわち、この場合 $q+2$ 個のメンバーよりなるブロックをうまく定義できて S 上にスタイナー系 $S(3, q+2, \theta_q(d)+1)$ の構造が入る。このとき適当な整数条件から $q = 2$ または 4 が導ける。 $q = 4$ の時にはスタイナー系 $S(3, 6, 22)$ の一意性から、対応する $PG(5, 4)$ 中の 2 次元極型双対超卵形の自己同型群は、このスタイナー系の自己同型群 $M_{22.2}$ の部分群であることがわかる。中川氏がその講演で示されたように、この事実を全く異なる方法で、しかもより具体的に示すことも出来るが、上の考えも興味深い。メンバー上にある種の 3-スタイナー系を構成できるような双対超卵形については A. Del Fra, M. Buratti や私による最近の研究もある [BD], [DY]。

Del Fra は $d = 2$ の場合に上の命題の結論を満たす $PG(5, 2)$ と $PG(5, 4)$ 中の 2 次元双対超卵形の分類を行っている。それを引用すれば、結局次が得られる。

Proposition 3 $PG(5, q)$ 中の 2 次元極型双対超卵形は M か $S_{1,1}^3$ に同値である。

更に次の命題は色々な議論に有効に使える。中川氏による M の具体的構成の基本にも、 $d = 2$ に対するこの事実が使われている。ここで、形式 f の与えられたベクトル空間 V の部分空間 π に対して π^\perp は f または (f が直交形式の時) f に随判する対称形式によって π のすべてのベクトルと直交するベクトルのなす V の部分空間である。

Lemma 4 S を $PG(2d+1, q)$ 中の d 次元極型双対超卵形とし、 $X \in S$ をその一つのメンバーとする。 π を X の部分空間でその射影次元が $\text{proj. dim}(\pi) = d - i$ ($i = 1, \dots, d-1$) で与えられるものとすれば、 $Y \cap \pi^\perp$ の射影次元は $X \cap Y$ が π に入るか否かに応じて次のように与えられる。

$$\text{proj. dim}(Y \cap \pi^\perp) = \begin{cases} i & \text{if } X \cap Y \in \pi \\ i - 1 & \text{if } X \cap Y \notin \pi \end{cases}$$

この事実を用いて次が示せる。しかしながら、ここで使われた議論は $d > 3$ に対しては何らの結論ももたらさない。

Proposition 5 $PG(7, q)$ 中には極型の 3 次元双対超卵形は存在しない。

4.7 プラス型の直交形式に関する極型双対超卵形 プラス型の直交形式に関する極型双対超卵形に関しては、交換子群 $\Omega_{2d+2}^+(q)$ が $d+1$ 次元の特異部分空間全体のなす集合上に二つの軌道を持つことを用いて、次の事実を示せる。

Proposition 6 $PG(2d+1, q)$ 中にプラス型の直交形式に関する d 次元極型双対超卵形が存在するならば、 d は偶数である。

先の例 $S_{-2m, m}^{d+1}$ を見ると、逆に任意の偶数 d に対して、 $PG(2d+1, q)$ (ただし $q = 2$) 中にプラス型直交形式に関して極型の d 次元双対超卵形が存在する。 $q > 2$ ならびに奇数 q についての存在はいまのところ不明である。

5. 自己同型群

この節では高次元の双対超卵形の自己同型群に関する性質について述べる。そのため次のように記号を準備する。

5.1 記号 A を $PG(n, q)$ における d 次元の双対弧とし、 A が生成する $GF(q)$ 上 $n+1$ 次元のベクトル空間を V とする。[HP] に始まる伝統的な自己同型群の定義は次のように与えられる。

$$Aut(A) := \{g \in Aut(PG(n, q)) \mid X^g \in A (\forall X \in A)\}$$

この定義によれば $Aut(A)$ は $Aut(PG(n, q)) \cong PSL(n+1, q).GF(q)^\times.Z_e$ の部分群である。ここで $q = p^e$ (p は素数) としている。線形自己同型群については、次のような定義も考えられる。

$$GL(A) := \{g \in GL(V) \cong GL_{n+1}(q) \mid X^g \in A (\forall X \in A)\}.$$

この群は V 上のスカラー変換のなす群 $Sc(V) \cong GF(q)^\times$ をその中心に含む。しかし、拡大 $GL(A)/Sc(V)$ の様子は双対弧 A によって変化する。例えば $PG(5, 4)$ 中のユニタリ形式に関する 2 次元極型双対超卵形 M についてみると $GL(M)/Sc(V) \cong M_{22}$, $Sc(V) \cong GF(4)^\times \cong Z_3$ であるが、拡大 $GL(M)/Sc(V)$ は非分裂である。

$$PGL(A) := GL(A)/Sc(V)$$

とおくと、これが $Aut(A)$ の線形部分 $PGL(V) \cap Aut(A)$ になる。

群 $GL(A)$ は A のメンバーの置換群を引き起こし、 $Sc(V)$ はこの作用の核に含まれる。 A のメンバー上の偶置換を引き起こすもの全体のなす部分群を

$$GL^e(A) := \{g \in GL(A) \mid g \text{ は } A \text{ 上に偶置換を引き起こす}\},$$

とすれば、 $GL^e(V)$ は $Sc(V)$ を含む $GL(A)$ の指数 2 以下の部分群である。

もし A が V 上のある形式 f に関して極型であるならば、上の自己同型群の定義を次のように変更する。まず f を保つ線形変換のなす群を、 f がシンプレクティック形式かユニタリ形式の場合には

$$GL(V, f) := \{g \in GL(V) \mid f(x, y) = f(x^g, y^g) (\forall x, y \in V)\}$$

と定める。このとき $GL(V, f) \cong Sp_{n+1}(q)$ または $GU_{n+1}(q)$ である。 f が直交形式の場合には

$$GL(V, f) := \{g \in GL(V) \mid f(x) = f(x^g) (\forall x \in V)\}$$

と定める。このとき $n+1$ が奇数ならば $GL(V, f) \cong GO_{n+1}(q)$ 、 $n+1$ が偶数ならば直交形式 f の型 ε に応じて $GL(V, f) \cong GO_{n+1}^\varepsilon(q)$ である。これらとの共通部分を取って

$$GL(A, f) := GL(A) \cap GL(V, f), \quad PGL(A, f) := GL(A, f) / (Sc(V) \cap GL(V, f))$$

を極型の双対弧の自己同型群とする。

また、よく使う記号であるが、(線形) 自己同型 $g \in GL(A)$ に対して、それが (全体として) 固定する A のメンバーの集合を

$$A(g) := \{X \in A \mid X^g = X\}$$

とおく。

5.2 基本定理 次が (高次元の) 双対超卵形の自己同型群に関する基本定理である。一口に言って、自己同型が十分多くのメンバーを固定するならば、そこからより低次元の双対超卵形が得られるというものである。この事実がこの形ではっきり述べられたのは、松本での集会がはじめてであったと思われる。論文 [Yo2] には標数が $q=2$ のときに限った形で、この事実がさりげなく述べられている。

Theorem 7 S を $PG(n, q)$ 中の d 次元双対超卵形、 p を $GL(S)$ の位数を割り切る素数とする。このとき、次のいずれかが成り立つ。⁵

(1) p は $q-1$ を割り切る。

⁵ 松本での講演において、最後の場合 $p=2$ のときに $e=0$ となる可能性があることに言及するのを忘れたので、修正する。

- (2) $|GL(S)|$ のシロー p -部分群の位数は $|S| = \theta_q(d) + 1$ を割り切る。
- (3) S の 1 個または 2 個のメンバーからなる集合 Ω で、 $GL(S)$ の p 元すべての生成する正規部分群 $N = O_{p'}(GL(S))$ により不変なものが存在する。
- (4) $GL(S)$ は p -強閉部分群 H を持つ。つまり H は $GL(S)$ のシロー p -部分群を含み、任意の $x \in GL(S) \setminus H$ に対して $H \cap H^x$ は p' -部分群である。
- (5) ある位数 p の元 $g \in GL(S)$ が存在して、それぞれの $X \in S(g)$ に対する固定部分ベクトル空間 $C_X(g) = \{x \in X \mid x^g = x\}$ を集めて得られる集合

$$S[g] := \{C_X(g) \mid X \in S(g)\}$$

は、ある非負整数 e ($0 \leq e \leq d-1$) に対して e 次元の双対超卵形をなす。 $e=0$ となる可能性があるのは $p=2$ のときのみである。ただし 0 次元双対超卵形とは、単に 2 個のメンバーからなる部分集合のこととする。

上の (5) の場合、固定空間 $C_X(g)$ の次元は $X \in S(g)$ の取り方によらない。また $S(g)$ のメンバーたちの生成する空間は $C_V(g) = \{v \in V \mid v^g = v\}$ の部分空間というだけで、どれぐらい大きくなるかはわからない。(もちろん $q > 2$ の場合、その射影次元は $2e$ 以上 $e(e+3)/2$ 以下であるが。)

5.2 基本定理の応用 「双対超卵形が存在すれば q は偶数である」という予想を念頭に置けば、この定理の最も重要な応用は、偶数 q に対して素数 $p=2$ を位数とする自己同型を選んだときに得られる。このとき (1) は起こらないので (2)-(5) のいずれかが生ずる。従って、 $GL(S)$ のシロー 2-部分群及び involution の中心化群の構造は強い制限を受ける。 $(q$ が偶数の時には $PGL(S)$ の involution の $GL(S)$ における逆像には、involution が存在するので、 $PGL(S)$ における位数 2 の元の中心化群の構造が強く制限されるといっても良い。) $p=2$ のときには、(4) における 2-強閉部分群は、単に強閉部分群と呼ばれ、そのような部分群を持つ有限群の分類 (Zassenhaus, 伊藤、鈴木などの成果をふまえて最終的に Bender により得られた) は、単純群分類以前の古典的群論における優れた成果の一つとして、その証明も込めて十分に完成したものである。

特に次の状況を考えよう。

q は偶数 (2 のべき) で $q \geq 4$, d は 4 の倍数,
 S は $PG(2d+1, q)$ 中の d 次元極型双対超卵形。

このとき、古典的な有限群論の結果 (強閉部分群を持つ群の分類、二面体群をシロー 2-群に持つ群の分類) を用いるだけで、 $GL^e(S)$ の部分群について、その構造の可能性が決まってしまう。詳しくは論文 [Y05] を参照して頂くとして、ここでは次の系を述べておく。

Proposition 8 上の仮定の下で、 $GL(S)$ は S のメンバー上に可移に作用する準単純群を含まない。

5.3 コメントと幾つかの問題 上の結果を $PG(5, 4)$ 中の 2 次元極型双対超卵形 \mathcal{M} (このとき $GL(\mathcal{M}) = GL^e(\mathcal{M})$ は \mathcal{M} 上二重可移であった) の存在と見比べると、制限「 d は 4 の倍数」が非常に重要であることに気づく。上の結果の証明を眺めてみると、他の d (modulo 4) の値に対しても q を十分大きく取るとき、上の命題と類似したことがいえる可能性があるようにも思われる。

また、上記の定理を見ればすぐに次の形の問題が考えられよう。

q を偶数とする。 $PG(n, q)$ 中の d 次元の双対超卵形 S で、
その位数 2 の自己同型 $t \in GL(S)$ に対する $S[t]$ が
与えられた e 次元双対超卵形であるものを分類せよ。

これは有限単純群論における、involution の中心化群による特徴付け問題に極めて似ている。ここで、Brauer-Fowler の原理に相当する結果が存在するであろうか？また、この状況は置換群の可移拡大に例えられるかもしれない。ともあれ、大きな自己同型群を持つ高次元双対超卵形の研究には (不幸な endless game に陥るという可能性も皆無ではないが)、将来の発展が十分期待できると思われる。

参考文献

- [BD] M.Buratti and A.Del Fra, Semi-Boolean Steiner quadruple systems and dimensional dual hyperovals, *Advances in Geometry* 3 (2003), Special Volume, S245–S253.
- [CT] B.Cooperstein and J.Thas, On generalized k -arcs in $PG(2n, q)$, *Ann. Combin.* 5 (2001), 141–152.
- [DF] A.Del Fra, On d -dimensional dual hyperovals, *Geom. Dedicata*, 79(2000), 157–178.
- [DY] A.Del Fra and S.Yoshiara, Dimensional dual hyperovals associated with Steiner systems, to appear in *Europ. J. Combin.*
- [HP] C.Huybrechts and A.Pasini, Flag-transitive extensions of dual affine spaces, *Contrib. Algebra Geom.* 40 (1999), 503–532.
- [Hu] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AG^*$ geometries, *Discrete Math.* 255 (2002), 503–532.
- [PY1] A. Pasini and S. Yoshiara, On a new family of flag-transitive semiplanes, *European J. Combin.* 22 (2001), 529–545.
- [PY2] A. Pasini and S. Yoshiara, New distance regular graphs arising from dimensional dual hyperovals, *European J. Combin.* 22 (2001), 547–560.

- [Ta1] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with q even, to appear in *Europ. J. Combin.*
- [Ta2] H. Taniguchi, A note on the automorphism of $\mathcal{T}_\sigma(V)$, preprint, 2003.
- [TV1] J.Thas and H.van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, *Quart. J. Math. Oxford. Ser.2.*
- [TV2] J.Thas and H.van Maldeghem, Characterizations of the finite quadric and Hermitian Veroneseans over finite fields, *J.Ggeom.* **76** (2003), 282–293.
- [Yo1] S.Yoshiara, A family of d -dimensional dual hyperovals in $PG(2d + 1, 2)$, *Europ. J. Combin.* **20** (1999) 589–603.
- [Yo2] S.Yoshiara, On a family of planes of a polar space, *Europ. J. Combin.*, **22**(2001), 107–118.
- [Yo3] S.Yoshiara, Ambient spaces of dimensional dual arcs, *J. Alg. Combin.* **19** (2004), 5–23.
- [Yo4] S.Yoshiara, Some remarks on dimensional dual hyperovals of polar type, submitted to the proceeding of La Roche Conference on Incidence Geometry, May, 2004.
- [Yo5] S.Yoshiara, Automorphism groups of some dimensional dual hyperovals, Preprint, April, 2004.

2004年7月27日(火)提出

符号と超特異 $K3$ 曲面のモジュライ

北大・理 島田 伊知朗 (Ichiro SHIMADA)

標数 2 の射影平面の純非分離な 2 重被覆として得られる超特異 $K3$ 曲面の幾何学的構造が、ある性質をもつ長さ 21 の線形符号によって記述されるということを解説する。標数 2 の超特異 $K3$ 曲面のモジュライは、これらの線形符号の同型類に対応した strata に分割される。次元の低い strata について詳しく調べる。

証明の細部については [8], [9] および [11] を参照されたい。論説 [10] と重なる部分が多くあることをお断りしておく。

1 超特異 $K3$ 符号と超特異 $K3$ 格子

超特異 $K3$ 符号も超特異 $K3$ 格子も、どちらもこの論説のなかでのみ使われる用語である。

定義 1.1 次を満たす長さ 21 の線形符号 $C \subset \mathbb{F}_2^{21}$ を超特異 $K3$ 符号という。

- (i) $[1, 1, \dots, 1] \in C$,
- (ii) 任意の語 $A \in C$ の Hamming 重み $|A|$ は $|A| \in \{0, 5, 8, 9, 12, 13, 16, 21\}$ をみたす。

計算機を使って超特異 $K3$ 符号の同型類を完全に決定した。超特異 $K3$ 符号の次元は高々 10 であり、 d 次元の超特異 $K3$ 符号の同型類の個数 $s(d)$ は下の表で与えられる：

d	10	9	8	7	6	5	4	3	2	1
$s(d)$	1	3	13	41	58	43	21	8	3	1

21 個の元からなる集合

$$\mathcal{P} := \{1, 2, \dots, 21\}$$

を固定し、 \mathbb{F}_2^{21} を \mathcal{P} のベキ集合 $\text{Pow}(\mathcal{P})$ と自然に同一視する。超特異 $K3$ 符号の各語は、長さ 21 の \mathbb{F}_2 -係数のベクトルとして表され、また \mathcal{P} の部分集合としても表される。

定義 1.2 重みが 5, 8 または 9 の語 $A \in \mathbb{F}_2^{21}$ の次数 $\deg A$ を

$$\deg A := \begin{cases} 1 & \text{if } |A| = 5, \\ 2 & \text{if } |A| = 8, \\ 3 & \text{if } |A| = 9 \end{cases}$$

により定める. C を超特異 $K3$ 符号とし, $A \in C$ かつ $|A| \in \{5, 8, 9\}$ とする. 分解

$$A = A_1 + A_2 \quad (A_1, A_2 \in C_G)$$

で, $|A_1|, |A_2| \in \{5, 8, 9\}$ かつ $\deg A = \deg A_1 + \deg A_2$ なるものが存在するとき, A は C において可約であるという. A が C のなかで可約でないとき, A は C のなかで既約であるという.

定義により, 超特異 $K3$ 符号は $\mathcal{P} = [1, 1, \dots, 1]$ と既約な語により生成される. 次数 $\deg A$ の幾何学的な意味については §4 を参照されたい.

この論説の最後に, 各同型類を代表する超特異 $K3$ 符号の一覧表を載せる. この表には次のデータが記載されている.

- $\sigma = 11 - \dim C$.
- basis: \mathbb{F}_2 上の基底.
- l: 重さ 5 の語の個数. (重さ 5 の語はすべて既約である.)
- q: 重さ 8 の既約な語の個数.
- e: 重さ 9 の既約な語の個数.
- tl: 相異なる重さ 5 の語の 3 つ組 L_1, L_2, L_3 で, 各語を \mathcal{P} の部分集合とみたときの共通部分 $L_1 \cap L_2 \cap L_3$ が 1 点からなるものの個数.
- lq: 重さ 5 の語 L と既約な重さ 8 の語 Q のペア (L, Q) で, $L \cap Q$ が空集合となるものの個数.
- qq: 既約な重さ 8 の語のペア (Q_1, Q_2) で, $|Q_1 \cap Q_2| = 2$ となるものの個数.

basis においては, C の各元は長さ 21 の bit ベクトル $[\alpha_0, \dots, \alpha_{20}]$ によりあらわされ, bit ベクトルは, 整数 $2^{20}\alpha_0 + \dots + 2\alpha_{19} + \alpha_{20}$ によりあらわされている. ただし, $[1, 1, \dots, 1] = 2^{21} - 1$ はすべての基底にあらわれるので省略されている.

例 1.3 No. 191 の 10 次元超特異 $K3$ 符号 C_{191} は Dolgachev-Kondo 符号 C_{DK} とよばれ ([3]), 次のように構成される. 射影平面の \mathbb{F}_4 -有理点の集合 $\mathbb{P}^2(\mathbb{F}_4)$ は 21 個の元か

らなる. C_{DK} は, 1 直線上にある 5 個の \mathbb{F}_4 -有理点のなす 21 個の語で生成される符号である. その weight-enumerator は

$$1 + 21z^5 + 210z^8 + 280z^9 + 280z^{12} + 210z^{13} + 21z^{16} + z^{21}$$

であたえられる.

注意 1.4 定義より直ちにわかるように, C_{DK} の部分符号で $\mathcal{P} = [1, 1, \dots, 1]$ を含むものは超特異 $K3$ 符号である. Nos. 139, 150, 179, 185 以外の同型類はこの方法で作られる. 同型類 Nos. 139, 150, 179, 185 はこの方法では作れない.

定義 1.5 超特異 $K3$ 符号 C が与えられたとする. 語 $A \in C$ に対し, 長さ 22 の語 \tilde{A} を

$$\tilde{A} := \begin{cases} (A, 0) & \text{if } |A| \equiv 0 \pmod{4}, \\ (A, 1) & \text{if } |A| \equiv 1 \pmod{4} \end{cases}$$

により定義し,

$$\tilde{C} := \{ \tilde{A} \mid A \in C \} \subset \mathbb{F}_2^{21} \oplus \mathbb{F}_2$$

とおく. \tilde{C} は線形符号になり, $\dim \tilde{C}$ は $\dim C$ と等しい. このようにして得られる線形符号 \tilde{C} を拡大超特異 $K3$ 符号とよぶ.

注意 1.6 講演中に指摘されたことであるが, \tilde{C}_{DK} は 24 次元の binary Golay code の引き戻しとして得られる. φ を拡大に対応する新しい座標とし, $\mathbb{P}^2(\mathbb{F}_4) \sqcup \{\varphi\}$ から MOG の positions への写像 γ を表 1.1 により定義すると, γ による Golay code の引き戻しが \tilde{C}_{DK} になる. この写像 γ は, 論文 [7] において標数 2 における Fermat cubic 4-fold の中間次元のある代数的サイクルのなす格子が laminated lattice Λ_{22} ([2, Chapter 6]) と同型であることを示すときにもあらわれた.

定義 1.7 σ を 10 以下の正整数とする. ランク 22 の格子 L が次をみたすとき, L を超特異 $K3$ 格子という.

- (i) even (すなわち $v^2 \in 2\mathbb{Z}$ がすべての $v \in L$ に対して成立),
- (ii) hyperbolic (すなわち L の signature は $(1, 21)$),
- (iii) disc $L = -2^{2\sigma}$,
- (iv) 2-elementary (すなわち $L^\vee/L \cong (\mathbb{Z}/2\mathbb{Z})^{2\sigma}$, ここで L^\vee は L の双対格子 $\text{Hom}(L, \mathbb{Z})$),
- (v) type I (すなわち $v^2 \in \mathbb{Z}$ がすべての $v \in L^\vee$ に対して成立).

- (ii) $\{v \in S \mid vh = 1, v^2 = 0\}$ は空集合であり,
- (iii) $\{v \in S \mid vh = 0, v^2 = -2\}$ は $\{\pm r_1, \dots, \pm r_{21}\}$ と一致する.

2 K3 曲面とその Néron-Severi 格子

k を代数閉体とし, 代数多様体はすべてこの上で定義されているとする.

定義 2.1 非特異射影代数曲面 X は, どの点でも 0 とならない正則 2-形式をもち, かつ $h^1(X, \mathcal{O}_X) = 0$ となるとき, K3 曲面と呼ばれる.

定義 2.2 X を非特異射影代数曲面とする. X 上の因子 $D = \sum m_i C_i$ (m_i は整数, C_i は X 上の既約な曲線) を考える. X 上の任意の曲線 C' に対して D と C' の交点数 DC' が 0 となるとき, D は数値的に 0 と同値であるという. D を含む数値的同値類を $[D]$ と書く.

定義 2.3 X を非特異射影代数曲面とする. X 上の因子の数値的同値類のなすアーベル群を $NS(X)$ と書く. $[D][D'] := DD'$ により $NS(X)$ は格子になる. この格子を X の Néron-Severi 格子という. またそのランクを X の Picard 数という.

標数 0 の体上で定義された K3 曲面の Picard 数は高々 20 である. 一方, 正標数の体上で定義された K3 曲面の Picard 数は, 20 以下であるかあるいは 22 である.

定義 2.4 K3 曲面は, その Picard 数が 22 となるとき, (Shioda の意味で) 超特異であるといわれる.

例 2.5 4 次曲面

$$X = \{x_0^4 + x_1^4 + x_2^4 + x_3^4 = 0\} \subset \mathbb{P}^3$$

を考える. 基礎体 k の標数が 2 でなければ, この 4 次曲面は非特異ではしたがって K3 曲面になる. Picard 数は

$$\text{rank } NS(X) = \begin{cases} 20 & \text{if char } k = 0 \text{ or char } k \equiv 1 \pmod{4}, \\ 22 & \text{if char } k \equiv 3 \pmod{4} \end{cases}$$

となる.

つぎの定理は, Artin [1] および Rudakov-Shafarevich [6] によって示された.

定理 2.6 標数 $p > 0$ の基礎体の上で考える. 超特異 $K3$ 曲面 X の Néron-Severi 格子 $NS(X)$ は, even かつ hyperbolic であり, $NS(X)^\vee/NS(X)$ は $(\mathbb{Z}/p\mathbb{Z})^{2\sigma(X)}$ と同型になる. ここで, $\sigma(X)$ は 10 以下の正整数であり, X の Artin 不変量とよばれる.

さらに, $p = 2$ なら $NS(X)$ は type I である.

定理 1.8 と定理 2.6 より次を得る.

系 2.7 標数 2 の体上定義された超特異 $K3$ 曲面の Néron-Severi 格子は, 超特異 $K3$ 格子である.

つぎの存在定理は, Artin [1], Shioda [12] および Rudakov-Shafarevich [5] によって示された.

定理 2.8 素数 p と 10 以下の正整数 σ の任意のペア (p, σ) に対し, 標数 p の体上定義された超特異 $K3$ 曲面で, Artin 不変量が σ となるものが存在する.

3 標数 2 における超特異 $K3$ 曲面のモジュライ

以下, 基礎体 k の標数は 2 であるとする.

$G = G(X, Y, Z)$ を 3 変数 6 次同次多項式, すなわち射影平面 \mathbb{P}^2 の可逆層 $\mathcal{O}(6)$ の大域切断とする. 標数 2 においては, G の微分 dG をベクトル束 $\Omega^1(6)$ の大域切断として定義できる. 実際, 同型 $\mathcal{O}(6) \cong \mathcal{O}(3)^{\otimes 2}$ を用いることにより, 直線束 $\mathcal{O}(6)$ の局所自明化でその変換関数がすべて t^2 のかたちをしているものをとることができる. $g = t^2 g'$ なら $dg = t^2 dg'$ が成立するので, G の局所データ g の微分 dg ははり合わさってベクトル束 $\Omega^1(6)$ の大域切断 dG を定める. $Z(dG)$ により, $dG = 0$ で定義された \mathbb{P}^2 の部分スキームをあらわす. $P \in Z(dG)$ とする. ベクトル束 $\Omega^1(6)$ の全空間のなかで, 切断 dG とゼロ切断が P において横断的に交わっているとき, $Z(dG)$ は P において 0 次元かつ被約であるという. すべての $P \in Z(dG)$ において $Z(dG)$ が 0 次元かつ被約であるとき, $Z(dG)$ は 0 次元かつ被約であるという.

定義 3.1 $Z(dG)$ が 0 次元かつ被約となる次数 6 の同次多項式 G のなす集合を \mathcal{U} と書く. \mathcal{U} は次数 6 の同次多項式全体のなす 28 次元のベクトル空間 $H^0(\mathbb{P}^2, \mathcal{O}(6))$ の Zariski 開集合である.

G が \mathcal{U} に属する同次多項式なら, $Z(dG)$ は

$$c_2(\Omega^1(6)) = 21$$

個の被約な点からなる. ここで c_2 は第 2 Chern 類である. 逆に, $Z(dG)$ が 21 個の点からなれば, それらの点はすべて被約であり, $G \in \mathcal{U}$ が成立する.

例 3.2 Dolgachev-Kondo [3] によって発見された次の同次 6 次多項式を考えよう.

$$G_{\text{DK}} := XYZ(X^3 + Y^3 + Z^3).$$

$Z(dG_{\text{DK}})$ は \mathbb{P}^2 の \mathbb{F}_4 -有理点の集合 $\mathbb{P}^2(\mathbb{F}_4)$ と一致する. $|\mathbb{P}^2(\mathbb{F}_4)| = 21$ より $G_{\text{DK}} \in \mathcal{U}$ である. したがって \mathcal{U} は空でない.

直線束 $\mathcal{O}(3)$ の全空間のなかで, 方程式

$$w^2 = G$$

により定義される曲面 Y_G を考える. ここで, w は直線束 $\mathcal{O}(3)$ のファイバー座標である. 被覆射 $\pi_G : Y_G \rightarrow \mathbb{P}^2$ は純非分離射となる. Y_G の特異点集合 $\text{Sing } Y_G$ は $\pi_G^{-1}(Z(dG))$ と一致し, さらに $P \in Z(dG)$ が被約な点であるという条件と P 上の Y_G の特異点が通常 2 重点であるという条件は同値である. したがって, G が \mathcal{U} に属する同次多項式であるための必要十分条件は, $\text{Sing}(Y_G)$ が 21 個の通常 2 重点からなることである.

非特異曲面上の自己交点数が -2 の非特異有理曲線を (-2) -曲線という. 通常 2 重点の最小特異点解消には例外曲線として (-2) -曲線が 1 本あらわれる. $G \in \mathcal{U}$ のとき, Y_G の最小特異点解消として得られる曲面 X_G は超特異 $K3$ 曲面となる. 実際, $K3$ 曲面 X_G の上には, \mathbb{P}^2 の直線の引き戻しとして得られる曲線と, 最小特異点解消 $X_G \rightarrow Y_G$ により Y_G の特異点につぶされる 21 本の (-2) -曲線が存在し, これらの数値的同値類は \mathbb{Q} 上 1 次独立であるから, X_G の Néron-Severi 格子 $NS(X_G)$ のランクは 22 となる.

逆に次が成立する:

定理 3.3 ([8]) X を標数 2 における超特異 $K3$ 曲面とすると, ある $G \in \mathcal{U}$ が存在して, X は X_G と同型になる.

線型写像 $G \mapsto dG$ の核を \mathcal{V} とする.

$$\mathcal{V} = \{ H^2 \in H^0(\mathbb{P}^2, \mathcal{O}(6)) \mid H \in H^0(\mathbb{P}^2, \mathcal{O}(3)) \}$$

である. $G \in \mathcal{U}$ ならば, 任意の $H^2 \in \mathcal{V}$ に対して $G + H^2 \in \mathcal{U}$ である. すなわち, \mathcal{V} は \mathcal{U} に平行移動により作用する. G と G' を \mathcal{U} に属する同次多項式とする. X_G と $X_{G'}$ が \mathbb{P}^2 上同型であるための必要十分条件は, ある $c \in k^\times$ と $H^2 \in \mathcal{V}$ が存在して,

$$G' = cG + H^2$$

が成立することである。したがって、標数2における次数2の超特異 $K3$ 曲面のモジュライ空間を

$$\mathfrak{M} := PGL(3, k) \backslash \mathbb{P}_*(U/V)$$

により構成することができる。 \mathfrak{M} の次元は

$$\dim \mathfrak{M} = h^0(\mathbb{P}^2, \mathcal{O}(6)) - h^0(\mathbb{P}^2, \mathcal{O}(3)) - 1 - \dim PGL(3, k) = 9$$

であるから、たしかに Artin [1] の結果と一致する。

注意 3.4 一般に、 \mathbb{P}^2 の純非分離被覆として得られる曲面は Zariski 曲面とよばれ、その一般的な性質が [4] において詳しく調べられている。

G を U に属する次数6の同次多項式とする。 $[G] \in \mathfrak{M}$ により、対応するモジュライ空間上の点をあらわす。また、

$$\phi_G : X_G \rightarrow \mathbb{P}^2$$

により、 Y_G の最小特異点解消 $X_G \rightarrow Y_G$ と純非分離な被覆射 $\pi_G : Y_G \rightarrow \mathbb{P}^2$ の合成をあらわす。 \mathbb{P}^2 の general な直線の引き戻しとして得られる既約曲線を $H_G \subset X_G$ とする。また、

$$Z(dG) = \{P_1, \dots, P_{21}\}$$

とし、 $\Gamma_i \subset X_G$ で P_i につぶされる (-2) -曲線をあらわす。 X_G の Néron-Severi 格子 $NS(X_G)$ のなかで、数値的同値類 $[\Gamma_1], \dots, [\Gamma_{21}]$ および $[H_G]$ により生成される部分格子を $NS(X_G)_0$ と書く。対応 $r_i \mapsto [\Gamma_i]$, $h \mapsto [H_G]$ により、格子 $NS(X_G)_0$ は (1.1) で定義された格子 S_0 と同型になる。したがって、 $NS(X_G)_0$ の discriminant group $(NS(X_G)_0)^\vee / NS(X_G)_0$ は $\mathbb{F}_2^{21} \oplus \mathbb{F}_2$ と同型であり、第1ファクター \mathbb{F}_2^{21} は $Z(dG)$ のベキ集合 $\text{Pow}(Z(dG))$ と自然に同一視できる。 $NS(X_G)$ と $NS(X_G)_0$ はともにランクが22であるから、 $NS(X_G)$ は $NS(X_G)_0$ の overlattice である。長さ22の線形符号 C_G^\sim を、

$$C_G^\sim := NS(X_G) / NS(X_G)_0 \subset (NS(X_G)_0)^\vee / NS(X_G)_0 = \mathbb{F}_2^{21} \oplus \mathbb{F}_2 = \text{Pow}(Z(dG)) \oplus \mathbb{F}_2$$

により定義し、長さ21の線形符号

$$C_G \subset \mathbb{F}_2^{21} = \text{Pow}(Z(dG))$$

を C_G^\sim の第1ファクターへの射影とする。 X_G の Artin 不変量 $\sigma(X_G)$ は

$$\sigma(X_G) = 11 - \dim_{\mathbb{F}_2} C_G^\sim = 11 - \dim_{\mathbb{F}_2} C_G$$

により求められる。次の定理が基本的である。この定理は、命題 1.9 と系 2.7 を用いて証明される。

定理 3.5 長さ 21 の線形符号 C に対し、ある $G \in \mathcal{U}$ が存在して C が C_G と同型になるための必要十分条件は、 C が超特異 $K3$ 符号であることである。

この定理により、モジュライ空間 \mathfrak{M} を超特異 $K3$ 符号の同型類に対応した 192 個の部分集合に分割することができる。すなわち、 $[C_0], \dots, [C_{191}]$ を §5 の一覧表により番号付けされた超特異 $K3$ 符号の同型類とし、

$$\mathfrak{M}_i := \{ [G] \in \mathfrak{M} \mid C_G \text{ は } C_i \text{ と同型} \}$$

とおくと、分割

$$\mathfrak{M} = \bigsqcup_{i=0}^{191} \mathfrak{M}_i$$

を得る。 \mathfrak{M}_0 は \mathfrak{M} の Zariski 開集合になる。 $\mathfrak{M}_1, \mathfrak{M}_2, \mathfrak{M}_3$ は \mathfrak{M} において余次元 1 であり、かつ既約であることが証明される。

4 符号から超特異 $K3$ 曲面の幾何学へ

符号 C_G から超特異 $K3$ 曲面 X_G 、あるいは純非分離被覆 $Y_G \rightarrow \mathbb{P}^2$ の幾何学的性質についての情報を得ることができる。以下にいくつかの例をあげる。 C_G の各語は、 $Z(dG)$ の部分集合と自然にみなされることに注意する。

命題 4.1 3 点 $P_{i_1}, P_{i_2}, P_{i_3} \in Z(dG)$ が直線上にあるための必要十分条件は、 C_G の重さ 5 の語で $P_{i_1}, P_{i_2}, P_{i_3}$ を含むものが存在することである。

系 4.2 $Z(dG)$ のある 3 点が直線 $L \subset \mathbb{P}^2$ 上であれば、 $L \cap Z(dG)$ は 5 点からなる。

命題 4.3 6 点 $P_{i_1}, \dots, P_{i_6} \in Z(dG)$ が非特異 2 次曲線上にあるための必要十分条件は、 C_G の重さ 8 の既約な語で P_{i_1}, \dots, P_{i_6} を含むものが存在することである。

系 4.4 $Z(dG)$ のある 6 点が非特異 2 次曲線 $Q \subset \mathbb{P}^2$ 上であれば、 $Q \cap Z(dG)$ は 8 点からなる。

定義 4.5 平面 3 次曲線の pencil $\mathcal{E} = \{E_t\}$ が regular であるとは次の条件を満たすことである。

- (i) \mathcal{E} の base locus は 9 点からなる.
- (ii) \mathcal{E} の特異メンバーはすべて I_0 型である.

命題 4.6 C_G の重さ 9 の既約な語 A に対し, A を base locus とする 3 次曲線の regular pencil が存在する.

X_G の射影的自己同型群

$$\text{ProjAut}(X_G) := \{ g \in PGL(3, k) \mid g(Z(dG)) = Z(dG) \}$$

を考える. $\text{ProjAut}(X_G)$ の各元は $Z(dG)$ の置換を引き起こす. 定義により, 各 $g \in \text{ProjAut}(X_G)$ は部分空間 $C_G \subset \text{Pow}(Z(dG))$ を保つ. したがって, $K3$ 曲面の射影的自己同型群 $\text{ProjAut}(X_G)$ を符号の自己同型群 $\text{Aut}(C_G)$ のなかに埋め込むことができる.

Artin 不変量の小さな超特異 $K3$ 曲面の同型類のなす strata, すなわち次元の大きな超特異 $K3$ 符号に対応する strata の構造を詳しく見てみよう.

Artin 不変量 1 の超特異 $K3$ 曲面の同型類からなる stratum \mathfrak{M}_{191} は 1 点 $[G_{\text{DK}}]$ からなる. (例 3.2 参照.) $\text{ProjAut}(X_{G_{\text{DK}}})$ は $PGL(3, \mathbb{F}_4)$ に等しい. Dolgachev-Kondo [3] は $X_{G_{\text{DK}}}$ の全自己同型群 $\text{Aut}(X_{G_{\text{DK}}})$ も決定している.

Artin 不変量 2 の超特異 $K3$ 曲面の同型類からなる 3 個の strata $\mathfrak{M}_{188}, \mathfrak{M}_{189}, \mathfrak{M}_{190}$ はいずれも 1 次元であり, アフィン直線 \mathbb{A}^1 から原点を取り除いたものと同型である.

$$GA[\lambda] := XYZ(X+Y+Z)(X^2+Y^2+(\lambda^2+\lambda)Z^2+XY+YZ+ZX)$$

とおく. $\lambda \notin \mathbb{F}_4$ ならば, $[GA[\lambda]]$ は \mathfrak{M}_{188} の点となる. 逆に, \mathfrak{M}_{188} の任意の点はある $\lambda \notin \mathbb{F}_4$ により $[GA[\lambda]]$ と表される.

$$J_A(\lambda) := \frac{(\lambda^2 + \lambda + 1)^3}{\lambda^2(\lambda + 1)^2}$$

とおく. \mathfrak{M} のなかで $[GA[\lambda]] = [GA[\lambda']]$ となるのは $J_A(\lambda) = J_A(\lambda')$ のときおよびそのときに限る. つまり J_A が $\mathfrak{M}_{188} \cong \mathbb{A}^1 \setminus \{0\}$ 上の自然な座標を与える. $\text{Aut}(C_{188})$ は位数 1152 の群であり, $\text{ProjAut}(X_{GA[\lambda]})$ はその位数 96 の部分群となる. $\lambda = \omega$ または $\lambda = \bar{\omega}$ のとき (すなわち $J_A(\lambda) = 0$ のとき), $[GA[\lambda]]$ の Artin 不変量は 1 になる, つまり $[GA[\lambda]] = [G_{\text{DK}}]$ となる.

$$Q_\lambda := (\bar{\omega}\lambda + \omega)X^2 + \bar{\omega}Y^2 + \omega\lambda Z^2 + (\lambda + 1)XY + (\bar{\omega}\lambda + \omega)YZ + (\lambda + 1)ZX,$$

$$GB[\lambda] := XYZ(X+Y+Z)Q_\lambda$$

とおく. $\lambda \notin \mathbb{F}_4$ ならば, $[GB[\lambda]]$ は \mathfrak{M}_{189} の点となる. 逆に, \mathfrak{M}_{189} の任意の点はある $\lambda \notin \mathbb{F}_4$ により $[GB[\lambda]]$ と表される.

$$J_B(\lambda) := \frac{(\lambda + \omega)^{12}}{\lambda^3(\lambda + 1)^3(\lambda + \bar{\omega})^3}$$

とおくと, $[GB[\lambda]] = [GB[\lambda']]$ となるのは $J_B(\lambda) = J_B(\lambda')$ のときおよびそのときに限る. つまり J_B が $\mathfrak{M}_{189} \cong \mathbb{A}^1 \setminus \{0\}$ 上の自然な座標を与える. $\text{Aut}(C_{189})$ は位数 432 の群であり, $\text{ProjAut}(X_{GB[\lambda]})$ はその位数 18 の部分群となる. $\lambda = \omega$ のとき (すなわち $J_B(\lambda) = 0$ のとき), $[GB[\lambda]]$ の Artin 不変量は 1 になる, つまり $[GB[\lambda]] = [G_{DK}]$ となる.

$$GC[\lambda] := XYZ(X^3 + Y^3 + Z^3) + (\lambda^4 + \lambda)X^3Y^3$$

とおく. $\lambda \notin \mathbb{F}_4$ ならば, $[GC[\lambda]]$ は \mathfrak{M}_{190} の点となる. 逆に, \mathfrak{M}_{190} の任意の点はある $\lambda \notin \mathbb{F}_4$ により $[GC[\lambda]]$ と表される.

$$J_C := (\lambda^4 + \lambda)^3$$

とおくと, $[GC[\lambda]] = [GC[\lambda']]$ となるのは $J_C(\lambda) = J_C(\lambda')$ のときおよびそのときに限る. つまり J_C が $\mathfrak{M}_{190} \cong \mathbb{A}^1 \setminus \{0\}$ 上の自然な座標を与える. $\text{Aut}(C_{190})$ は位数 23040 の群であり, $\text{ProjAut}(X_{GC[\lambda]})$ はその位数 960 の部分群となる. $\lambda \in \mathbb{F}_4$ のとき (すなわち $J_C(\lambda) = 0$ のとき), $[GC[\lambda]]$ の Artin 不変量は 1 になる, つまり $[GC[\lambda]] = [G_{DK}]$ となる.

以上のことからわかるように, 3 個の strata $\mathfrak{M}_{188}, \mathfrak{M}_{189}, \mathfrak{M}_{190}$ は \mathfrak{M} のなかで 1 点 $[G_{DK}]$ において交わる.

5 超特異 $K3$ 符号の同型類

No. σ	basis	1 q e t1 lq qq
----------------	-------	------------------

$\dim C = 1.$ $s(1) = 1.$

0 101	0 0 0 0 0 0
---------	---------------

$\dim C = 2.$ $s(2) = 3.$

1 9 31	1 0 0 0 0 0
2 9 255	0 1 0 0 0 0
3 9 511	0 0 1 0 0 0

$\dim C = 3.$ $s(3) = 8.$

4 8 31, 481	2 0 0 0 0 0
5 8 31, 8160	1 2 0 0 2 0
6 8 31, 2019	1 1 0 0 0 0
7 8 31, 8161	1 0 2 0 0 0
8 8 255, 3855	0 3 0 0 0 0
9 8 255, 16131	0 2 1 0 0 1
10 8 255, 7951	0 1 2 0 0 0
11 8 511, 32263	0 0 3 0 0 0

$\dim C = 4.$ $s(4) = 21.$

12 7 31, 8160, 481	3 1 0 1 3 0
13 7 31, 2019, 2301	3 0 0 0 0 0
14 7 31, 8160, 516193	2 2 0 0 2 0
15 7 31, 2019, 6244	2 2 0 0 0 0
16 7 31, 8161, 253987	2 1 1 0 0 0
17 7 31, 8160, 123360	1 6 0 0 6 0
18 7 31, 8160, 25059	1 4 0 0 2 2
19 7 31, 2019, 63533	1 3 0 0 0 3
20 7 31, 2019, 14565	1 3 0 0 0 0
21 7 31, 8160, 123361	1 2 4 0 2 0
22 7 31, 8161, 25062	1 2 2 0 0 1
23 7 31, 8161, 254178	1 1 4 0 0 0
24 7 255, 3855, 13107	0 7 0 0 0 0
25 7 255, 3855, 28951	0 6 1 0 0 3
26 7 255, 3855, 62211	0 5 2 0 0 4
27 7 255, 3855, 127249	0 4 3 0 0 3
28 7 255, 16131, 115471	0 3 4 0 0 3
29 7 255, 3855, 29491	0 3 4 0 0 0
30 7 255, 16131, 50973	0 2 5 0 0 1
31 7 255, 7951, 123187	0 1 6 0 0 0
32 7 511, 32263, 233016	0 0 7 0 0 0

$\dim C = 5.$ $s(5) = 43.$

33 6 31, 8160, 123360, 1966081	5 0 0 10 0 0
34 6 31, 8160, 25059, 28385	4 1 0 1 3 0
35 6 31, 2019, 6244, 8637	4 1 0 0 0 0
36 6 31, 8160, 25059, 105991	3 5 0 1 7 0
37 6 31, 8160, 25059, 26215	3 5 0 1 3 4
38 6 31, 8161, 253987, 319591	3 3 1 0 0 0
39 6 31, 8160, 25059, 238049	3 3 0 1 3 0
40 6 31, 8160, 25059, 42497	3 3 0 0 2 1
41 6 31, 8160, 516193, 582560	2 6 0 0 6 0
42 6 31, 8160, 25059, 100324	2 6 0 0 4 6
43 6 31, 8160, 25059, 44583	2 6 0 0 2 6
44 6 31, 2019, 63533, 68551	2 6 0 0 0 12
45 6 31, 2019, 6244, 27049	2 6 0 0 0 0
46 6 31, 8160, 25059, 492257	2 4 2 0 2 2
47 6 31, 8161, 253987, 271302	2 4 2 0 0 5
48 6 31, 8161, 253987, 288708	2 4 2 0 0 2
49 6 31, 8160, 123360, 419424	1 14 0 0 14 0
50 6 31, 8160, 25059, 241184	1 10 0 0 6 12
51 6 31, 8160, 25059, 124512	1 10 0 0 6 12
52 6 31, 8160, 25059, 492069	1 8 0 0 2 12
53 6 31, 8160, 25059, 42605	1 8 0 0 2 6
54 6 31, 8160, 123360, 419425	1 6 8 0 6 0
55 6 31, 8160, 25059, 99948	1 6 4 0 2 8
56 6 31, 8160, 25059, 238119	1 6 4 0 2 8
57 6 31, 8161, 25062, 99051	1 6 2 0 0 9
58 6 31, 8161, 25062, 42602	1 6 2 0 0 3
59 6 31, 8160, 25059, 239201	1 4 8 0 2 2
60 6 31, 8161, 25062, 229998	1 4 6 0 0 6
61 6 31, 8161, 25062, 501288	1 4 6 0 0 3
62 6 255, 3855, 13107, 21845	0 15 0 0 0 0
63 6 255, 3855, 28951, 46881	0 13 2 0 0 12
64 6 255, 3855, 28951, 492145	0 11 4 0 0 16
65 6 255, 3855, 62211, 208947	0 9 6 0 0 18
66 6 255, 3855, 28951, 233577	0 9 6 0 0 15
67 6 255, 3855, 13107, 116021	0 9 6 0 0 12
68 6 255, 3855, 127249, 405606	0 7 8 0 0 12
69 6 255, 3855, 28951, 111147	0 7 8 0 0 9

70	6	255, 3855, 13107, 54613	0	7	8	0	0	0
71	6	255, 16131, 115471, 412723	0	5	10	0	0	10
72	6	255, 3855, 127249, 144998	0	5	10	0	0	7
73	6	255, 3855, 62211, 79157	0	5	10	0	0	4
74	6	255, 16131, 115471, 396597	0	3	12	0	0	3
75	6	255, 3855, 29491, 230741	0	3	12	0	0	0

$\dim C = 6.$ $s(6) = 58.$

76	5	31, 8160, 25059, 238049, 3618	6	0	0	10	0	0
77	5	31, 2019, 6244, 8637, 19179	6	0	0	0	0	0
78	5	31, 8160, 25059, 105991, 26232	5	8	0	10	8	0
79	5	31, 8160, 25059, 105991, 147041	5	4	0	2	8	0
80	5	31, 8160, 25059, 42605, 26781	5	4	0	1	3	3
81	5	31, 8161, 253987, 288708, 894990	4	7	2	0	0	0
82	5	31, 8160, 25059, 238119, 25661	4	7	0	1	7	4
83	5	31, 8160, 25059, 42605, 98704	4	7	0	1	5	8
84	5	31, 8160, 25059, 492069, 534498	4	7	0	0	4	10
85	5	31, 8160, 25059, 105991, 394851	3	13	0	1	15	24
86	5	31, 8160, 25059, 105991, 42605	3	13	0	1	15	0
87	5	31, 8160, 25059, 238119, 377379	3	13	0	1	11	28
88	5	31, 8160, 25059, 105991, 434281	3	13	0	1	7	32
89	5	31, 8160, 25059, 42605, 2724	3	13	0	1	3	12
90	5	31, 8161, 253987, 271302, 901198	3	9	3	0	0	27
91	5	31, 8160, 25059, 42605, 100414	3	9	2	0	2	13
92	5	31, 8160, 25059, 238119, 49277	3	9	1	0	4	17
93	5	31, 8160, 25059, 105991, 140901	3	9	0	1	7	8
94	5	31, 8160, 25059, 238119, 1736	3	9	0	1	3	18
95	5	31, 8160, 25059, 492069, 106180	3	9	0	0	6	15
96	5	31, 8160, 25059, 124512, 951009	3	9	0	0	6	9
97	5	31, 8160, 25059, 238119, 1869504	2	14	0	0	8	36
98	5	31, 8160, 25059, 492069, 1615373	2	14	0	0	4	42
99	5	31, 8160, 25059, 42605, 101942	2	14	0	0	4	30
100	5	31, 8160, 25059, 241184, 370273	2	10	4	0	6	12
101	5	31, 8160, 25059, 492069, 101592	2	10	4	0	4	24
102	5	31, 8160, 25059, 238119, 884843	2	10	4	0	4	18
103	5	31, 8160, 25059, 238119, 888353	2	10	4	0	2	24
104	5	31, 8161, 253987, 288708, 622825	2	10	4	0	0	30

105	5	31, 8161, 253987, 288708, 796873	2	10	4	0	0	24
106	5	31, 8161, 253987, 288708, 567406	2	10	4	0	0	12
107	5	31, 8160, 123360, 419424, 699040	1	30	0	0	30	0
108	5	31, 8160, 25059, 124512, 494240	1	22	0	0	14	56
109	5	31, 8160, 25059, 124512, 396941	1	18	0	0	6	60
110	5	31, 8160, 25059, 124512, 166317	1	18	0	0	6	54
111	5	31, 8160, 25059, 124512, 43685	1	18	0	0	6	36
112	5	31, 8160, 123360, 419424, 699041	1	14	16	0	14	0
113	5	31, 8160, 25059, 238119, 828508	1	14	8	0	6	40
114	5	31, 8160, 25059, 238119, 372292	1	14	8	0	6	40
115	5	31, 8160, 25059, 492069, 124520	1	14	4	0	2	48
116	5	31, 8160, 25059, 238119, 885801	1	14	4	0	2	42
117	5	31, 8160, 25059, 42605, 101044	1	14	4	0	2	24
118	5	31, 8160, 25059, 124512, 436897	1	10	16	0	6	12
119	5	31, 8160, 25059, 238119, 296165	1	10	12	0	2	26
120	5	31, 8160, 25059, 42605, 477857	1	10	12	0	2	20
121	5	31, 8161, 25062, 99051, 427305	1	10	10	0	0	30
122	5	31, 8161, 25062, 99051, 173347	1	10	10	0	0	24
123	5	255, 3855, 28951, 492145, 538402	0	25	6	0	0	60
124	5	255, 3855, 28951, 492145, 564498	0	21	10	0	0	66
125	5	255, 3855, 28951, 492145, 558755	0	21	10	0	0	60
126	5	255, 3855, 28951, 492145, 110650	0	17	14	0	0	58
127	5	255, 3855, 28951, 492145, 623923	0	17	14	0	0	52
128	5	255, 3855, 28951, 233577, 893570	0	13	18	0	0	42
129	5	255, 3855, 13107, 116021, 415508	0	13	18	0	0	42
130	5	255, 3855, 28951, 492145, 570411	0	13	18	0	0	36
131	5	255, 3855, 28951, 111147, 398693	0	9	22	0	0	24
132	5	255, 3855, 127249, 144998, 284986	0	9	22	0	0	24
133	5	255, 3855, 62211, 208947, 87381	0	9	22	0	0	18

$\dim C = 7.$ $s(7) = 41.$

134	4	31, 8160, 25059, 238119, 1736, 1867799	7	7	0	11	9	0
135	4	31, 8160, 25059, 105991, 394851, 139649	7	7	0	7	21	0
136	4	31, 8160, 25059, 105991, 434281, 614571	7	7	0	3	9	12
137	4	31, 8160, 25059, 238119, 884843, 418183	6	12	0	3	15	24
138	4	31, 8160, 25059, 42605, 2724, 987586	6	12	0	2	6	18
139	4	31, 8160, 25059, 492069, 534498, 1812520	6	12	0	0	12	30

140	4	31, 8160, 25059, 238119, 372292, 29575	5	24	0	10	24	96
141	4	31, 8160, 25059, 105991, 26232, 43689	5	24	0	10	24	0
142	4	31, 8160, 25059, 238119, 884843, 1058259	5	16	0	2	16	44
143	4	31, 8160, 25059, 238119, 884843, 7297	5	16	0	2	16	20
144	4	31, 8160, 25059, 238119, 49277, 516264	5	16	0	1	11	53
145	4	31, 8160, 25059, 238119, 884843, 1409677	4	19	2	0	8	74
146	4	31, 8160, 25059, 238119, 884843, 52788	4	19	0	1	13	70
147	4	31, 8160, 25059, 238119, 884843, 1474759	4	19	0	1	9	66
148	4	31, 8160, 25059, 238119, 49277, 984106	4	19	0	0	12	78
149	4	31, 8160, 25059, 238119, 372292, 103644	3	29	0	1	23	152
150	4	31, 8160, 25059, 105991, 394851, 696425	3	29	0	1	15	184
151	4	31, 8160, 25059, 238119, 377379, 950861	3	29	0	1	15	160
152	4	31, 8160, 25059, 238119, 49277, 281774	3	21	4	0	6	111
153	4	31, 8160, 25059, 238119, 884843, 1475209	3	21	4	0	6	87
154	4	31, 8160, 25059, 238119, 884843, 1451537	3	21	2	0	10	95
155	4	31, 8160, 25059, 238119, 884843, 1352755	3	21	0	1	15	72
156	4	31, 8160, 25059, 105991, 42605, 141990	3	21	0	1	15	48
157	4	31, 8160, 25059, 238119, 372292, 699489	3	21	0	1	7	104
158	4	31, 8160, 25059, 238119, 1869504, 475241	2	30	0	0	12	186
159	4	31, 8160, 25059, 238119, 1869504, 1902665	2	30	0	0	12	162
160	4	31, 8160, 25059, 238119, 884843, 321232	2	22	8	0	8	110
161	4	31, 8160, 25059, 238119, 884843, 167565	2	22	8	0	4	122
162	4	31, 8160, 25059, 238119, 888353, 1355336	2	22	8	0	4	122
163	4	31, 8160, 25059, 124512, 494240, 700700	1	46	0	0	30	240
164	4	31, 8160, 25059, 124512, 396941, 662065	1	38	0	0	14	240
165	4	31, 8160, 25059, 238119, 372292, 955584	1	30	16	0	14	176
166	4	31, 8160, 25059, 238119, 372292, 442537	1	30	8	0	6	192
167	4	31, 8160, 25059, 238119, 372292, 950861	1	30	8	0	6	192
168	4	31, 8160, 25059, 238119, 372292, 829089	1	22	24	0	6	120
169	4	31, 8160, 25059, 238119, 296165, 591468	1	22	20	0	2	128
170	4	255, 3855, 28951, 492145, 564498, 42406	0	45	18	0	0	270
171	4	255, 3855, 28951, 492145, 564498, 722490	0	37	26	0	0	246
172	4	255, 3855, 28951, 492145, 564498, 1127602	0	29	34	0	0	190
173	4	255, 3855, 28951, 233577, 893570, 308270	0	21	42	0	0	126
174	4	255, 3855, 13107, 116021, 415508, 714818	0	21	42	0	0	126

$\dim C = 8.$ $s(8) = 13.$

175	3	31, 8160, 25059, 238119, 884843, 1474759, 475241	9	18	0	20	18	0
176	3	31, 8160, 25059, 238119, 884843, 418183, 1451537	9	18	0	16	30	48
177	3	31, 8160, 25059, 238119, 884843, 418183, 57025	9	18	0	9	27	63
178	3	31, 8160, 25059, 238119, 884843, 418183, 699489	7	31	0	5	35	182
179	3	31, 8160, 25059, 238119, 884843, 1409677, 1058259	7	31	0	3	33	204
180	3	31, 8160, 25059, 238119, 372292, 29575, 955584	5	56	0	10	56	576
181	3	31, 8160, 25059, 238119, 884843, 1451537, 699489	5	40	0	2	32	324
182	3	31, 8160, 25059, 238119, 884843, 1451537, 1474759	5	40	0	1	27	357
183	3	31, 8160, 25059, 238119, 372292, 442537, 934222	3	61	0	1	39	744
184	3	31, 8160, 25059, 238119, 884843, 1451537, 167565	3	45	6	0	18	495
185	3	31, 8160, 25059, 238119, 884843, 167565, 1352755	3	45	0	1	15	504
186	3	31, 8160, 25059, 124512, 396941, 662065, 700700	1	78	0	0	30	1008
187	3	31, 8160, 25059, 238119, 372292, 442537, 955584	1	62	16	0	14	816

$\dim C = 9.$ $s(9) = 3.$

188	2	31, 8160, 25059, 238119, 884843, 418183, 1451537, 699489	13	28	0	46	60	96
189	2	31, 8160, 25059, 238119, 884843, 418183, 699489, 152785	9	66	0	12	90	864
190	2	31, 8160, 25059, 238119, 372292, 442537, 934222, 1844576	5	120	0	10	120	2880

$\dim C = 10.$ $s(10) = 1.$

191	1	31, 8160, 25059, 238119, 884843, 418183, 1451537, 699489, 929948	21	0	0	210	0	0
-----	---	---	----	---	---	-----	---	---

参考文献

- [1] M. Artin, *Supersingular K3 surfaces*, Ann. Sci. École Norm. Sup. (4) 7 (1974), 543-567 (1975).
- [2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Springer-Verlag, New York, 1999.

- [3] I. R. Dolgachev and S. Kondō, *A supersingular $K3$ surface in characteristic 2 and the Leech lattice*, Int. Math. Res. Not. 2003, no. 1, 1–23. (2001).
- [4] P. Blass and J. Lang, *Zariski surfaces and differential equations in characteristic $p > 0$* , Marcel Dekker Inc., New York, 1987.
- [5] A. N. Rudakov and I. R. Šafarevič, *Supersingular $K3$ surfaces over fields of characteristic 2*, Izv. Akad. Nauk SSSR Ser. Mat. 42 (1978), no. 4, 848–869: Igor R. Shafarevich, Collected mathematical papers, Springer-Verlag, Berlin, 1989, pp. 614–632.
- [6] ———; *Surfaces of type $K3$ over fields of finite characteristic*, Current problems in mathematics, Vol. 18, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1981, pp. 115–207: Igor R. Shafarevich, Collected mathematical papers, Springer-Verlag, Berlin, 1989, pp. 657–714.
- [7] I. Shimada, *Lattices of algebraic cycles on Fermat varieties in positive characteristics*, Proc. London Math. Soc. (3) 82 (2001), no. 1, 131–172.
- [8] ———, *Rational double points on supersingular $K3$ surfaces*, Math. Comp. 73 (2004), no. 248, 1989–2017 (electronic).
- [9] ———, *Supersingular $K3$ surfaces in characteristic 2 as double covers of a projective plane*, preprint, to appear in Asian J. Math.
<http://www.math.hokudai.ac.jp/~shimada/ssK3.html>
- [10] ———, *Supersingular $K3$ surfaces as double covers of the projective plane* (日本語), 京都大学数理解析研究所講究録, No. 1345, 代数曲線束の局所不変量の研究, 89–108. http://www.math.hokudai.ac.jp/~shimada/ronzetsu_j.html
- [11] ———, *Moduli curves of supersingular $K3$ surfaces in characteristic 2 with Artin invariant 2*, preprint.
<http://www.math.hokudai.ac.jp/~shimada/ssK3.html>
- [12] T. Shioda, *Supersingular $K3$ surfaces*, Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978), Lecture Notes in Math., Vol. 732, Springer, Berlin, 1979, pp. 564–591.

060-0810

札幌市北区北10条西8丁目

北海道大学理学部数学教室

shimada@math.sci.hokudai.ac.jp

長さ 72 の extremal doubly even self-dual code に 関係した 5-design について*

原田昌晃 (山形大), 北詰正顕 (千葉大)[†], 宗政昭弘 (東北大)

1 序文

まず最初に, 今回の講演, ならびに, この原稿は, 講演者を含む著者 3 人の共著論文 ([3]) に基づいていることを明記しておく。

よく知られているように, 長さ 72 の extremal doubly even self-dual code の存在は知られておらず, 否定されてもいない。長く未解決となっている, 有名な問題である ([6])。残念なことながら, 本稿で符号・デザインの存否に関係したり, 言及したりするような結果を述べるわけではない。

この符号が存在すると Assmus-Mattson の定理から, $5-(72, 16, 78)$ デザインが存在するが, このデザイン自体の存在がわかっていない。今回の結果は, デザインの存在を仮定して (ただし, デザインのブロックについて, 符号語として内積が 0 であるという条件 (後述の "self-orthogonal") も仮定して) そのブロックを符号語として符号を生成させると, 「問題の符号」が生成されることが, 比較的簡単な計算から得られることを示すことである。

なお, 集会終了後に主張を少し強めることが出来ることがわかったので, ここでは強めた形で書いておくことにした。具体的な違いについては, 3 節をご覧ください。

*2004.06.29 代数的組合せ論シンポジウム (於: 信州大学理学部)

[†]講演者であり, 本稿の文責を負う。

2 符号とデザインに関する準備

まず幾つか言葉の説明から始めることにする。2元体 \mathbb{F}_2 上の n 次元行ベクトル空間の部分空間を、長さ n の符号と呼ぶ。符号に属するベクトルは符号語 (codeword) と呼ばれる。通常の内積を考えて、 $C = C^\perp$ がみたされるとき、符号 C は self-dual であると言う。さらに、ベクトルの 0 でない成分の個数を、その weight (重み) と呼ぶが、全ての符号語の weight が 4 の倍数であるとき、doubly even と言う。doubly even self-dual を、より短く Type II と呼ぶことにする。Type II code が存在するための必要十分条件は、 n が 8 の倍数であることが知られている。

符号においては、その誤り訂正能力との関連もあって、0 でない符号語の weight の最小値が重要である。特に self-dual code の場合に、その値がある種の理論値 ([1], p.189) の限界であるとき extremal であると呼ばれる。長さ $24m$ の Type II code の場合、その限界は $4m+4$ となるので、長さ $24m$ の extremal Type II code とは、その最小 weight が $4m+4$ であるものと定義する。すなわち $[24m, 12m, 4m+4]$ -code の事である。長さを 24 の倍数に限定したのは、24 の倍数ごとに理論値の限界が跳ね上がるからである。例えば、長さ 32, 40 のときも、その限界値は 24 のときと同じ値である。長さ 24, 48 の extremal code は、共に、extended quadratic residue code として与えられる。24 の場合は、有名な extended Golay code である。共に、その長さでただ一つの extremal Type II code であることがわかっている。(後者については、最近の [5] による結果である。) 長さ 72, 96 の extremal code は存在・非存在が知られていない。それ以上の長さについても同様であるが、長さを大きくしてゆくに従って、非存在が確信されるようになってきているようである。実際、 $n \geq 24 \times 154$ ならば非存在であることが知られている。未解決問題としては、72, 96 あたりまでが良いところのようである。

長さ 24, 48 の extremal Type II code の最小 weight (それぞれ 8, 12) の符号語の全体を考えると、5-(24,8,1), 5-(48,12,8) というパラメータのデザインが作られる。ここで、 t -(v, k, λ) デザインとは、 v 個の "点" からなる集合 Ω と、"ブロック" と呼ばれる k 点部分集合のある族 B のペア (Ω, B) で、 Ω の任意の t 点部分集合を含むブロックの個数が、一定値 λ であるものことである。符号語から作るときは、 Ω をベクトル空間の成分の index $\{1, 2, \dots, n\}$ とし、符号語の 0 でない成分の index の集合をブロックとするのである。逆に言えば、符号語とは Ω の部分集合のことであると言っても差し支えない。そうした場合、ベクトルの和は部分集合の対称差 $(A \cup B) \setminus (A \cap B)$ に対応する。また、weight とは集合の濃度に他ならない。

符号から作るデザインについては、有名な一般論があって、Assmus-Mattson の

定理として知られている。符号の性質から、デザインであることを導く定理であるが、ここでは内容は省略する。もし、長さ 72 の extremal Type II code が存在するならば、そこから 5-(72,16,78) デザインが作られることが、この定理から示される。

t -design は $i \leq t$ なる非負整数 i に対して、 i -design でもある。すなわち i 個の点を含むブロックの個数 λ_i は一定である。定義から λ_0 とはブロックの総数であり、 $\lambda_t = \lambda$ である。一般に、初等的な計算から

$$\lambda_i = \lambda \binom{v-i}{t-i} / \binom{k-i}{t-i}$$

が得られる。5-(72, 16, 78) デザインの場合、

$$\lambda_0 = 249849, \lambda_1 = 55522, \lambda_2 = 11730, \lambda_3 = 2346, \lambda_4 = 442, \lambda_5 = 78.$$

である。もう少し一般に、5-(72, 16, λ) デザインの場合、

$$\lambda_0 = \frac{249849}{78} \lambda, \lambda_1 = \frac{55522}{78} \lambda, \lambda_2 = \frac{11730}{78} \lambda, \lambda_3 = \frac{2346}{78} \lambda, \lambda_4 = \frac{442}{78} \lambda, \lambda_5 = \lambda,$$

である（あえて分数の約分はしていない）。

3 主結果とその証明

主結果を述べるために、ひとつだけ定義を付け加える。デザインが self-orthogonal であるとは、任意の 2 つのブロックの共通部分の濃度が、ブロックの濃度 k と偶奇が一致することを意味するものとする。今の場合は $k = 16$ なので、2 つのブロックが偶数個で交わるということである。self-dual code から作られたデザインが、この意味で self-orthogonal であることは、内積が 0 であることから容易に得られる。5-(24,8,1) デザインは、このパラメータから self-orthogonal であることが言える（例えば "How many octads" ([1], p.278) による）。他の場合 (48, 72) について、同じ parameter の non self-orthogonal デザインが存在するかどうか、というのも興味ある問題であろう。

定理. Self-orthogonal 5-(72, 16, λ) design のブロックは、長さ 72 の extremal Type II code を生成する。従って、 $\lambda = 78$ である。特に、長さ 72 の extremal Type II code があれば、その weight 16 の符号語が符号を生成する。

集会当日は、 $\lambda = 78$ を最初から仮定して主張を述べ、それを証明した。その後、主張を少し強められることがわかったので、上記の形にまとめることにした。"self-orthogonal" という仮定を付けておくと、 λ は大きくも小さくもなれない、というのは面白いと思う。

証明は、基本的な議論による。以下、その全てを記述することにしよう。

Self-orthogonal $5-(72, 16, \lambda)$ design D が存在すると仮定し、そのブロックが生成する符号を C で表す。ブロックサイズが 4 の倍数 16 であることと、仮定 (D : self-orthogonal) から C は doubly even self-orthogonal である。その dual code C^\perp を考える。

Step 1. $w \in C^\perp$ とし、 $m = \text{wt}(w)$ とおく。最初の節で述べたように、 $\Omega = \{1, 2, \dots, 72\}$ とおき、 \mathbb{F}_2^{72} のベクトル (特に w) を Ω の部分集合と見なすことにする。このとき、 n_i を

D のブロックで w との共通部分の濃度が i であるものの個数

と定義する。簡単な計算 (double counting) により、次の等式 (n_i に関する連立方程式) が成り立つ。

$$(1) \quad \sum_{i=0}^8 n_{2i} \binom{2i}{j} = \binom{m}{j} \lambda_j \quad (j = 0, 1, \dots, 5).$$

右辺は、 w の m 個の中から j 個を選んでから、その j 個を含むブロックの個数 λ_j をかけたものである。左辺では、そのようなブロックの総数を w との共通部分の濃度ごとに計算したものである。 $w \in C^\perp$ ゆえ、 C の元であるブロックとの共通部分は偶数個であり、ブロックの weight は 16 であるから、未知数は n_{2i} ($i = 0, 1, \dots, 8$) の 9 つである。

Step 2. $n_{2i} \neq 0$ ($\exists i \geq 5$).

証明. 6 つの式からなる連立方程式を実際に解いてみる。すると、 n_0 から n_{10} までの 6 つの未知数を、残りの n_{12} から n_{16} で表すことが出来る。特に、 n_{10} については、

$$n_{10} = \alpha - 6n_{12} - 21n_{14} - 56n_{16}$$

となる。ただし、

$$\begin{aligned} \alpha &= \frac{\lambda}{78 \times 1920} (3650496m - 800440m^2 + 67410m^3 - 2600m^4 + 39m^5) \\ &= \frac{\lambda m}{78 \times 1920} \left(39 \left(m^2 - \frac{100}{3}m + 275 \right)^2 + \frac{7880}{3} \left(m - \frac{3204}{197} \right)^2 + \frac{1245957}{197} \right). \end{aligned}$$

平方完成した式から $\alpha \neq 0$ がわかるので、ここでの結論を得る。 \square

Step 3. $C^\perp = C$.

証明. w として $C^\perp \setminus C$ の元で, weight が最小のものを取る. すると, Step 2 により, ブロック b で w と 10 点以上で交わるものがあるので, $b+w \in C^\perp$ を考えると, ベクトルの和は集合の対称差であるから,

$$\text{wt}(b+w) = \text{wt}(b) + \text{wt}(w) - 2|b \cap w| \leq 16 + \text{wt}(w) - 2 \times 10 = \text{wt}(w) - 4$$

となって, w の weight が最小であるという仮定より $b+w \in C$ を得る. よって $w \in C$ となり, 仮定 $w \in C^\perp \setminus C$ に反する. これは $C^\perp = C$ を意味している. \square

Step 4. $\min(C) = 16$.

証明. w として $C \setminus \{0\}$ の weight が最小のものを取れば, Step 3 と全く同様の議論で, w の weight の最小性から, $b+w=0$ を得る. すなわち, $\text{wt}(w) = 16$ が C の minimum weight である. \square

Step 5. $\lambda = 78$.

証明. Step 4 において $w=b$ が示されたので, C の weight 16 の元は, 全てデザイン D のブロックから得られることも示されている. 従って, デザインから作られた符号 C から, Assmus-Mattson の定理で与えられるデザインは D に一致する. それは 5-(72, 16, 78) デザインである. すなわち $\lambda = 78$ である.

最後の部分の議論を, 少し丁寧に書いておく. Assmus-Mattson の定理は D が 5-design であることを保証する. 一方, Type II [72, 36, 16]-code の weight enumerator は符号のパラメータから一意に決まる. つまり, 各 weight の符号語の個数はパラメータだけから決まる. 特に weight 16 の符号語 (すなわち, デザイン D のブロック) の個数が 249849 と決まる. この値が, 2 節の λ_0 でなければならぬから, $\lambda = 78$ が得られる. \square

以上で, 定理は証明された. \square

4 付記

(1) まず, 裏話を少し書いておく. 一番最初に得た証明では, C^\perp の元の weight m に関する数学的帰納法を用いて, 連立方程式 (1) に m を代入しながら議論を進めていた. Step 2 の主張に気が付いて, このような簡素な証明になったのである. ただし, 出版された論文には (本質的に同じ議論であるが) 数学的帰納法の名残が残っ

ていて、少々心残りである。本稿では、さらに λ を決めずに議論を進めて、少し強い主張を述べた。本稿での証明（および、定理の主張）を決定版としたい。

(2) 前節の議論，特に Step 1 の連立方程式を立てる部分は，全く一般的な（標準的な）方法である。特に，系列とも言える $5-(24,8,1)$, $5-(48,12,8)$ というデザインについても同様の議論が可能である。これらの場合はブロックのサイズが小さいので，Step 2 の主張は，

$$24 \text{ のとき } n_{2i} \neq 0 \ (\exists i \geq 3), \quad 48 \text{ のとき } n_{2i} \neq 0 \ (\exists i \geq 4)$$

となる。すなわち，ブロックサイズの半分より大きい intersection で交わるブロックが存在するという主張である。非常に雑にいうと，その証明の心は，

$$24 \text{ (resp. } 48) \text{ の場合に } n_{2i} = 0 \ (\forall i \geq 3 \text{ (resp. } 4)) \text{ を仮定すると矛盾する}$$

というものである。この仮定の下では，残っている未知数は 3 つ (resp. 4 つ) である。とすると，方程式 (1) の式が 6 つというのは（感覚的に）多すぎると言える。実際，これらの場合には (1) の 6 つの式は不要である。すなわち，

$$5-(24,8,1) \text{ design は self-orthogonal 3-design として，}$$

$$5-(48,12,8) \text{ design は self-orthogonal 4-design として，}$$

同様の議論を続けることが出来て（従って，式の数はそれぞれ 4 と 5 になる）ブロックの生成する符号が，それぞれの長さ (24, 48) の extremal code を生成することが示されるのである。さらに，前節の最後にも注意したように，ブロックと minimum weight の符号語とは一致するから，extremal code の一意性からデザインの一意性も示される ([4])。

今の話は同時に，我々の議論が 96 点上のデザインと，長さ 96 の extremal code には通用しないことを示してもいるようである。Assmus-Mattson の定理では 96 点の場合でも 5-design であることしか，保証してくれないからである。しかし，集会終了直後の原田昌晃氏からの連絡によると，weight enumerator に関する議論を併用することによって，（全く同様の議論ではないが）同様の結果を得たということである ([2])。

(3) 今述べたように， $5-(24,8,1)$ design については 3-design としての連立方程式で十分であったが，しかしそれは，5-design としての情報が不要というのではない。やはり，情報をフルに活用すれば，それなりの成果は得られるというものである。以下の件は，原田昌晃氏 ([7]) による。

5-design として 6 つの式を考える。 $w \in C^\perp$ とすれば、未知数は n_0, n_2, n_4, n_6, n_8 の 5 つである。そこで、この連立方程式が解を持つための条件を求めてみるのである。結果は m に関する式が出てくるわけであるが、 $\binom{m}{5}$ を含んでいるから m の 5 次式が出て来る。これがきれいに因数分解できるのは、当然とは言え、なかなか感動的である。

$$m^5 - 60m^4 + 1280m^3 - 11520m^2 + 36864m \\ = m(m - 8)(m - 12)(m - 16)(m - 24) = 0.$$

このことから、 C^\perp が doubly even であることがわかり、従って、 $C = C^\perp$ と $\min(C) = 8$ が直ちに得られる。

参考文献

- [1] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups* (3rd ed.), Springer-Verlag, New York, 1999.
- [2] M. Harada, Remark on a 5-design related to a putative extremal doubly-even self-dual [96, 48, 20] code, to appear in *Designs, Codes and Cryptography*.
- [3] M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly even self-dual code of length 72, *Journal of Combinatorial Theory (A)*, **107** (2004), 143–146.
- [4] M. Harada, A. Munemasa, and V. D. Tonchev, A characterization of designs related to an extremal doubly-even self-dual code of length 48, submitted.
- [5] S. K. Houghten, C. W. H. Lam, L. H. Thiel and J. A. Parker, The extended quadratic residue code is the only (48, 24, 12) self-dual doubly-even code, *IEEE Trans. Inform. Theory* **49** (2003), 53–59.
- [6] N. J. A. Sloane, Is there a (72, 36) $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.
- [7] 原田昌晃, 室蘭工業大学数学談話会.

Bounds for Binary Matroids

Keisuke SHIROMOTO

Department of Information Systems

Aichi Prefectural University

Nagakute, Aichi 480-1198, JAPAN;

`keisuke@ist.aichi-pu.ac.jp`

1 Introduction

The following bounds are famous bounds on the minimum Hamming weight for binary $[n, n/2, d]$ self-dual code C ([10], [9]):

$$d \leq 2 \lfloor \frac{n}{8} \rfloor + 2.$$

In this note, we give similar bounds for binary matroids from the concept of binary matroids.

2 Notation and Terminology

We begin by introducing matroids, as in [11]. A *matroid* is an ordered pair $M = (E, \mathcal{I})$ consisting of a finite set E and a collection \mathcal{I} of subsets of E satisfying the following three conditions:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.

(I3) If I_1 and I_2 are in \mathcal{I} and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup e \in \mathcal{I}$.

The members of \mathcal{I} are the *independent sets* of M , and a subset of E that is not in \mathcal{I} is called *dependent*. A minimal dependent set in M is called a *circuit* of M , and a maximal independent set in M is called a *base* of M . For a subset X of E , we define the *rank* of X as follows:

$$r(X) := \max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\}.$$

The *dual matroid* M^* of M is defined as the matroid, the set of bases of which is

$$\{E - B : B \text{ is a base of } M\}.$$

When we denote the rank of M^* by r^* , the following is well-known:

$$r^*(X) = |X| - r(M) + r(E - X).$$

A matroid M is called to be *identically self-dual* (ISD) if $M = M^*$ (cf. [1], [8], [7]).

For a matroid $M = (E, \mathcal{I})$ and a subset T of E , it is easy to check that $M \setminus T = (E - T, \{I \subseteq E - T : I \in \mathcal{I}\})$ is a matroid which is called the *deletion of T from M* . The *contraction of T from M* is given by

$$M/T = (M^* \setminus T)^*.$$

For a binary $m \times n$ matrix A , if E is the set of column labels of A and \mathcal{I} is the set of subsets X of E for which the multiset of columns labeled by X is linearly independent in the binary vector space \mathbb{F}_2^m , then $M[A] := (E, \mathcal{I})$ is a matroid and is called *binary matroid of A* (cf. [11], [14]).

For a binary vector $\mathbf{x} = (x_1, \dots, x_n)$ and a subset $\mathcal{D} \subseteq \mathbb{F}_2^n$, we define the *supports* of \mathbf{x} and \mathcal{D} respectively as follows:

$$\begin{aligned} \text{supp}(\mathbf{x}) &:= \{i \mid x_i \neq 0\}, \\ \text{Supp}(\mathcal{D}) &:= \bigcup_{\mathbf{x} \in \mathcal{D}} \text{supp}(\mathbf{x}). \end{aligned}$$

Let \mathcal{C} be a binary $[n, k]$ code. For each r , $1 \leq r \leq k$, the r -th *generalized Hamming weight* (GHW) $d_r(\mathcal{C})$ is defined by Wei ([13]) as follows:

$$d_r(\mathcal{C}) := \min\{|\text{Supp}(\mathcal{D})| : \mathcal{D} \text{ is an } [n, r] \text{ subcode of } \mathcal{C}\}.$$

As a connection between supports of a binary code and its binary matroid, the following results are well-known (Theorem 3.1 and Lemma 3.4 in [2]).

Proposition 2.1 *For a binary $[n, k]$ code \mathcal{C} and r , $1 \leq r \leq k$, the family of minimal supports $\text{Supp}(\mathcal{D})$ of $[n, r]$ subcodes \mathcal{D} of \mathcal{C} forms the family $\mathcal{F}_{\nabla}^*(\mathcal{M}_{\mathcal{C}})$ of cocircuits of the $(r - 1)$ the truncation $T^{r-1}(\mathcal{M}_{\mathcal{C}})$ of the binary matroid $\mathcal{M}_{\mathcal{C}}$. And $\mathcal{F}_{\nabla}^*(\mathcal{M}_{\mathcal{C}})$ consists of the minimal unions of r cocircuits $C_1^*, C_2^*, \dots, C_r^*$ of $\mathcal{M}_{\mathcal{C}}$ that satisfy the condition*

$$C_j^* \not\subseteq \bigcup_{i \neq j} C_i^*, \tag{1}$$

for all j .

3 Bounds for binary matroids

Let M be a binary matroid. We define the *girth* $g(M)$ of M as follows:

$$g(M) = \min\{|C| : C \text{ is a circuit of } M\}$$

Proposition 3.1 (p. 317 in [11]) *Let C be a circuit of a matroid M which has no minor isomorphic to $U_{k,k+2}$ and let e be an element of $E(M) - C$. Then, in M/e , either C is a circuit, or, for some positive integer $n \leq k$, there is a partition of C into non-empty subsets X_1, X_2, \dots, X_n such that each of the sets $C - X_1, C - X_2, \dots, C - X_n$ is a circuit. In both case, M/e has no other circuits contained in C .*

Theorem 3.2 *Let M be a binary matroid of rank r . If M has a dependent set C such that $|C| = i$ for an i such that $r \leq i \leq r + 4$ and C is a circuit or disjoint union of circuits, then $2g(M) - 4 \leq r$.*

Proof. If C is a disjoint union of circuits, then there exist at least two disjoint circuits C_1 and C_2 contained in C . So we have that

$$r + 4 \geq |C| \geq |C_1| + |C_2| \geq 2g(M).$$

If $|C| \geq r + 2$, then C is not a circuit of M and so the theorem holds. Thus we assume that C is a circuit and so $i = r + 1$ or r .

(1) $i = r + 1$

For $e \in E - C$, C is not a circuit in M/e , because of $r(M/e) = r - 1$. So $C = C_1 \cup C_2$ for disjoint circuits C_1, C_2 in M/e by Proposition 3.1. It follows that

$$r + 1 \geq |C_1| + |C_2| \geq (g(M) - 1) + (g(M) - 1) = 2g(M) - 2.$$

(2) $i = r$

If, for $e_1 \in E - C$, C is not a circuit in M/e_1 , then the theorem follows as well as the case (1). We assume that C is a circuit in M/e_1 . Since $r(M/e_1/e_2) = r - 2$ for $e_1 \neq e_2 \in E - C$, C is not a circuit in $M/e_1/e_2$ and so $C = C_1 \cup C_2$ for disjoint circuits C_1, C_2 in $M/e_1/e_2$. Therefore we have that

$$r \geq |C_1| + |C_2| \geq (g(M) - 2) + (g(M) - 2) = 2g(M) - 4.$$

The theorem follows. □

For a binary matroid M , we consider the dual matroid of the (first) truncation $T^1(M) = T(M)$, that is, the (first) Higgs lift $L^1(M) = L(M)$. From Proposition 2.1, it finds that a circuit D in $L(M)$ is a minimal union of two distinct circuits of M . The following lemmas are essential.

Lemma 3.3 *Let M be a $GF(q)$ -representable matroid of rank r . If C is a circuit of M such that $|C| = r + 1$ and e is an element of $E - C$, then C contains at least one circuit of M/e .*

Proof. Since $U_{q,q+2}$ is a excluded minors of M and C is not a circuit of M/e , the lemma follows from Proposition 3.1. □

Lemma 3.4 *Let M be a binary matroid of rank r . Then $T(M)$ and $L(M)$ are representable over $GF(2^{r-1})$.*

Proof. See Proposition 9 in [3] and [15]. □

Then we have the following lemmas.

Lemma 3.5 *Let M be a binary matroid of rank r . If M has a dependent set C such that $|C| = i$ with $r \leq i \leq r + 4$ and C is a disjoint union of circuits of M , then $2g(L(M)) + g(M) - 8 \leq 2r$.*

Lemma 3.6 *Let M be a binary matroid of rank r with $n - r \geq 4$. If M has a circuit C such that $|C| = i$ for $i = r$ or $r + 1$, then $2g(L(M)) + g(M) - 8 \leq 2r$.*

Proof. We take a base B of M such that, for an $e \in C$, B contains $C - e$. We consider two different fundamental circuits $C_1 = C(e_1, B)$ and $C_2 = C(e_2, B)$ with respect to B , where $e_1, e_2 \in E - B - \{e\}$ and $e_1 \neq e_2$.

(1) $i = r + 1$

Without loss of generality, we can assume that $|C_1| \leq (r+3)/2$ and $|C_2| \leq (r+3)/2$, because if $|C_j| > (r+3)/2$, then we may take other circuit C'_j of M which is contained in $C \Delta C_j$. It follows that

$$g(L(M)) \leq |C_1 \cup C_2| = |C_1| + |C_2| - |C_1 \cap C_2| \leq r + 3 - |C_1 \cap C_2|.$$

Since $C_1 \Delta C_2$ is not equal to C , $C \Delta C_1 \Delta C_2$ is not empty and so has a circuit of M . Therefore we have that

$$\begin{aligned} g(M) &\leq |C \Delta C_1 \Delta C_2| \\ &= |C| + |C_1 \Delta C_2| - 2|C \cap (C_1 \Delta C_2)| \\ &= |C| + |C_1 \Delta C_2| - 2(|C_1 \Delta C_2 - \{e_1, e_2\}|) \\ &= r + 1 - |C_1 \cup C_2| + |C_1 \cap C_2| + 4 \\ &\leq r + 5 - g(L(M)) + (r + 3 - g(L(M))) = 2r + 8 - 2g(L(M)) \end{aligned}$$

(2) $i = r$

Let m be an integer which is 1 or 2. Because of $n - r \geq 4$, we can take circuits C_1 and C_2 such that $|C_j - C| = m$ for all $j = 1, 2$. From the same argument as the above case, we can assume that $|C_1| + |C_2| \leq r + 2m$. So we have that

$$g(L(M)) \leq r + 2m - |C_1 \cup C_2|.$$

Thus it follows that

$$\begin{aligned} g(M) &\leq |C \Delta C_1 \Delta C_2| \\ &= |C| + |C_1 \Delta C_2| - 2|C_1 \Delta C_2 - \{e_1, e_2\}| \\ &= r - |C_1 \cup C_2| + |C_1 \cap C_2| + 4 \\ &\leq r - g(L(M)) + (r + 2m - g(L(M))) + 4 \\ &\leq 2r + 8 - 2g(L(M)) \end{aligned}$$

The lemma follows. □

By combining Lemma 3.5 and 3.6, we have the following theorem.

Theorem 3.7 *Let M be a binary matroid of rank r with $n - r \geq 4$. If M has a dependent set C such that $|C| = i$ for an i such that $r \leq i \leq r + 4$ and C is a circuit or disjoint union of circuits of M , then $2g(L(M)) + g(M) - 8 \leq 2r$.*

4 Weight Distributions for Binary Codes

Since a cocircuit of M_C corresponds to a minimal support of a codeword of C and a cocircuit of $L(M_C)$ corresponds to a minimal support of a two dimensional subcode of C , we have the following results from Theorem 3.2 and 3.7.

Corollary 4.1 *Let C be an $[n, k, d]$ binary code. If $A_i \neq 0$ for an i such that $n - k \leq i \leq n - k + 4$, then $2d - 4 \leq n - k$.*

Corollary 4.2 *Let C be an $[n, k, d]$ binary code with $k \leq 4$. If $A_i \neq 0$ for an i such that $n - k \leq i \leq n - k + 4$, then*

$$2d_2 + d - 8 \leq 2(n - k).$$

So we shall investigate weight distributions for binary codes.

4.1 Krawtchouk Polynomials

For a positive integer n , the *binary Krawtchouk polynomial* is defined as follows (cf. [9]):

$$P_m(x) = \sum_{j=0}^m (-1)^j \binom{x}{j} \binom{n-x}{m-j}, \quad m = 0, 1, \dots, n.$$

And the polynomials satisfy the following equations:

$$(1+z)^{n-x}(1-z)^x = \sum_{m=0}^{\infty} P_m(x)z^m$$

$$P_m(i) = (-1)^i P_{n-m}(i), \quad i = 0, 1, \dots, n$$

$$\binom{n}{i} P_m(i) = \binom{n}{m} P_i(m), \quad \text{for integers } m \text{ and } i$$

$$(n-m)P_i(m+1) = (n-2i)P_i(m) - mP_i(m-1), \quad \text{for nonnegative integers } m \text{ and } i.$$

For an $[n, k]$ binary code C , it follows from the MacWilliams identity that

$$2^k A_m^\perp = \sum_{i=0}^n A_i P_m(i), \quad m = 0, 1, \dots, n \quad (2)$$

In [5] and [6], it was shown that

$$P_{n/2}(i) = (-1)^{i/2} \binom{n}{n/2} \binom{n/2}{i/2} / \binom{n}{i}, \quad (3)$$

for even n and i .

Proposition 4.3 *Let C be an $[n, k, d]$ binary code such that $n/2 \leq k \leq n/2 + 4$ and n is even. If the weights of all codeword of C^\perp are divisible by 4, then $2d - 4 \leq n - k$ and $2d_2 + d - 8 \leq 2(n - k)$.*

Proof. From (2) and (3), we have that

$$2^{n-k} A_{n/2} = \sum_{j=0}^{\lfloor n/4 \rfloor} A_{4j}^\perp P_{n/2}(4j) > 0.$$

Since $A_{n/2} \neq 0$ and $n/2 \leq k \leq n/2 + 4$, the proposition follows. \square

Corollary 4.4 *If C is a doubly-even self-dual code, then*

$$d_2 \leq \begin{cases} \frac{3}{8}n & (n \equiv 0 \pmod{16}) \\ \frac{3}{8}n + 3 & (\text{otherwise}) \end{cases}$$

Remark 4.5 The equality in the above bound holds for doubly-even self-dual codes of length 8,16,24,32 and 48.

References

- [1] J. A. Bondy and D. J. A. Welsh, Some results on transversal matroids and constructions for identically self-dual matroids, *Quart. J. Math. Oxford Ser. (2)*, **23** (1972), pp. 81–89.
- [2] T. Britz, Higher support matroids, preprint.
- [3] T. Britz, The supports of linear codes, preprint.
- [4] J. H. Conway and N. J. A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), pp. 1319–1333.
- [5] I. Krasikov and S. Litsyn, On spectra of BCH codes, *IEEE Trans. Inform. Theory* **41** (1995), pp. 786–788.
- [6] I. Krasikov and S. Litsyn, Linear programming bounds for doubly-even self-dual codes, *IEEE Trans. Inform. Theory* **43** (1997), pp. 1238–1244.
- [7] J. Graver, Boolean designs and self-dual matroids, *Linear Algebra and its Applications*, **10** (1975), pp. 111–128.
- [8] B. Lindström, On binary identically self-dual matroids, *Europ. J. Combinatorics*, **5** (1984), pp. 55–58.

- [9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.
- [10] C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Inform. Contr.*, **22** (1973), pp. 188–200.
- [11] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.
- [12] E. M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), pp. 134–139.
- [13] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991) pp. 1412–1418.
- [14] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.
- [15] N. White, *Theory of Matroids*, Cambridge University Press, Cambridge-New York, 1986.

A Characterization of Tight Graphs

Rie Hosoya

Department of Mathematics
International Christian University

In this talk, we characterize a tight distance-regular graph Γ with respect to a completely regular code Y of width 2. We introduce a *homogeneous property with respect to a subset*, which is a generalization of the 1-homogeneous property in the sense of K. Nomura. We show that Γ is a tight graph with respect to Y if and only if Γ is homogeneous with respect to Y whenever Y satisfies some conditions.

This is the joint work with Hiroshi Suzuki (ICU).

1 Preliminaries

Let X be a finite set. $\text{Mat}_X(\mathcal{C})$ denotes the set of the matrices indexed by X whose entries belong to \mathcal{C} . Let $V = \mathcal{C}^X$.

Let \hat{x} ($x \in X$) denote the vector in V whose x -th coordinate is 1 and others are 0. Then the set $\{\hat{x} \mid x \in X\}$ forms a basis of V . For a subset Y of X , let $1_Y = \sum_{y \in Y} \hat{y}$. The vector 1_Y is called the *characteristic vector* of Y .

Let $\Gamma = (X, R)$ be a connected graph with vertex set X and edge set R . Let $\partial(x, y)$ denote the distance between $x, y \in X$, and D the *diameter* of Γ . Let $\Gamma_i(x) = \{y \in Y \mid \partial(x, y) = i\}$. We write $\Gamma(x) = \Gamma_1(x)$. Let $k(x) = |\Gamma(x)|$. We call $k(x)$ the *valency* of x . We say Γ is *regular* of valency k if $k = k(x)$ is independent of $x \in X$. Moreover, we say Γ is *distance-regular* if for all integers h, i, j ($0 \leq h, i, j \leq D$) and for all vertices $x, y \in X$ with $\partial(x, y) = h$, the number

$$p_{ij}^h = |\Gamma_i(x) \cap \Gamma_j(y)|$$

is independent of x and y . We abbreviate $c_i = p_{1i-1}^i$ ($1 \leq i \leq D$), $a_i = p_{1i}^i$ ($0 \leq i \leq D$), and $b_i = p_{1i+1}^i$ ($0 \leq i \leq D-1$).

For $0 \leq i \leq D$, let A_i be the matrix in $\text{Mat}_X(\mathcal{C})$ with xy -entry

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } \partial(x, y) = i. \\ 0 & \text{otherwise.} \end{cases}$$

We call A_i the *i -th distance matrix* of Γ . For notational convenience we define $A_i = 0$, for $i < 0$ and $i > D$. We abbreviate $A = A_1$ and call it the *adjacency matrix* of Γ . Let \mathcal{M} be the subalgebra of $\text{Mat}_X(\mathcal{C})$ generated by A . We refer to \mathcal{M} as the Bose-Mesner algebra of Γ . We can verify that A_0, A_1, \dots, A_D form a basis for \mathcal{M} . A has $D+1$ distinct eigenvalues: $\theta_0, \theta_1, \dots, \theta_D$ where $\theta_0 > \theta_1 > \dots > \theta_D$.

Let E_i be the projection onto the eigenspace of A with respect to θ_i . Then we have

$$V = E_0V + E_1V + \cdots + E_DV. \quad (1)$$

Let $m_i (0 \leq i \leq D)$ be the rank of E_i , i.e., the dimension of E_iV . It is known that E_0, E_1, \dots, E_D form a basis of \mathcal{M} . They are called the *basis of primitive idempotents*.

2 Terwilliger Algebras with respect to Subsets

Throughout the paper, we assume $\Gamma = (X, R)$ is a distance-regular graph of diameter $D \geq 3$.

Let Y be a subset of X . We define the *width* $w = w(Y)$ of Y as follows.

$$w = w(Y) = \max\{\partial(y, y') \mid y, y' \in Y\}.$$

Let $\Delta = \Delta(Y) = (Y, R|_{Y \times Y})$ be the subgraph of Γ induced from Y . In this paper, we assume Δ is regular.

We call a subset Y in Γ a *code* of Γ . Let $Y_i = \{z \in X \mid \partial(z, Y) = \min\{\partial(z, y) \mid y \in Y\} = i\}$, i.e., the i -th subconstituent with respect to Y ($0 \leq i \leq D$). Obviously, we get $Y = Y_0$. Let $\tau = \min\{i \mid 0 \leq i \leq D, Y_i \neq \emptyset\}$. We call τ the *covering radius* of a code Y . Then we have the following *distance partition* of X with respect to Y .

$$X = Y \cup Y_1 \cup \cdots \cup Y_\tau. \quad (2)$$

A code Y is said to be a *completely regular code* of Γ if for all integers h, i, j ($0 \leq h, i \leq \tau, 0 \leq j \leq D$) and for all vertices $z \in Y_h$, the number

$$\pi_{ij}^h = |Y_i \cap \Gamma_j(z)|$$

is independent of z .

Let Y be a subset of X (or a code of Γ). Let $E_i^* = E_i^*(Y)$ ($0 \leq i \leq \tau$) denote the projection matrix onto Y_i , i.e., the diagonal matrix in $\text{Mat}_X(C)$ with zz -entry

$$(E_i^*)_{zz} = \begin{cases} 1 & \text{if } z \in Y_i. \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathcal{T} = \mathcal{T}(Y) = \langle A, E_0^*, E_1^*, \dots, E_\tau^* \rangle$ denote the algebra generated by the adjacency matrix A and $E_i^* = E_i^*(Y)$ ($0 \leq i \leq \tau$). $\mathcal{T}(Y)$ is called the *Terwilliger algebra of Γ with respect to Y* . This is the generalization of a Terwilliger algebra (or a subconstituent algebra) $\mathcal{T}(x)$ of a distance-regular graph introduced by P. Terwilliger [6, 7, 8] concerning the set of neighbours of a vertex x as a subset. H. Suzuki formulated the theory of $\mathcal{T}(Y)$. We get the similar results as on $\mathcal{T}(x)$ [5]. The theory of $\mathcal{T}(Y)$ is expected to provide powerful tools for the study of subsets or codes of distance-regular graphs.

Let $V = C^X$. We observe $\mathcal{T}(Y)$ acts on V , and V is called the standard module. Let W denote an irreducible \mathcal{T} -module. We have

$$W = E_0^*W + E_1^*W + \cdots + E_\tau^*W \quad (\text{the orthogonal direct sum}).$$

Let $e = \min\{i \mid 0 \leq i \leq \tau, E_i^*W \neq \phi\}$. The integer e is called the *endpoint* of W . W is called *thin* if $\dim E_i^*W \leq 1$ for all i ($0 \leq i \leq \tau$). A vector v is called *thin* if $\mathcal{T}(Y)v$, the algebra generated by the vector v , is thin.

3 Tight Vectors and Their Modules

Definition 3.1 A vector $v \in E_0^*V$ is said to be *tight with respect to Y* if

$$w(Y) = |\{i \mid E_i v = 0, 0 \leq i \leq D.\}|$$

holds.

Definition 3.2 Γ is said to be *tight with respect to Y* if $E_0^*V \cap (\mathbf{1}_Y)^\perp$ is spanned by tight vectors.

Proposition 3.1 (Theorem 9.2, [5]) Let v be a nonzero vector in E_0^*V . If v is tight with respect to Y , then $\mathcal{M}v$ is a thin irreducible \mathcal{T} -module. In particular, v is a common eigenvector of $E_0^*\mathcal{M}E_0^*$.

Proposition 3.2 (Proposition 7.2, [5]) Let $\mathbf{1}_Y$ be the characteristic vector of Y . Then the following are equivalent.

- (i) Y is a completely regular code of Γ with covering radius τ .
- (ii) $\mathcal{T}\mathbf{1}_Y$ is a thin irreducible \mathcal{T} -module.
- (iii) $\mathcal{T}\mathbf{1}_Y = \text{Span}(\mathbf{1}_Y, \mathbf{1}_{Y_1}, \dots, \mathbf{1}_{Y_\tau})$.

By the propositions above, Y is completely regular with $\tau = D - w(Y)$, if $\mathbf{1}_Y$ is tight with respect to Y .

4 Correspondence between Eigenvalues

The following is essential.

Proposition 4.1 Let Y be a subset of X with $w(Y) = 2$. Let $\Delta(Y)$ be connected and regular of valency κ . The following are equivalent.

(i) Γ is tight with respect to Y .

(ii) $\Delta(Y)$ has the distinct eigenvalues $\eta_0 = \kappa$, $\eta_1 = \bar{\theta}_D$, and $\eta_2 = \bar{\theta}_1$ where

$$\bar{\theta} = -1 - \frac{b_1}{1 + \theta}.$$

Corollary 4.2 Let v be a vector in $E_0^*V \cap \langle 1_Y \rangle^\perp$. If $E_i v = 0$ for some $i > 0$, then $i = 1$ or $i = D$. Moreover, if v is not a tight vector with respect to Y , then $E_i v \neq 0$ for any $i > 0$.

As another corollary, we obtain the following.

Theorem 4.3 Let Y be a subset of X with width 2 whose induced subgraph $\Delta(Y)$ is connected and regular of valency κ . Then the following are equivalent.

(i) Γ is tight with respect to Y .

(ii) $\Delta(Y)$ is a strongly regular graph having eigenvalues κ , $-1 - \frac{b_1}{1 + \theta_D}$, and $-1 - \frac{b_1}{1 + \theta_1}$.

5 Tight Distance-Regular Graphs with respect to Completely Regular Codes

Let Y be a subset of X . Let $w = w(Y)$ be the width of Y . Suppose $\Delta(Y)$ is connected and regular.

Definition 5.1 Γ is called homogeneous with respect to Y if W_y is A -invariant for all $y \in Y$, where

$$W_y = \text{Span}\{E_i^* A_j \hat{y} \mid 0 \leq i \leq \tau, 0 \leq j \leq D\}.$$

Remarks. If Γ is homogeneous with respect to Y and $\Delta(Y)$ is connected and regular, $\Delta(Y)$ is a distance-regular graph. It is easily proved by using the fact that if $\Delta(Y)$ is connected, regular and distance-regular with respect to every vertex in $\Delta(Y)$, then $\Delta(Y)$ is distance-regular [3].

Let Y be a completely regular code of covering radius τ .

Lemma 5.1 Suppose for any two distinct vertices y, y' in Y there exists a shortest path connecting y, y' such that every vertex in the shortest path belongs to Y . If $\tau = D - w$, then $\dim W_y = (w + 1)(D - w + 1)$ for all $y \in Y$.

To prove the lemma above, we use the following lemma.

Lemma 5.2 Let $\tau = D - w$. Let $y \in Y$. The following hold.

- (i) $E_i^* A_j \hat{y} = 0$ if $j < i$ or $j > i + w$ for all i ($0 \leq i \leq \tau$).
- (ii) $E_i^* A_i \hat{y} \neq 0$ for all i ($0 \leq i \leq \tau$).
- (iii) $E_i^* A_{i+w} \hat{y} \neq 0$ for all i ($0 \leq i \leq \tau$).
- (iv) Suppose for any vertex $y' \in Y$ there exists a shortest path connecting y, y' such that every vertex in the shortest path belongs to Y . Then $E_i^* A_j \hat{y} \neq 0$ for all i, j ($i < j < i + w, 0 \leq i \leq \tau$).

Proof of Lemma 5.1.) Let $y \in Y$. By Lemma 5.2, we have

$$\begin{aligned} \dim W_y &= \dim \text{Span}\{E_i^* A_j \hat{y} \mid 0 \leq i \leq \tau, 0 \leq j \leq D\} \\ &= \dim \text{Span}\{E_i^* A_j \hat{y} \mid 0 \leq i \leq D - w, i \leq j \leq i + w\} \\ &= (w + 1)(D - w + 1). \end{aligned}$$

□

The assumption in Lemma 5.1: for any two distinct vertices y, y' in Y there exists a shortest path connecting y, y' such that every vertex in the shortest path belongs to Y , implies that $\partial_{\Delta(Y)}(y, y') = \partial_{\Gamma}(y, y')$, where $\partial_{\Delta(Y)}, \partial_{\Gamma}$ denote the distance in $\Delta(Y)$ and that in Γ respectively (we usually denote ∂_{Γ} by ∂ for short). We call Y “weakly closed” if Y satisfies the above property.

The next proposition shows that a tight distance-regular graph with respect to a “weakly closed” completely regular code has the homogeneous property.

Proposition 5.3 *Suppose that for any two distinct vertices y, y' in Y there exists a shortest path connecting y, y' such that every vertex in the shortest path belongs to Y , and that 1_Y is tight with respect to Y , i.e., Y is a completely regular code of $\tau = D - w$. If Γ is tight with respect to Y , then Γ is homogeneous with respect to Y .*

Proof. Let $y \in Y$. Note that $\dim E_0^* W_y = w + 1$ by the assumption. Since $E_0^* V$ is spanned by tight vectors, $E_0^* W_y$ is also spanned by tight vectors u_0, u_1, \dots, u_w . We have

$$\begin{aligned} \dim T E_0^* W_y &= \dim(T u_0 + T u_1 + \dots + T u_w) \\ &\leq \dim T u_0 + \dim T u_1 + \dots + \dim T u_w \\ &= (w + 1)(D - w + 1). \end{aligned}$$

On the other hand, since $T E_0^* W_y \supset W_y$, we have

$$\dim T E_0^* W_y \geq \dim W_y.$$

By Lemma 5.1, we have $\dim W_y = (w + 1)(D - w + 1)$. Hence $\dim T E_0^* W_y = \dim W_y$ and so $T E_0^* W_y = W_y$. Therefore W_y is A -invariant. □

The converse is true for the case of $w(Y) = 2$.

Proposition 5.4 *Let $w = 2$. Suppose 1_Y is tight. If Γ is homogeneous with respect to Y , then Γ is tight with respect to Y .*

Proof. As we mentioned in Remarks, $\Delta(Y)$ is a strongly regular graph. So we can choose an orthogonal basis $1_Y, \mathbf{u}_1, \mathbf{u}_2$ of $E_0^*W_y$ so that \mathbf{u}_i becomes a common eigenvector of $E_0^*A_iE_0^*$ ($i = 0, 1, 2$). It is clear that W_y is E_i^* -invariant ($0 \leq i \leq \tau$). Since W_y is A -invariant, W_y is T -module and $TE_0^*W_y = W_y$.

We can verify that $T1_Y = \text{Span}(1_Y, 1_{Y_1}, \dots, 1_{Y_w})$ and $E_0^*T\text{Span}(\mathbf{u}_1, \mathbf{u}_2) = \text{Span}(\mathbf{u}_1, \mathbf{u}_2)$. If $T\text{Span}(\mathbf{u}_1, \mathbf{u}_2)$ contains 1_Y , it also contains 1_Y . Hence $1_Y \in E_0^*T\text{Span}(\mathbf{u}_1, \mathbf{u}_2)$. This contradicts the fact that $1_Y, \mathbf{u}_1, \mathbf{u}_2$ are linearly independent. To sum up, we have

$$W_y = TE_0^*W_y = T1_Y + T\text{Span}(\mathbf{u}_1, \mathbf{u}_2). \quad (\text{direct sum})$$

Because $\Delta(Y)$ is strongly regular, the assumption in Lemma 5.1 holds and we have $\dim W_y = (w+1)(D-w+1) = 3(D-1)$. Then we get

$$\begin{aligned} \dim T\text{Span}(\mathbf{u}_1, \mathbf{u}_2) &= \dim W_y - \dim T1_Y \\ &= 3(D-1) - (D-1) \\ &= 2(D-1). \end{aligned}$$

On the other hand, we have

$$\begin{aligned} \dim T\text{Span}(\mathbf{u}_1, \mathbf{u}_2) &\geq \dim \mathcal{M}\text{Span}(\mathbf{u}_1, \mathbf{u}_2) \\ &= \sum_{i=0}^D \dim E_i \text{Span}(\mathbf{u}_1, \mathbf{u}_2) \\ &= \dim E_0 \text{Span}(\mathbf{u}_1, \mathbf{u}_2) + \dim E_1 \text{Span}(\mathbf{u}_1, \mathbf{u}_2) \\ &\quad + \sum_{i=2}^{D-1} \dim E_i \text{Span}(\mathbf{u}_1, \mathbf{u}_2) + \dim E_D \text{Span}(\mathbf{u}_1, \mathbf{u}_2). \end{aligned}$$

Since $\mathbf{u}_1, \mathbf{u}_2$ are orthogonal to 1_Y , $\dim E_0 \text{Span}(\mathbf{u}_1, \mathbf{u}_2) = 0$. By Corollary 4.2, we have $\dim E_i \text{Span}(\mathbf{u}_1, \mathbf{u}_2) = 2$ for i ($2 \leq i \leq D-1$). Since $|\{i \mid E_i \mathbf{u} = \mathbf{0}, 1 \leq i \leq D\}| \leq 1$ for any $\mathbf{u} \in \text{Span}(\mathbf{u}_1, \mathbf{u}_2)$, $\dim E_i \text{Span}(\mathbf{u}_1, \mathbf{u}_2) \geq 1$ for $i = 1, D$. Thus $\dim T\text{Span}(\mathbf{u}_1, \mathbf{u}_2) \geq 2(D-2) + 2 = 2(D-1)$. Hence $\dim T\text{Span}(\mathbf{u}_1, \mathbf{u}_2) = 2(D-1)$, and $\dim E_i \text{Span}(\mathbf{u}_1, \mathbf{u}_2) = 1$ for $i = 1, D$. Therefore $E_i \mathbf{u}_1 = \mathbf{0}$ and $E_j \mathbf{u}_2 = \mathbf{0}$ where $\{i, j\} = \{1, D\}$, i.e., $\mathbf{u}_1, \mathbf{u}_2$ are tight vectors. Then we can easily show that any common eigenvector \mathbf{u} of $E_0^*A_iE_0^*$ ($0 \leq i \leq w$) is a tight vector. So E_0^*V is spanned by tight vectors. \square

The following is the main theorem.

Theorem 5.5 *Suppose 1_Y is tight with respect to Y , i.e., Y is a completely regular code with $\tau = D - 2$. Then the following are equivalent.*

(i) Γ is tight with respect to Y .

(iii) Γ is homogeneous with respect to Y .

Proof. (i) \Rightarrow (ii) : Suppose that Γ is tight with respect to Y . By Theorem 4.3, $\Delta(Y)$ is a strongly regular graph. Then Y satisfies the assumption of Proposition 5.3, so Γ is homogeneous with respect to Y .

(ii) \Rightarrow (i) : Clear from Proposition 5.4. □

References

- [1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, California, 1984.
- [2] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer Verlag, Berlin, Heidelberg, 1989.
- [3] C. D. Godsil and J. Shawe-Taylor, Distance-regularised graphs are distance-regular or distance-biregular, *J. Combin. Th. (B)* 43 (1987), 14-24.
- [4] A. Jurišić, J. Koolen and P. Terwilliger, Tight distance-regular graphs, *J. Alg. Combin.* 12 (2000), 163-197.
- [5] H. Suzuki, The Terwilliger algebra associated with a set of vertices in a distance-regular graph, preprint.
- [6] P. Terwilliger, The subconstituent algebra of an association schemes, (part I), *J. Alg. Combin.* 1 (1992), 363-388.
- [7] P. Terwilliger, The subconstituent algebra of an association schemes, (part II), *J. Alg. Combin.* 2 (1993), 73-103.
- [8] P. Terwilliger, The subconstituent algebra of an association schemes, (part III), *J. Alg. Combin.* 2 (1993), 177-210.

Galois 環上の有限上半平面に対する固有値について

九州大学・数理学研究院 田上 真 (Makoto Tagami)

Graduate School of Mathematics,
Kyushu University

1 Introduction

有限上半平面はポアンカレ上半平面の有限類似として定義された ([1], [2], [12] 参照). ポアンカレ上半平面には特殊線形群 $SL(2, \mathbb{R})$ が一次分数変換により可移に作用しているが, 有限上半平面には一般線形群が同様の作用により可移に作用している. この作用によりアソシエーションスキームが得られ, その relation はポアンカレ計量の有限類似 (ポアンカレ距離) により与えられる. よってこのアソシエーションスキームは対称になり, 特に可換になることが解る. アソシエーションスキームの可換性は重要な性質で, 可換であればこそ, その character table が定義される. character table から我々は多くのグラフ理論的性質を得る. 例えば intersection number や expansion 定数の情報等である. よく知られている有限上半平面は有限体上のものと有限環 $\mathbb{Z}/p^n\mathbb{Z}$ 上のものがあるが, 有限体上の上半平面に対してのみ character table は求められている (Evans[5], Soto-Andrade[8] 参照).

k -regular グラフが Ramanujan グラフであるとは, 任意のグラフの固有値 θ でその絶対値が k と異なるものに対して $|\theta| \leq 2\sqrt{k-1}$ が成り立つものを言う. グラフが Ramanujan グラフであることはそのグラフの Ihara-Zeta 関数が Riemann 仮説を満たすことと同値である (詳しくは [12] 参照). ポアンカレ距離を用いて, 有限上半平面にはグラフが定義されるが (上半平面グラフ), Nick Katz [6] は character table を用いて有限体上の上半平面グラフが 2 つの例外を除いて Ramanujan グラフであることを示した.

有限環上の上半平面は Angel, Shook, Terras, Trimble [3] の中で $\mathbb{Z}/p^n\mathbb{Z}$ 上で定義された (ここで p は奇素数). その論文で, $n = 2, p \geq 5$ に対して有限上半平面グラフは有限体上のものと対照的に Ramanujan グラフにならないことが示されている. また [9] において, $\mathbb{Z}/p^n\mathbb{Z}$ (p : 奇素数) 上の一般線形群の作用から得られるアソシエーションスキームの relation はポアンカレ距離では与えられず, 修正ポアンカレ距離で与えられること, 特にアソシエーションスキームが対称であることが示されている. $\mathbb{Z}/2^n\mathbb{Z}$ 上の上半平面に対しても [10] でアソシエーションスキームの対称性が示されている.

このように有限環上の上半平面は $\mathbb{Z}/p^n\mathbb{Z}$ に対して調べられてきたわけであるが, 有限体上の上半平面は 2 次拡大体の部分集合として定義されているので, 有限体や $\mathbb{Z}/p^n\mathbb{Z}$ の一つの一般化である Galois 環の 2 次拡大の部分集合として有限環上の上半平面を定義する方が自然である. このことは金沢大学の伊藤達郎先生により指摘された. よってこの報告では [3], [9], [10] の結果の Galois 環上への一般化を考える. 第 2, 3 節でアソシエーションスキームと Galois 環について簡単に復習する. 第 4 節で Galois 環上の上半平面を定義する. 第 5 節で有限上半平面のアソシエーションスキームとしての構造を奇標数に対してのみ調べる (アソシエーションスキームの対称性は $p = 2$ に対しても言えるがこの報告では割愛する). 最後に第 5 節の系として体上ではない有限上半平面グラフが一つの例外を除いて Ramanujan グラフでないことを示す.

2 Association Scheme

この節で、群の作用から得られるアソシエーションスキームの基本的な事柄について簡単に復習する。詳しくは [4] を参照のこと。

X は有限集合とし、有限群 G が X 上に左から可移に作用しているとする。 H を X の 1 点の G における安定部分群とする。一般的に群 G とその部分群 H に対して、 G の G/H への左側からの積による作用によって得られるアソシエーションスキームを $\mathfrak{X}(G, H)$ と表すことにする。 $\mathfrak{X}(G, H)$ の relation R_i は G の H による両側剰余分解 $G = \sum_{i=0}^d H a_i H$ を用いて次のように書ける：

$$R_i = \{(bH, cH) \mid b^{-1}c \in H a_i H\}.$$

定義 2.1 (Gelfand pair). G を有限群、 H をその部分群とする。 (G, H) が Gelfand pair であるとはアソシエーションスキーム $\mathfrak{X}(G, H)$ が可換であることと定義する。

定義 2.1 は [12] で与えられているものと異なっているけれども、もちろんそれらは同値である。

$(X, \{R_i\}_{i=0, \dots, d})$ をクラス d の可換アソシエーションスキームとする。 A_i を R_i に対する adjacency matrix とする、但し行列は X で index 付けられているとする。

Bose-Mesner 代数 \mathfrak{A} を adjacency matrix 達 A_0, \dots, A_d で張られている $M_X(\mathbb{C})$ の部分代数とする。ここで $M_X(\mathbb{C})$ は X によって index 付けられた複素数体 \mathbb{C} 上の全行列環である。 A_0, \dots, A_d は互いに可換な正規行列であるので同時対角化可能である。 A_0, \dots, A_d の最大共通固有空間の個数は $d+1$ で $\langle (1, 1, \dots, 1) \rangle$ はその一つとなっている。それらを $V_0 = \langle (1, 1, \dots, 1) \rangle, V_1, \dots, V_d$ と書いておく。 E_i を $\mathbb{C}^{|X|}$ から V_i への射影の単位ベクトル $\{e_x \mid x \in X\}$ により行列表示したものとす。この時、次が成り立つ。 [4, p.59, Theorem 3.1] 参照。

定理 2.1. E_0, \dots, E_d は \mathfrak{A} の原始冪等元全体である。

定理 2.1 より、 $\{E_0, \dots, E_d\}$ は \mathfrak{A} の新しい基底となるので、 A_0, \dots, A_d は $\{E_0, \dots, E_d\}$ の一次結合で書ける。それを $A_i = \sum_{j=0}^d p_i(j) E_j$ と書く。

定義 2.2 (character table). $d+1$ 次の行列 $P = (p_j(i))$ を character table と呼ぶ。ここで $p_j(i)$ は P の (i, j) -成分を表している。

対称アソシエーションスキームの relation i を固定すると正則グラフ (X, R_i) を得る。 $p_i(j)$ ($j = 0, \dots, d$) は正則グラフ (X, R_i) の固有値になっている。

次に $\mathfrak{X}(G, H)$ の character table を考える。 $\mathfrak{X}(G, H)$ のクラスは d とし、 1_H^G は G の G/H 上の置換指標を表すとする。 $\mathfrak{X}(G, H)$ が可換である必要十分条件は 1_H^G が multiplicity-free であることである。さらにこの時、 1_H^G の既約分解に現れる既約指標の個数は $d+1$ となる、そして単位指標 1_G は必ず既約分解に現れる。

1_H^G は multiplicity free であると仮定し、 $1_H^G = \chi_0 + \chi_1 + \dots + \chi_d$ と分解されているとする。ここで、 $\chi_0 = 1_G, \chi_1, \dots, \chi_d$ は互いに異なる G の既約指標となる。この時、次の指標公式がよく知られている。 [4, p.174, Theorem 11.6] 参照。

定理 2.2. $\{E_0, \dots, E_d\}$ のある順序付けに関して、 character table $P = (p_i(j))$ は次の公式で与えられる：

$$p_i(j) = \frac{1}{|H|} \sum_{x \in H a_i H} \chi_j(x).$$

3 Galois rings

この節で Galois 環の基本的な事柄について簡単に復習する。Galois 環についての詳しい参考文献としては McDonald[7] 等がある。

有限体は素体 $\mathbb{Z}/p\mathbb{Z}$ 上の有限次拡大, 即ち $\mathbb{Z}/p\mathbb{Z}$ 係数既約多項式による $\mathbb{Z}/p\mathbb{Z}$ の拡大として与えられる。又, 有限体は同じ濃度を持つ時, $\mathbb{Z}/p\mathbb{Z}$ -代数として同型になる。Galois 環は有限体の拡大理論の有限環版として与えられる。以下この報告を通して, 環は積についての単位元を持った有限濃度の可換環を意味するものとし, また環 R に対してその単元群を $U(R)$ で表すことにする。

R を極大イデアル \mathfrak{m} を持った局所環とし $\mu: R \rightarrow R/\mathfrak{m}$ は自然な環準同型とする。 $R[x], R/\mathfrak{m}[x]$ はそれぞれ $R, R/\mathfrak{m}$ 上の多項式環とする。 R/\mathfrak{m} は有限体であることに注意する。上と同じ記号を用いて, 環準同型 $\mu: R[x] \rightarrow R/\mathfrak{m}[x]$ を自然な方法で定義する。即ち $f(x) = \sum_i a_i x^i \in R[x]$ に対して, $\mu f(x) = \sum_i \mu(a_i) x^i \in R/\mathfrak{m}[x]$ と定義する。 $f(x) \in R[x]$ が *basic irreducible* であるとは $\mu f(x)$ が既約であることと定義する。

定義 3.1 (Galois 拡大). S を局所環, R を S の単位元を共有する部分局所環とする。この時, S が R の Galois 拡大であるとは, ある monic basic irreducible 多項式 $f(x) \in R[x]$ が存在し, R -代数として $S \cong R[x]/(f(x))$ となることと定義する。またこの時 $f(x)$ の次数を拡大 S/R の次数と言う。

上の定義は [7] のものと異なっているが同値である。

S/R を Galois 拡大, $\text{Gal}(S/R)$ を S の R -自己同型全体のなす群とする。 $\text{Gal}(S/R)$ を拡大 S/R の Galois 群と言う。 Galois 拡大に対して次の諸定理がよく知られている。

定理 3.1. R の 2 つの同次数の Galois 拡大は R -代数として同型である。

定理 3.2. Galois 群は巡回群であり, その位数は拡大の次数と一致する。

定理 3.3. $S/R, T/S$ を Galois 拡大とする。その時, T/R はまた Galois 拡大である。

定理 3.1, 3.2, 3.3 の証明については [7, Corollary XV.3, Corollary XV.4, Theorem XV.7] を参照のこと。

定義 3.2 (Galois 環). n を自然数, p を素数とする。 $\mathbb{Z}/p^n\mathbb{Z}$ の Galois 拡大を Galois 環 という。 $\mathbb{Z}/p^n\mathbb{Z}$ の r 次の Galois 拡大を $\text{GR}(p^n, r)$ と書く。

$\text{GR}(p^n, 1) = \mathbb{Z}/p^n\mathbb{Z}, \text{GR}(p, r) = \text{GF}(p^r)$ である。このことは Galois 環が有限体や $\mathbb{Z}/p^n\mathbb{Z}$ の一般化であることを示している。 Galois 環 $R = \text{GR}(p^n, r)$ の極大イデアルは pR で $R/pR \cong \text{GF}(p^r)$ である。

定理 3.3 によって Galois 環 R の Galois 拡大 S はまた Galois 環である。有限体の時と同様にして norm 写像 $N_{S/R}$ を次のように定義する: Galois 群を $G = \text{Gal}(S/R)$ として,

$$\begin{aligned} N_{S/R}: S &\rightarrow R \\ t &\mapsto \prod_{\sigma \in G} \sigma(t) \end{aligned}$$

$N_{S/R}$ は積を保存するので, $N_{S/R}$ は $U(S)$ を $U(R)$ へ写す。次の補題は Hilbert の定理 90 の環版である。

補題 3.1 (Hilbert の定理 90). $\text{Gal}(S/R) = \langle \sigma \rangle$ とする。この時 $\beta \in S$ に対して, $N_{S/R}(\beta) = 1$ である必要十分条件は, ある $\alpha \in U(S)$ が存在し, $\beta = \alpha \sigma(\alpha)^{-1}$ が成り立つことである。

証明は [7, Exercise XV.8] を参照のこと。

補題 3.2. R を Galois 環, S を R の Galois 拡大とする. $G = \text{Gal}(S/R)$ とする. この時,

$$S^G := \{a \in S \mid \sigma(a) = a \ (\forall \sigma \in G)\} = R.$$

証明は [7, Corollary XV.3] を参照のこと. 次に norm 写像が有限体の場合と同様に $U(S)$ から $U(R)$ への全射準同型であることを示す.

補題 3.3. R は Galois 環, S を R の Galois 拡大とする. この時, norm 写像 $N_{S/R}$ は $U(S)$ から $U(R)$ への全射準同型である.

[証明] $R = \text{GR}(p^n, r)$ を Galois 環, $G = \langle \sigma \rangle$ を S/R の Galois 群とする. 補題 3.1 から, $\alpha \in \text{Ker } N_{S/R} = \{t \in U(S) \mid N_{S/R}(t) = 1\}$ である必要十分条件はある β が存在し $\alpha = \sigma(\beta)\beta^{-1}$ が成り立つことである. よって $h: U(S) \ni \beta \rightarrow \sigma(\beta)\beta^{-1} \in \text{Ker } N_{S/R}$ は全射準同型. $\beta \in \text{Ker } h$ である必要十分条件は $\sigma(\beta) = \beta$, 即ち $\beta \in S^G$ である. 補題 3.2 により, これは $\beta \in R$ と同値になる. S/R は Galois 拡大であるので, $R \cap U(S) = U(R)$ である. よって $\beta \in \text{Ker } h$ である必要十分条件は $\beta \in U(R)$, 即ち $\text{Ker } h = U(R)$ である. それ故 $|\text{Ker } N_{S/R}| = |U(S)|/|\text{Ker } h| = |U(S)|/|U(R)|$. これは $N_{S/R}(U(S)) = U(R)$ を示している.

[証明終]

また Galois 環の単元群の構造が知られている. [7, Theorem XVI.9] を参照.

補題 3.4. p を奇素数, $R = \text{GR}(p^n, r)$ とする. この時,

$$U(R) \cong \mathbb{Z}/(p^r - 1)\mathbb{Z} \times \underbrace{\mathbb{Z}/p^{n-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n-1}\mathbb{Z}}_{r \text{ times}}.$$

補題 3.4 により, 特に Galois 環の単元群は巡回群でないことがわかる. 単元群は巡回群でないけれども平方元をある $U(R)$ の元の 2 乗でかけることと定義する. 平方元でない元を非平方元という. この時, 次が成り立つ.

補題 3.5. p を奇素数, $R = \text{GR}(p^n, r)$ とする. この時, $a \in U(R)$ が平方元である必要十分条件は $\mu(a)$ が有限体 $\text{GF}(p^r)$ の元として平方元であることである.

[証明] 補題 3.4 によって,

$$G_1 \cong \mathbb{Z}/(p^r - 1)\mathbb{Z}, \quad G_2 \cong \underbrace{\mathbb{Z}/p^{n-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n-1}\mathbb{Z}}_{r \text{ times}}.$$

とすると, $U(R) = G_1 \times G_2$ と書ける. $a \in U(R)$ に対して, $a = a_1 \cdot a_2$ ($a_1 \in G_1, a_2 \in G_2$) と置く. G_2 で元を 2 乗することは G_2 の乗法群としての自己同型になる. よって a が平方元である必要十分条件は a_1 が平方元であることである. $x \in G_2$ に対して, $\mu(x)^{p^{n-1}} = 1$ となる. p 乗冪は $\text{GF}(p^r)$ の自己同型であるので, 実は $\mu(x) = 1$ となっている. 結果的に $\mu(x) = 1 (\forall x \in G_2)$ となり, $\mu(G_1) = U(\text{GF}(p^r))$ となる. しかし今 $|G_1| = |U(\text{GF}(p^r))|$ であるので, μ は G_1 から $U(\text{GF}(p^r))$ への同型になる.

[証明終]

定義 3.3 (p -進付値). $a \in R = \text{GR}(p^n, r)$ に対して, $a \in (p^i) - (p^{i+1})$ の時, $\text{ord}_p(a) = i$ と定義する, ここで $(p^{n+1}) = \emptyset$ としている.

$R = R_n = R_{n,r} = \text{GR}(p^n, r)$ とする. 便宜上 $R_{0,r} = 0$ とする. 行列 X, Y に対して $X \equiv Y \pmod{p}$ は X と Y の各成分が \pmod{p} で等しい事とする. 簡潔の為, \pmod{p} の代わりに (p) を書く. 次の補題は後で使われる.

補題 3.6. $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(R)$ に対して, $v := \min_{1 \leq i, j \leq 2} \text{ord}_p(a_{ij})$, $a_{ij} = p^v a'_{ij}$ ($a'_{ij} \in R_{n-h}$), $A' := \begin{pmatrix} a'_{11} & a'_{12} \\ a'_{21} & a'_{22} \end{pmatrix}$ とおく. この時, 線型方程式 $A \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^n}$ の解で, $(x, y) \not\equiv (0, 0) \pmod{p}$ なるものが存在する必要十分条件は $\det A' \equiv 0 \pmod{p^{n-v}}$ となることである.

[証明] $A = 0$ であれば明らかなので, $A \neq 0$ とする.

$$A \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^n} \iff A' \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^{n-v}}.$$

である. 仮定より, ある $a'_{ij} \in U(R_{n-v})$ となる. $a'_{11} \in U(R_{n-v})$ と仮定する (他の場合も同様に示される). この時, $x \equiv (a'_{12}/a'_{11})y \pmod{p^{n-v}}$. この式を $a'_{21}x + a'_{22}y \equiv 0 \pmod{p^{n-v}}$ に代入して $(\det A')y \equiv 0 \pmod{p^{n-v}}$ を得る. もし $\det A' \equiv 0 \pmod{p^{n-v}}$ ならば, y を任意に取って $x \equiv (a'_{12}/a'_{11})y$ と置けば求めたい解が求まる. もし $\det A' \not\equiv 0 \pmod{p^{n-v}}$ であるならば, $y \equiv 0 \pmod{p}$ よって $x \equiv 0 \pmod{p}$ となる. [証明終]

4 The finite upper half planes over Galois rings

この節で Galois 環上の有限上半平面を定義する. n, r を自然数, p を素数とする.

$R = R_n = R_{n,r} = \text{GR}(p^n, r)$, $U = U_n = U_{n,r} = U(R_{n,r})$ とする. 便宜上 $R_{0,r} = U_{0,r} := \{0\}$ とする. U_n の位数は $p^{(n-1)r}(p^r - 1)$ である. $M = M_{n,r} = \text{GR}(p^n, 2r)$ と置く. M は R の 2 次の Galois 拡大として与えられるので, 定理 3.3 により, 一般性を失うことなく, 奇素数 p に対して $M = R[T]/(T^2 - \delta)$, $p = 2$ に対して $M = R[T]/(T^2 - T - \gamma)$ と書ける. ここで T は不定元で, δ は $U(R)$ の非平方元, $c \in U(R)$ は $\mu(c)$ が $t^2 - t$ ($t \in U(\text{GF}(2^r))$) の形で書けないものとする.

定義 4.1 (Galois 環上の上半平面).

$$\mathfrak{H} := \{x + yT \in M \mid x \in R, y \in U\}.$$

次に R 上の一般線形群を考える:

$$G := \text{GL}(2, R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R, ad - bc \not\equiv 0 \pmod{p} \right\}.$$

G の中心 $Z(G)$ は次のようになる:

$$Z(G) = \{aI \mid a \in U\}.$$

補題 4.1. $z \in \mathfrak{H}$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ に対して次が成り立つ:

(i) $cz + d \in U(M)$

(ii) $(az + b)/(cz + d) \in \mathfrak{H}$

証明は [3, Proposition 1] を参照のこと.

補題 4.1 により, G は \mathfrak{H} 上に一次分数変換により作用することがわかる. この作用が可移であることは次の G の部分群を考えることにより解る.

$$A := \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \mid y \in U, x \in R \right\}.$$

A をアフィン群と言う。 $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \cdot \sqrt{\delta} = x + y\sqrt{\delta}$ であるので、 A は \mathfrak{H} 上に可移に作用している。従って G も可移に作用している。

K を $T \in \mathfrak{H}$ の G における安定部分群とする。 K はポアンカレ上半平面の場合と比較して直交群と呼ばれる。我々は $K \backslash G / K$ の両側剰余分解を決定したいわけである。明らかに G は K によって次のように左剰余分解される：

$$G = \sum_{x \in R, y \in U} \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} K = \sum_{z \in A} zK.$$

よって $K \backslash G / K$ の代表元を A の元からとることができることが解る。以下 $\mathfrak{H}, G/K, A$ を G -集合として次の対応で同一視する：

$$x + yT \longleftrightarrow \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} K \longleftrightarrow \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}.$$

以下 \mathfrak{H} 上の関数などを G/K や A 上のものとみなす。

5 The criterion of double cosets and symmetry of the association schemes for odd primes

この節で奇素数 p に対して A の 2 元が同じ両側剰余類に入る条件を求める。表記を解りやすくするために T を $\sqrt{\delta}$ と書くことにする。

まずいくつかの定義と補題を用意する。ポアンカレ上半平面の時のように、 M の元に対して実部、虚部、共役を定義する：

$$\operatorname{Re}(z) := x, \operatorname{Im}(z) := y, \bar{z} := x - y\sqrt{\delta} \text{ for } z = x + y\sqrt{\delta} \in M.$$

写像 $x + y\sqrt{\delta} \rightarrow x - y\sqrt{\delta}$ は M の R -自己同型であることと、 M/R の拡大次数が 2 であることから、norm 写像 $N_n = N_{M_n/R_n}$ は

$$N_n(z) := x^2 - y^2\delta \text{ for } z = x + y\sqrt{\delta} \in M_n$$

となる。 N_n はもちろん M_n の積を保存する： $N_n(zw) = N_n(z)N_n(w)$ for $z, w \in M_n$.

次の補題は簡単であるがとても有用である。

補題 5.1. $c \in U_n$ とする。この時、

$$\#\{(x, y) \mid x, y \in R_n, x^2 - y^2\delta = c\} = p^{(n-1)r}(p^r + 1).$$

[証明] $x^2 - y^2\delta$ は $x + y\sqrt{\delta}$ の norm 写像である。補題 3.3 によって $N_n : U(M) \rightarrow U_n$ は全射準同型であるので、 $x^2 - y^2\delta = c$ の解の個数は U_n の任意の元 c に対して $x^2 - y^2\delta = 1$ の解の個数、即ち $|U(M_n)| / |U_n|$ となる。 [証明終]

奇素数 p に対して、 $\sqrt{\delta}$ の G における安定部分群 K_n は次のようになる：

$$K_n = \left\{ g \in G \mid g \cdot \sqrt{\delta} = \sqrt{\delta} \right\} = \left\{ \begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} \mid a, b \in R_n, a^2 - b^2\delta \neq 0(p) \right\}.$$

次に有限上半平面にポアンカレ計量の有限類似を定義する ([3] 参照)。

定義 5.1 (ポアンカレ距離). $z, w \in \mathfrak{h}$ に対して,

$$d(z, w) := \frac{N(z-w)}{\operatorname{Im}(z)\operatorname{Im}(w)}.$$

ポアンカレ距離は G の作用に対して不変である. よって $a \in \mathbb{R}_n$ に対して,

$$S(a) := \{g \in A \mid d(\sqrt{\delta}, g \cdot \sqrt{\delta}) = a\}.$$

と定義すると, $S(a)$ は両側剰余類のいくつかの和になっている. ここで両側剰余類は右剰余類の和とみなしておき, また A と G/K を同一視していることに注意する. よって後は $S(a)$ の両側剰余類への分解を考えればよい.

有限体の場合には $S(a)$ がすでに 1 つの両側剰余類であったが, 有限環の場合には, 一般的に $S(a)$ はいくつかの両側剰余類に分解する. しかしいくつかの距離に対しては次が成り立つ.

定理 5.1. $a \not\equiv 0, 4\delta \pmod{p}$ に対して, $S(a)$ は両側剰余類である.

証明については [9, Theorem 4.1] を参照のこと.

$a \equiv 0, 4\delta \pmod{p}$ に対しては, $S(a)$ はいくつかの両側剰余類に分解する. この分解を調べるために, 2 つの写像 $H : \cup_{a \equiv 0, 4\delta \pmod{p}} S(a) \rightarrow \{0, 1, \dots, n\}$, $L_H : \cup_{a \equiv 0, 4\delta \pmod{p}} S(a) \rightarrow \bigcup_{i=0}^n U_i$ を定義する. $a \equiv 0 \pmod{p}$ と $a \equiv 4\delta \pmod{p}$ の場合に分ける.

(i) $a \equiv 0 \pmod{p}$

$g = \begin{pmatrix} 1+l & k \\ 0 & 1 \end{pmatrix} \in S(a)$ に対して, $H(g) := \min\{\operatorname{ord}_p(l), \operatorname{ord}_p(k)\}$, $k = k'p^{H(g)}$, $l = l'p^{H(g)}$ ($k', l' \in U_{n-H(g)}$) と置く. この時

$$L_H(g) := \frac{N_{n-H(g)}(k' + l'\sqrt{\delta})}{1+l}$$

と定義する.

(ii) $a \equiv 4\delta \pmod{p}$

$g = \begin{pmatrix} -1+l & k \\ 0 & 1 \end{pmatrix} \in S(a)$ に対して, $H(g) := \min\{\operatorname{ord}_p(l), \operatorname{ord}_p(k)\}$, $k = k'p^{H(g)}$, $l = l'p^{H(g)}$ ($k', l' \in U_{n-H(g)}$) と置く. この時

$$L_H(g) := \frac{N_{n-H(g)}(k' + l'\sqrt{\delta})}{-1+l}$$

と定義する.

この時, 次が成り立つ.

定理 5.2. $a \equiv 0$ or $4\delta \pmod{p}$, $g_1, g_2 \in S(a)$ とする. この時, $Kg_1K = Kg_2K$ である必要十分条件は $H(g_1) = H(g_2)$ かつ $L_H(g_1) = L_H(g_2)$.

Galois 環においても補題 3.6 が成り立つので, 定理 5.2 は [9] のものと全く同様に証明できる. よってここでは割愛する.

同じ両側剰余類に入るかどうかの判定条件式は対称であるので, つぎの系が得られる.

系 5.1. 奇素数に対して, $\mathfrak{X}(G, K)$ は対称アソシエーションスキームである.

次にアソシエーションスキームの relation を決定する. $z, w \in \mathfrak{H}$ に対して, 修正ポアンカレ距離 d_R を次のように定義する:

- (i) $d(z, w) \not\equiv 4\delta \pmod{p}$ の時. $r := \operatorname{Re}(z - w)$, $k := \operatorname{Im}(z - w)$, $v := \min\{\operatorname{ord}_p(r), \operatorname{ord}_p(k)\}$ と置く, さらに $r = p^v r'$, $k = p^v k'$ ($r', k' \in R_{n-v}$) と置く. この時,

$$d_R(z, w) := \frac{N_{n-v}(r' + k'\sqrt{\delta})p^v}{\operatorname{Im}(z)\operatorname{Im}(w)}$$

と定義する. $N_{n-v}(r' + k'\sqrt{\delta})$ は R_{n-v} の元であるが, p^v をかけているので, $d_R(z, w)$ は R_n の元とみなすことができる.

- (ii) $d(z, w) \equiv 4\delta \pmod{p}$ の時. $r := \operatorname{Re}(z - w)$, $k := \operatorname{Im}(z + w)$, $v := \min\{\operatorname{ord}_p(r), \operatorname{ord}_p(k)\}$, さらに $r = p^v r'$, $k = p^v k'$, ($r', k' \in R_{n-v}$) と置く. この時

$$d_R(z, w) := \frac{N_{n-v}(r' + k'\sqrt{\delta})p^v}{\operatorname{Im}(z)\operatorname{Im}(w)} + 4\delta$$

と定義する. (i) と同様に, $d_R(z, w) \in R_n$ とみなせる.

$a \in R_n$ に対して, $L_a := \{(z, w) \mid z, w \in \mathfrak{H}, d_R(z, w) = a\}$ と置くと, $\{L_a\}_{a \in R_n}$ は $\mathfrak{X}(G, K)$ の relation になっている.

6 Graph spectra for finite upper half planes

この節で定理 5.1 の一つの応用を考える. $n > l$ とし, $\mu_{n,l} : R_n \rightarrow R_l$ を自然な準同型とする. 簡単のため, $\mu_{n,l}(t)$ を \bar{t} で表す.

補題 6.1. $n \geq 1, l < n$ とする. $a \in R_n$ を $a \not\equiv 0, 4\delta \pmod{p}$ なる元とする. $c + d\sqrt{\delta} \in S(\bar{a})$ を固定する. この時次が成り立つ.

$$\#\{x + y\sqrt{\delta} \in S(a) \mid x \equiv c, y \equiv d \pmod{p^l}\} = p^{(n-l)r}.$$

[証明] $\lfloor n/2 \rfloor \leq l$ の場合を証明すれば後は l について帰納的に示せる. 自然な準同型 $K_n \mathfrak{g} K_n \rightarrow K_l \mathfrak{g} K_l$ は全射であるので, 定理 5.1 からある $x_0 + y_0\sqrt{\delta} \in S(a)$ で $x_0 \equiv c \pmod{p^l}$, $y_0 \equiv d \pmod{p^l}$ なるものがある. そんな $x_0 + y_0\sqrt{\delta} \in S(a)$ を固定する. $c \not\equiv 0 \pmod{p}$ と $c \equiv 0 \pmod{p}$ の場合に分ける.

(I) $c \not\equiv 0 \pmod{p}$ の場合.

$y = y_0 + p^l t$ と置く. $x + y\sqrt{\delta} \in S(a)$ である必要十分条件は

$$x^2 = ay + (y - 1)^2 \delta \tag{1}$$

である. 方程式 (1) が解 x をもつ必要十分条件は $ay + (y - 1)^2 \delta$ が平方元となることである. 補題 3.5 により, これは $ay_0 + (y_0 - 1)^2 \delta$ が平方元であることと同値である. この条件は t のとり方には依存しない. そんなそれぞれの y に対して, 丁度 2 つの解 $\pm x \in R_n$ が存在する. よって補題は成り立つ.

(II) $c \equiv 0 \pmod{p}$ の場合

$x = x_0 + sp^l$ と置き, $f_s(y) := ay + (y - 1)^2 - x^2$ と定義する. $y = y_0 + p^l t$ に対して,

$$f_s(y) = f_s(y_0 + p^l t) = f_s(y_0) + f'_s(y_0)p^l t$$

となる. $a \neq 0, 4\delta(p)$ であるので, $f'_s(y_0) \neq 0(p)$. また仮定より $f_s(y_0) \equiv 0(p^l)$. よってそれぞれの t に対して, $f_s(y) = 0$ の解 y で $y \equiv y_0(p^l)$ なるものが丁度 1 つ存在する. よって補題が成り立つ. [証明終]

一般的に群 G に対して, G の既約指標全体のなす集合を $\text{Irr}(G)$ で表す.

G 上の複素数値関数全体のなすベクトル空間に次のようにして内積を定義する. 複素数値関数 ϕ, ψ に対して,

$$(\phi, \psi)_G = \frac{1}{|G|} \sum_{x \in G} \phi(x)\psi(x^{-1}).$$

とする. 指標 ϕ と既約指標 χ に対して, $(\phi, \chi)_G$ は ϕ の既約指標分解における χ の重複度になる. G' を群とし, $f: G \rightarrow G'$ が存在すると仮定する. この時 $\chi \in \text{Irr}(G')$ は $\chi(x) := \chi(f(x))$ として $\chi \in \text{Irr}(G)$ とみなせる.

補題 6.2. $G > K$ と $G' > K'$ は群とし, $f: G \rightarrow G'$ は $f(K) = K'$ を満たす全射準同型とする. この時 $\chi \in \text{Irr}(G')$ に対して,

$$(1_K^G, \chi)_G = (1_{K'}^{G'}, \chi)_{G'}$$

となる.

[証明] Frobenius reciprocity より,

$$\begin{aligned} (1_K^G, \chi)_G &= (1_K, \chi)_K = \frac{1}{|K|} \sum_{x \in K} \chi(x) = \frac{1}{|K|} \sum_{t \in K'} \frac{|K|}{|K'|} \chi(t) = \frac{1}{|K'|} \sum_{t \in K'} \chi(x) \\ &= (1_{K'}^{G'}, \chi)_{G'} \end{aligned}$$

[証明終]

補題 6.2 によって, もし $\chi \in \text{Irr}(G_l)$ が $1_{K_l}^{G_l}$ の既約指標分解に現れるならばそれは $1_{K_n}^{G_n}$ の既約指標分解にも現れることがわかる.

ポアンカレ距離を用いて有限上半平面グラフを定義する.

定義 6.1 (有限上半平面グラフ). $a \in R$ を固定する. 有限上半平面グラフ $X_R(\delta, a)$ を次のようにして定義する. 頂点集合として H_R の元をとる. 2 頂点 z, w は $d(z, w) = a$ である時, 隣接しているとする.

以下有限上半平面グラフの固有値について調べる.

補題 6.3. $1 \leq l \leq n$ とし, $a \in R_n$ を $a \neq 0, 4\delta(p)$ なるものとする. この時 $X_{R_l}(\bar{\delta}, \bar{a})$ の任意の固有値 μ に対して, $p^{(n-l)r} \mu$ は $X_{R_n}(\delta, a)$ の固有値になっている.

[証明] $g \in S(a)$ をとる. 定理 2.2 により, $\chi \in \text{Irr}(G_l)$ で

$$\mu = \frac{1}{|K_l|} \sum_{z \in K_l, gK_l} \chi(\bar{z})$$

なるものが存在する。補題 6.1 によって、

$$\begin{aligned} \frac{1}{|K_l|} \sum_{x \in K_l \bar{g} K_l} \chi(\bar{x}) &= \frac{1}{|K_l|} \sum_{x \in K_n \bar{g} K_n} \chi(x) \cdot \frac{1}{p^{(n-l)r}} \cdot \frac{|K_l|}{|K_n|} \\ &= \frac{1}{p^{(n-l)r}} \cdot \frac{1}{|K_n|} \sum_{x \in K_n \bar{g} K_n} \chi(x). \end{aligned}$$

$\frac{1}{|K_n|} \sum_{x \in K_n \bar{g} K_n} \chi(x)$ は $X_{R_n}(\delta, a)$ の固有値であるので、補題は証明された。

[証明終]

定理 6.1. $a \neq 0, 4\delta(p)$ とする。 $n \geq 2$ に対して、 $X_{R_n}(\delta, a)$ は $\mathbb{Z}/9\mathbb{Z}$ の場合のみ Ramanujan グラフである。

[証明] まず Angel の方法を紹介する。一般に X を n 頂点からなる k -正則連結グラフで non-bipartite なものとする。 A をその adjacency matrix とする。 X の固有値を

$$k = \lambda_1 > \lambda_2 \geq \dots \geq \lambda_n$$

と並べておく。この時

$$\sum_{j=1}^n \lambda_j^2 = \text{tr}(A^2) = kn \tag{2}$$

μ を固有値の絶対値の中での 2 番目に大きな値とする。この時、方程式 (2) から

$$\mu \geq \sqrt{\frac{kn - k^2}{n - 1}} \tag{3}$$

を得る。

グラフ $X_{R_n}(\delta, a)$ と $X_{R_1}(\bar{\delta}, \bar{a})$ を考える。有限体 $R_1 = \text{GF}(p^r)$ 上の有限上半平面グラフは $a \neq 0, 4\delta(p)$ の時連結な non-bipartite グラフであるから、不等式 (3) を適用できる。頂点数は $n = p^r(p^r - 1)$, valency は $k = p^r + 1$ であるので、

$$\mu \geq \sqrt{p^r + 1} \sqrt{\frac{p^{2r} - 2p^r - 1}{p^{2r} - p^r - 1}}$$

となる。補題 6.3 により、は固有値 $p^{(n-1)r}\mu$ を持っているので、

$$p^{(n-1)r} \sqrt{p^r + 1} \sqrt{\frac{p^{2r} - 2p^r - 1}{p^{2r} - p^r - 1}} > 2\sqrt{p^{nr} + p^{(n-1)r} - 1} \tag{4}$$

が成り立てば、 $X_{R_n}(\delta, a)$ は Ramanujan グラフではない。実際不等式 (4) は $(n, r, p) = (3, 1, 3), (2, 1, 3), (2, 1, 5)$ の場合を除いて成り立っている。またグラフの固有値を直接計算することにより、 $X_{R_n}(\delta, a)$ は $(2, 1, 3)$ の時 Ramanujan グラフで $(2, 1, 5), (3, 1, 3)$ の時は Ramanujan グラフでないことが確かめられる。 [証明終]

参考文献

- [1] J. Angel, Finite upper half planes over finite fields, *Finite Fields Appl.*, 2(1996), 62-86.
- [2] J. Angel, N. Celniker, S. Poulos, A. Terras, C. Trimble, and E. Velasquez, Special functions on finite upper half planes, *Contemp. Math.* 138 (1992), 1-26.

- [3] J. Angel, B. Shook, A. Terras, C. Trimble, Graph spectra for finite upper half planes over rings, *Linear Algebra and Its Applications*, **226-228** (1995), 423-457.
- [4] Eiichi Bannai and T. Ito, *Algebraic Combinatorics I, Association Schemes*, Benjamin/Cummings, Menlo Park, CA, 1984.
- [5] R. Evans, Characters sums as orthogonal eigenfunctions of adjacency operators for Cayley graphs, *Cont. Math.*, **168** (1994), 33-50.
- [6] N. Katz, Estimates for Soto-Andrade sums, *J. Reine Angew. Math.*, **438** (1993), 143-161.
- [7] B.R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974.
- [8] J. Soto-Andrade, Geometrical Gelfand models, tensor quotients, and Weil representations, *Proc. Symp. Pure Math.*, **47**, Amer. Math. Soc., Providence, (1987), 305-316.
- [9] M. Tagami, Symmetric association schemes attached to finite upper half planes over rings, *Linear Algebra and Its Applications*, **376** (2004), 225-234.
- [10] M. Tagami, Gelfand pairs obtained from the finite upper half planes over $\mathbb{Z}/2^n\mathbb{Z}$, to appear in *J. Combin. Math. and Combin. Computing*.
- [11] M. Tagami, On graph spectra for finite upper half planes over Galois rings, submitted.
- [12] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Math. Soc., 1999.

ON GRAPHS WITH THE SMALLEST EIGENVALUE AT LEAST $-1 - \sqrt{2}$

TETSUJI TANIGUCHI

ABSTRACT. There are many results on graphs with the smallest eigenvalue at least -2 . As a next step, A. J. Hoffman proposed to study graphs with the smallest eigenvalue at least $-1 - \sqrt{2}$. In order to deal with such graphs, R. Woo and A. Neumaier defined a new generalization of line graphs which depends on a family of isomorphism classes of graphs with a distinguished coclique. In this paper, we deal with a generalization depending on a family smaller than the family which they dealt with. The main result is that a minimal graph without a structure characterized by such generalization of line graphs, and with the smallest eigenvalue at least $-1 - \sqrt{2}$, is just isomorphic to one of the 37 graphs found by computer.

1. INTRODUCTION

In [1], P. J. Cameron, J. M. Goethals, J. J. Seidel, and E. E. Shult have shown that graphs with least eigenvalue -2 are represented by a subset of the root system A_n , D_n or E_8 . A graph represented by a subset of A_n is the line graph of a bipartite graph. A graph represented by a subset of D_n is a generalized line graph. A graph represented by a subset of E_8 has at most 36 vertices, and its maximum valency is at most 28. A graph is said to be exceptional if it is connected, has least eigenvalue -2 , and is not a generalized line graph. Such graphs are represented by a subset of E_8 , hence the number of exceptional graphs is finite. The 473 maximal exceptional graphs have been found by computer. (cf. [6]).

Let $\lambda^1(G)$ be the smallest eigenvalue of a graph G . Let Λ^1 be the set of all real numbers λ such that $\lambda = \lambda^1(G)$ for some connected graph G . Let $\delta(G)$ denote the minimum valency of the vertices of a graph G . In [3], A. J. Hoffman have shown the following theorem:

Theorem 1.1 (A. J. Hoffman). *There exists an integer valued function f , defined on the intersection of Λ^1 with the half-open interval $[-1, -1 - \sqrt{2})$, such that*

- (1) *if $-1 \geq \lambda > -2$, $\lambda^1(G) = \lambda$, $\delta(G) \geq f(\lambda)$, then G is a clique and $\lambda^1(G) = -1$ (note that a clique is also a generalized line graph);*
- (2) *if $-2 \geq \lambda > -1 - \sqrt{2}$, $\lambda^1(G) = \lambda$, $\delta(G) \geq f(\lambda)$, then G is a generalized line graph and $\lambda^1(G) = -2$.*

A remark about the function f . Since $\lambda^1(G) \leq -1$ if G has at least one edge, and $\lambda^1(G) = -1$ if and only if G is a clique, $f(-1) = 1$.

Since a exceptional graph has the maximum valency at most 28 as mentioned above, if a graph with the smallest eigenvalue at least -2 and the maximum valency at least 29, then it is a generalized line graph. Hence we may take $f(-2) = 29$.

Hoffman claims that it is reasonable to believe that there is a sequence of numbers $\alpha_1 = -1 > \alpha_2 = -2 > \alpha_3 = -1 - \sqrt{2} > \alpha_4 > \dots$ tending to some limit $\tilde{\alpha}$ such that for each $\lambda \in \Lambda^1$, if $\alpha_i \geq \lambda > \alpha_{i+1}$, there is a number $f(\lambda)$ such that $\lambda^1(G) = \lambda$, and $\delta(G) \geq f(\lambda)$ implies

Date: October 12, 2004.

2000 Mathematics Subject Classification. 05C50.

Key words and phrases. Generalized line graph, Spectrum.

$\lambda = \alpha_i$. We scarcely find any entries of the sequence $\{\alpha_i\}$, and do not determine the value $\bar{\alpha}$. In order to deal with such graphs, R. Woo and A. Neumaier defined a new generalization of line graph in [2]. In [2], R. Woo and A. Neumaier claims that Hoffman's analysis was based on the properties of simple subgraphs involving large cliques, which Hoffman depicted by fat vertices. A Hoffman graph is a graph with a distinguished coclique Δ . Vertices in Δ are called fat; other vertices slim. The following definition is the above-mentioned generalization of line graph.

Definition 1.2 (R. Woo and A. Neumaier). *Let \mathcal{H} be a family of isomorphism classes of Hoffman graphs. An \mathcal{H} -line graph is a subgraph of a graph H with the following property:*

(L): *There is a family of (induced) subgraphs H^l ($l = 1, \dots, m$) of H such that:*

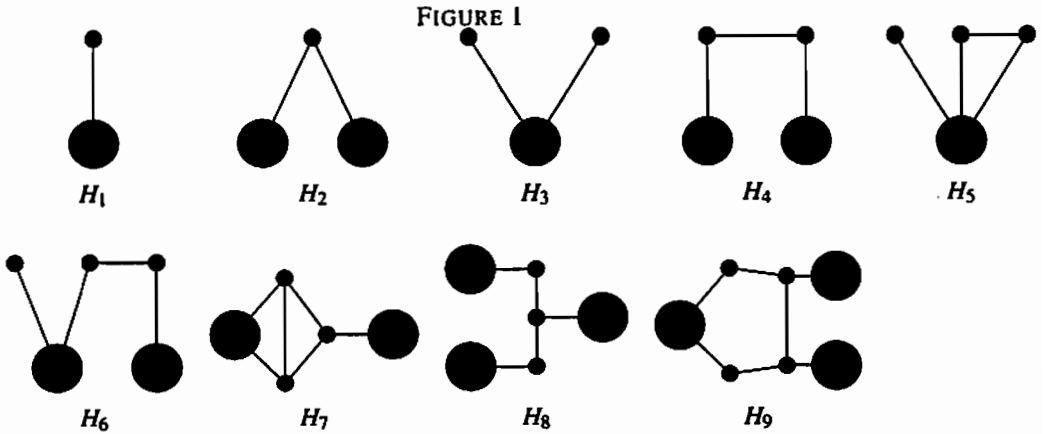
- (i) *Each slim vertex of H is in exactly one H^l .*
- (ii) *Two slim vertices in different H^l have at most one common fat neighbor, and they have one iff they are adjacent.*
- (iii) *Each H^l is isomorphic to a graph in \mathcal{H} .*
- (iv) *Each vertex of H is in one of the H^l .*
- (v) *If a slim vertex is adjacent to a fat vertex, then there exists an H^l containing both vertices.*

They consider it one of the problems to find a complete list of minimal forbidden subgraphs for slim (or arbitrary) $\{H_2, H_5, H_7, H_9\}$ -line graphs, where H_2, H_5, H_7 and H_9 are Hoffman graphs in Figure 1. If there exists the list, then it is expected that there exist the maximal forbidden graphs for slim $\{H_2, H_5, H_7, H_9\}$ -line graphs, by using the star complement technique. (see [6]). This might lead to the determination of the value $f(-1 - \sqrt{2})$. But it seems very difficult to find all minimal forbidden subgraphs in this case. In this paper, we investigate $\{H_2, H_5\}$ -line graphs and find all minimal forbidden subgraphs. Since non $\{H_2, H_5, H_7, H_9\}$ -line graphs are non $\{H_2, H_5\}$ -line graphs, it is a natural stream to consider this case.

We draw Hoffman graphs by depicting vertices as large (small) black dots if they are fat (slim). For a Hoffman graph H , $V_s H$ ($V_f H$) is the set of all slim (fat) vertices of H , $E_s H = E(H - V_f H)$, $s_H = \#V_s H$, and $f_H = \#V_f H$. For a slim vertex s of a Hoffman graph H , we define $N_H^s(s)$ ($N_H^f(s)$) to be the set of all slim (fat) neighbours of s , and $N_H(s)$ to be the set of all neighbours of s , i.e., $N_H(s) = N_H^s(s) \cup N_H^f(s)$. If Hoffman graphs X and Y satisfy that there exists a set V such that $X, Y \subset V$, then we say that two Hoffman graphs have same type vertices. Ordinary graphs can be regarded as Hoffman graphs without fat vertices, and such graphs are called slim. We write $G \subset H$ if G is an induced subgraph of H . We denote by $\langle S \rangle_H$ the subgraph of H induced by a set of vertices S . If a vertex x is adjacent to a vertex y , then we write $x \sim y$. We write $G \sqsubset H$ if H contains an induced subgraph isomorphic to G .

For a Hoffman graph Γ , its adjacency matrix $A_\Gamma = \begin{bmatrix} A(\Gamma) & C(\Gamma) \\ C(\Gamma)^T & O \end{bmatrix}$ is the $(0, 1)$ -matrix $(a_{i,j})$, where $a_{i,j} = 1$ if $i \sim j$, and $a_{i,j} = 0$ otherwise, in a labeling in which the fat vertices come last. Since $A(\Gamma) - C(\Gamma)C(\Gamma)^T$ is a real symmetric matrix, its eigenvalues must be real, and are called the eigenvalues of Γ . Let $\lambda_{\min}(\Gamma)$ denote the minimum eigenvalue of Γ . If $G \subset H$, then $\lambda_{\min}(G) \geq \lambda_{\min}(H)$ holds (see [2]).

In the following, all graphs considered are Hoffman graphs and all subgraphs considered are induced subgraphs.



2. THE GENERALIZATION OF LINE GRAPHS

Let \mathcal{H} be a family of isomorphism classes of Hoffman graphs. For any \mathcal{H} -line graph Γ , there exists a Hoffman graph H satisfying the property (L) of Definition 1.2. Then we call H an \mathcal{H} -cover graph of Γ . An \mathcal{H} -cover graph H of Γ is said to be strict if $V_3\Gamma = V_3H$. If Γ is an \mathcal{H} -strict cover graph of itself, then we call Γ a special \mathcal{H} -line graph. In this case, we call the set $\{H^i \mid i = 1, 2, \dots, m\}$ in Definition 1.2 an \mathcal{H} -partition of H . For Hoffman graphs Γ_1 and Γ_2 with same type vertices, let $\Gamma_1 \uplus \Gamma_2$ denote the Hoffman graph $(V\Gamma_1 \cup V\Gamma_2, E)$, where $E = \{v_1v_2 \mid v_i \in V\Gamma_i (i = 1, 2), N_{\Gamma_1}^f(v_1) \cap N_{\Gamma_2}^f(v_2) \neq \emptyset \text{ if } v_i \in V_3\Gamma_i (i = 1, 2)\} \cup E\Gamma_1 \cup E\Gamma_2$. Then it is clear that H is represented by $H^1 \uplus H^2 \uplus \dots \uplus H^s$.

It is shown in [2] that $\{H_2\}$ -line graphs without fat vertices are just the ordinary line graphs and $\{H_2, H_3\}$ -line graphs without fat vertices are just the generalized line graphs.

Lemma 2.1. *Let \mathcal{H} be a family of isomorphism classes of Hoffman graphs. Let K be an \mathcal{H} -line graph, and let $\mathcal{K} = \mathcal{H} \cup \{[K]\}$. Then a Hoffman graph Γ is an \mathcal{H} -line graph if and only if it is a \mathcal{K} -line graph.*

Proof. The necessity is obvious since $\mathcal{H} \subset \mathcal{K}$. Let Φ be a \mathcal{K} -partition of a \mathcal{K} -cover graph of Γ . Let $\Phi_0 = \{P \in \Phi \mid [P] = [K]\}$, and let $\Phi_1 = \Phi \setminus \Phi_0$. Now, for any $P \in \Phi_0$, there exists an \mathcal{H} -partition Φ_P of an \mathcal{H} -cover graph of P . Now we define $\Psi = \Phi_1 \cup \bigcup_{P \in \Phi_0} \Phi_P$. Then Ψ is an \mathcal{H} -partition of an \mathcal{H} -cover graph of Γ . We have completed the proof of Lemma. ■

Further we obtain the following lemma as a generalization of Lemma 2.1.

Lemma 2.2. *Let \mathcal{H} be a family of isomorphism classes of Hoffman graphs. Let \mathcal{G} be a family of isomorphism classes of \mathcal{H} -line graphs, and let $\mathcal{K} = \mathcal{H} \cup \mathcal{G}$. Then a Hoffman graph Γ is an \mathcal{H} -line graph if and only if it is a \mathcal{K} -line graph.*

For a family \mathcal{H} of isomorphism classes of Hoffman graphs, we define $\mathcal{H}^\# = \bigcup_{H \in \mathcal{H}} \{\{W \mid W \subset H\}\}$. Then $\mathcal{H} \subset \mathcal{H}^\#$ and an $\mathcal{H}^\#$ -line graph is an \mathcal{H} -line graph by Lemma 2.2. That is to say that the \mathcal{H} -line graphs are the same as $\mathcal{H}^\#$ -line graphs. An $\mathcal{H}^\#$ -line graph has more useful properties than an \mathcal{H} -line graph. In this paper, it is enough that the claim of Theorem 2.3 is satisfied. For example, every $\mathcal{H}^\#$ -line graph has $\mathcal{H}^\#$ -strict cover graph. We can give a proof of this claim in the same way as the proof of Theorem 2.3. But we need not to deal

with a size as large as $\#\mathcal{H}$. In order to compute easily, we would like to get a least-size family satisfying the claim of Theorem 2.3. We call \mathcal{K} an optimization of \mathcal{H} if \mathcal{K} is a minimum size family satisfying containing \mathcal{H} and having the following property:

(#1) For each $H \in \mathcal{K}$, there exists a \mathcal{H} -strict cover graph of H .

From now on, \mathcal{H} is a optimized family of isomorphism classes of Hoffman graphs.

Theorem 2.3. *Every \mathcal{H} -line graph has \mathcal{H} -strict cover graph.*

Proof. Let Γ be an \mathcal{H} -line graph, and let Γ' be an \mathcal{H} -cover graph of Γ . There exists an \mathcal{H} -partition P of Γ' . Let $P_0 = \{W \in P \mid V_s W \subset V_s \Gamma\}$. Fix $W \in P \setminus P_0$. Now there exists $H \in \mathcal{H}$ such that $[W \cap V_s \Gamma] \sqsubset H$. Hence $[W \cap V_s \Gamma] \in \mathcal{H}$. Thus there exists an \mathcal{H} -strict cover graph $\rho(W)$ of $W \cap V_s \Gamma$. Then $\biguplus_{W \in P_0} W \uplus \biguplus_{W \in P \setminus P_0} \rho(W)$ is an \mathcal{H} -strict cover graph of Γ . \blacksquare

3. A REPRESENTATION OF THE GENERALIZED LINE GRAPHS BY A MATRIX TECHNIQUE

For a Hoffman graph H , let $\Phi = \{H^k \mid k = 1, 2, \dots, s\}$ be a family of subgraphs of H satisfying $V_s H = \bigcup_{k=1}^s V_s H^k$. Put $\tilde{f}_H = \sum_{k=1}^s f_{H^k}$. Note that $f_H \leq \tilde{f}_H$. We define the matrices $F'(H^k)$, $F(\Phi)$ and $M(\Phi)$ with the following entries:

$$F'(H^k)_{i,j} = \begin{cases} 1 & i = j \text{ for } i \in V_f H^k, j \in V_f H, \\ 0 & \text{otherwise.} \end{cases} \quad : (f_{H^k} \times f_H)\text{-matrix.}$$

$$F(\Phi) = \begin{bmatrix} F'(H^1) \\ \vdots \\ F'(H^s) \end{bmatrix} \quad : (\tilde{f}_H \times f_H)\text{-matrix.}$$

$$M(\Phi) = \begin{bmatrix} C(H^1) & & \\ & \ddots & \\ & & C(H^s) \end{bmatrix} \quad \left(= \bigoplus_{l=1}^s C(H^l) \right) \quad : (s_H \times \tilde{f}_H)\text{-matrix.}$$

Lemma 3.1. *For a Hoffman graph H , let $\Phi = \{H^k \mid k = 1, 2, \dots, m\}$ be a family of subgraphs of H satisfying $V_s H = \bigcup_{k=1}^m V_s H^k$. Then $M(\Phi)F(\Phi) = C(H)$*

Let \mathcal{H} be a family of isomorphism classes of Hoffman graphs, and let $\mathbb{H}_n(\mathcal{H})$ be the set of special \mathcal{H} -line graphs with n slim vertices and same type vertices. We define $C_n(\mathcal{H}) = \bigcup_{H \in \mathbb{H}_n(\mathcal{H})} P(H)$, where $P(H)$ is a set with the \mathcal{H} -partitions of a special \mathcal{H} -line graph H as elements. For each $\Phi = \{H^1, H^2, \dots, H^s\} \in C_n(\mathcal{H})$, we put $\omega(\Phi)$ as follows:

$$\omega(\Phi) = M(\Phi)F(\Phi)F(\Phi)^T M(\Phi)^T - \bigoplus_{l=1}^s (C(H^l)C(H^l)^T - A(H^l)).$$

Lemma 3.2. *Let Γ be an \mathcal{H} -line graph. If Φ is an \mathcal{H} -partition of an \mathcal{H} -strict cover graph of Γ , then $\omega(\Phi)$ is equal to an adjacency matrix of $\Gamma \cap V_s \Gamma$.*

Proof. Obviously $\Phi \in C_n(\mathcal{H})$. Hence, since there exists a special \mathcal{H} -line graph $H \in \mathbb{H}_n(\mathcal{H})$ such that $H = \biguplus_{W \in \Phi} W$, we can put $\Phi = \{H^k \mid H^k \subset H, 1 \leq k \leq s\}$. Put $M = M(\Phi)$ and $F = F(\Phi)$. From Lemma 3.1, $(MFF^T M^T)_{i,j} = \sum_{l=1}^s (MF)_{i,l}(MF)_{j,l} =$

$\#(N_H^f(i) \cap N_H^f(j))$.

Without difficulty, we obtain the results as follows:

$$(\oplus_{l=1}^s C(H^l)C(H^l)^T)_{i,j} = \begin{cases} \#(N_H^f(i) \cap N_H^f(j)) & i, j \in V_s H^l, \\ 0 & \text{otherwise,} \end{cases} \quad (l = 1, 2, \dots, s).$$

$$(\oplus_{l=1}^s A(H^l))_{i,j} = \begin{cases} 1 & i \sim j \in V_s H^l, \\ 0 & \text{otherwise,} \end{cases} \quad (l = 1, 2, \dots, s).$$

Hence

$$\begin{aligned} \omega(\Phi)_{i,j} &= \begin{cases} 1 & i \sim j \in V_s H^l (l = 1, 2, \dots, s), \\ \#(N_H^f(i) \cap N_H^f(j)) & i \in V_s H^k, j \in V_s H^l (k \neq l), \\ 0 & \text{otherwise.} \end{cases} \\ &= \begin{cases} 1 & i \sim j, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

■

From Lemma 3.1 and Lemma 3.2, for an \mathcal{H} -partition Φ of any special \mathcal{H} -line graph Γ , $\omega(\Phi)$ is the adjacency matrix for the slim vertices of Γ , and $M(\Phi)F(\Phi)$ is the adjacency matrix for the slim vertices and the fat vertices of Γ . Hence, for $\Phi \in C_n(\mathcal{H})$, there exists a special \mathcal{H} -line graph Γ such that $A(\Gamma) = \omega(\Phi)$ and $C(\Gamma) = M(\Phi)F(\Phi)$.

4. FORBIDDEN GRAPHS FOUND BY COMPUTER SEARCH

In this section, we shall consider the $\{H_2, H_5\}$ -line graphs. It turns out that $\{H_2, H_3, H_5\}$ is an optimization of $\{H_2, H_5\}$. From now on, $\mathcal{H} = \{H_2, H_3, H_5\}$.

Proposition 4.6 and Proposition 4.7 are the main results in this section. It is very hard to obtain the propositions without computer search. In this paper, we have computed by the software MAGMA¹. In order to prove the propositions, we show some lemmas and some algorithm.

Lemma 4.1. *Let Γ be a connected special $\{H_2\}$ -line graph with an $\{H_2\}$ -partition \mathcal{Q} . Then there exists a Hoffman graph $P \in \mathcal{Q}$ such that $\bigcup_{W \in \mathcal{Q} \setminus \{P\}} W$ is connected.*

Proof. It is known that every connected graph has a vertex which is not a cut vertex. (see [7]). Hence we obtain the proof of this lemma without difficulty. ■

Lemma 4.2. *Let H be a special $\{[H^1], [H^2]\}$ -line graph with a $\{[H^1], [H^2]\}$ -partition $\Phi_0 = \{H^1, H^2\}$, where $H^k \subset H$ ($k = 1, 2$). Then $\omega(\Phi_0) = \omega(\Phi_1)$, $M(\Phi_0)F(\Phi_0) = M(\Phi_1)F(\Phi_1)$, where $\Phi_1 = \{H\}$.*

Proof. Without difficulty, we obtain the proof by checking the entries of the matrices. ■

Let $\text{entry}(M)$ denote the set of entries of a matrix M . We show the following algorithm to obtain $X \uplus Y$ for Hoffman graphs X and Y .

Algorithm 4.3. [Input: Hoffman graphs X and Y with same type vertices] [Output: $X \uplus Y$ or "error"]

1) $C := M(\{X, Y\})F(\{X, Y\})$, $A := \omega(\{X, Y\})$ and $V := VX \cup VY$.

¹URL: <http://magma.maths.usyd.edu.au/magma/>

2) If $\text{entry}(A) \subset \{0, 1\}$, return the graph $(V, \{xy \mid x, y \in V, (A_{x,y} = 1 \text{ or } C_{x,y} = 1)\})$. If not so, return the message "error". End.f

If $V_s X \cap V_s Y = \emptyset$, this algorithm returns $X \uplus Y$. If not so, it returns the message "error". Let Ω_n be a maximal indexed set of connected special $\{H_2\}$ -line graphs with n vertices such that the elements of Ω_n are not isomorphic to each other. Note that $\#\Omega_1 = 1$. Let $\Omega_1 = \{\Gamma_1\}$, where Γ_1 is a Hoffman graph satisfying $[\Gamma_1] = H_2$ and $V_s \Gamma_1 = \{1\}$. We shall show the following algorithm in order to obtain sets Ω_i ($i = 2, 3, \dots, n$).

Algorithm 4.4. [Input: a number $n (> 1)$] [Output: sets $\Omega_2, \Omega_3, \dots, \Omega_n$]

- 1) Let $L(X, Y)$ be the executive result of Algorithm 4.3 for Hoffman graphs X and Y .
 $i := 2$.
- 2) $j := 1$. $\Omega_i := \emptyset$.
- 3) $k := 1$. $H := (\Omega_{i-1})_j$. Let f be a fat vertex to be not in $V_f H$. Let Ψ be the indexed set $\{K \mid V_s K = \{i\}, V_f K \cap V_f H \neq \emptyset, f \in V_f K \text{ if } V_f K \not\subset V_f H, [K] = H_2\}$. (By Lemma 4.1, the set Ψ is enough to consider Ω_i)
- 4) $L := L(H, \Psi_k)$.
- 5) If $L \neq \text{"error"}$ and $[L] \notin \{[G] \mid G \in \Omega_i\}$, then $\Omega_i := \Omega_i \cup \{L\}$. (By Lemma 4.2, this operation has no problem.)
- 6) If $k < \#\Psi$, $k := k + 1$ and go to 4).
- 7) If $j < \#\Omega_{i-1}$, $j := j + 1$ and go to 3).
- 8) Return Ω_i . (Note that $\Omega_i \neq \emptyset$.)
- 9) If $i < n$, $i := i + 1$ and go to 2).
- 10) End.

Let S_n be the family of isomorphism classes of special \mathcal{H} -line graphs whose subgraph consist of the slim vertices is connected. Note that $S_i = \Omega_i$ ($i = 1, 2$). We shall show the following algorithm in order to obtain S_n .

Algorithm 4.5. [Input: a number $n (> 2)$] [Output: S_n]

- 1) Let $L(X, Y)$ be the executive result of Algorithm 4.3 for Hoffman graphs X and Y . Let $f(x)$ be the indexed set $\{(a_1, a_2, \dots, a_m) \mid a_i \leq a_{i+1}, a_i \in \{2, 3\}, \sum_{i=1}^m a_i = x\}$. (Note that $\#f(x) \neq \emptyset$ if x is a number at least 2.) $R_n := \{[G] \mid G \in \Omega_n\}$. $i = 0$. $F := f(n - i)$.
- 2) $j := 1$.
- 3) $k := 1$. $H := (\Omega_i)_j$.
- 4) $s := F_k$.
- 5) If $s = 2$, then $\Psi := \{K \mid V_s K = \{i+1, i+2\}, V_f K \subset V_f H, [K] = H_3\}$. If not so, then $\Psi := \{K \mid V_s K = \{i+1, i+2, i+3\}, V_f K \subset V_f H, [K] = H_5\}$. (Note that $(V_s(H \uplus K))_{H \uplus K}$ is not connected if $V_f K \cap V_f H = \emptyset$.)
- 6) $L := L(H, \Psi_k)$. (Note that $\#V_s L = n$.)
- 7) If $[L] \notin R_n$, then $R_n := R_n \cup \{[L]\}$. (Since $\#V_f \Psi_k = 1$, $L \neq \text{"error"}$. By Lemma 4.2, this operation has no problem.)
- 8) If $k < \#\Psi$, $k := k + 1$ and go to 6).
- 9) If $j < \#\Omega_i$, $j := j + 1$ and go to 3).
- 10) If $i < n - 2$, $i := i + 1$ and go to 2).
- 11) return R_n . End.

Let S'_n be the family of isomorphism classes of connected slim \mathcal{H} -line graphs. Let $S''_n = \{[(V_s \Gamma)_\Gamma] \mid [\Gamma] \in S_n\}$. We obtain Ω_n , ($2 \leq n \leq 9$) as the executive result of Algorithm 4.4 for a number $2 \leq n \leq 9$. Further, We obtain S_n ($3 \leq n \leq 9$) as the executive result of

Algorithm 4.5 for each number $3 \leq n \leq 9$. Then $\#S_n = \#S'_n = \#S''_n$ for $n = 7, 8, 9$. Hence we obtain the following proposition.

Proposition 4.6. *Let Γ be an \mathcal{H} -line graph without fat vertices. If $\#V\Gamma = 7, 8$ or 9 , then there exists one and only one \mathcal{H} -strict cover graph of Γ .*

For every vertex v of a non \mathcal{H} -line graph Γ without fat vertices, if $\Gamma - v$ is an \mathcal{H} -line graph, then Γ is said to be minimal. Let \mathcal{X}_n be the family of isomorphism classes of connected slim graphs with n vertices and the smallest eigenvalue at least $-1 - \sqrt{2}$.

Let \mathcal{F}_n be the family of isomorphism classes of minimal non \mathcal{H} -line graphs with n vertices and without fat vertices. By computer search, we obtain $\#S'_n = \#\mathcal{X}_n$ ($n = 1, 2, 3, 4$), and $\#S'_5 + 1 = \#\mathcal{X}_5$, i.e., $\mathcal{F}_5 = \{G_{5,1}\}$. The set $\mathcal{X}_n \setminus S'_n$ is the family of isomorphism classes of connected non \mathcal{H} -line graphs with n vertices. Hence we obtain $\mathcal{F}_6 = \{G_{6,i} \mid i = 1, 2, \dots, 28\}$, $\mathcal{F}_7 = \{G_{7,i} \mid i = 1, 2, \dots, 7\}$, and $\mathcal{F}_8 = \{G_{8,1}\}$ by removing the non \mathcal{H} -line graphs be not minimal from $\mathcal{X}_n \setminus S'_n$ ($n = 6, 7, 8, 9$). (cf. Figure 2). Let $\mathcal{F} = \mathcal{F}_5 \cup \mathcal{F}_6 \cup \mathcal{F}_7 \cup \mathcal{F}_8$. By the above discussion, we obtain the following proposition.

Proposition 4.7. *Let Γ be a minimal non \mathcal{H} -line graph without fat vertices. Then $[\Gamma] \in \mathcal{F}$ if $\lambda_{\min}(\Gamma) \geq -1 - \sqrt{2}$ and $\#V\Gamma \leq 9$.*

5. THE MINIMAL FORBIDDEN SUBGRAPHS

The property of being an \mathcal{H} -line graph is hereditary. Hence we can look for minimal graphs that are not \mathcal{H} -line graphs. In this section, we find all such graphs.

For a graph Γ , we define the set of vertices whose valency is equal to one in Γ by $P(\Gamma)$, and we define the valency of a vertex v in Γ by $\text{valency}(v)_\Gamma$. A star is a graph isomorphic to the complete bipartite graph $K_{n,1}$, and its center is the unique vertex of the rear part of $K_{n,1}$.

Lemma 5.1. *Let Γ be a connected slim graph. If, for any spanning tree T of Γ , $\langle P(T) \rangle_\Gamma$ is a complete graph, then Γ is a complete graph or a cycle.*

Proof. Let T be a spanning tree of Γ such that the size of $P(T)$ is a maximum. Let $\Gamma_0 = \langle V\Gamma \setminus P(T) \rangle_\Gamma$, let $E_1 = E\Gamma \setminus (E\Gamma_0 \cup E\langle P(T) \rangle_\Gamma)$, let $\Gamma_1 = \langle E_1 \rangle_\Gamma$, and let $T_0 = T \setminus P(T)$. Now T_0 is a spanning tree of Γ_0 .

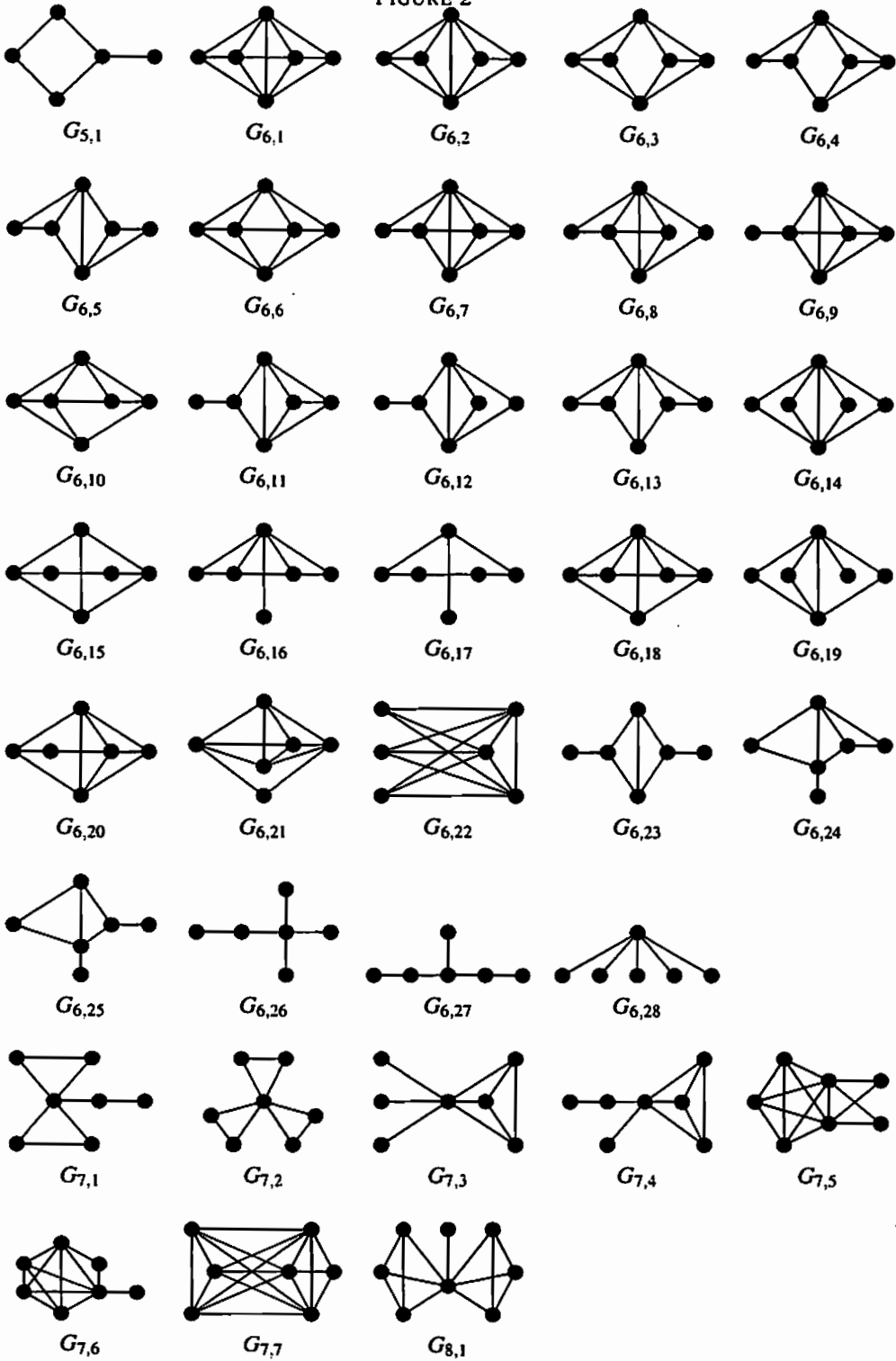
Now suppose $P(T_0) \setminus V\Gamma_1 \neq \emptyset$. Then there exists a vertex v such that $v \in P(T_0) \setminus V\Gamma_1$. Now $\text{valency}(v)_{T_0} = 1$ and $\text{valency}(v)_T \geq 2$. Hence there exists a vertex u in $V\Gamma \setminus V\Gamma_0 (= P(T))$ such that $v \sim u$. And therefore $uv \in E_1$, i.e., $v \in \Gamma_1$. But then v dose not satisfy the hypothesis. Hence $P(T_0) \subset \Gamma_1$.

Case 1. If $\#P(T_0) = 0$, then Γ is a complete graph.

Case 2. Suppose $\#P(T_0) \geq 3$. Let $u_1 \in P(T_0)$. Then there exists a vertex $v_1 \in VP(T)$ such that $v_1 u_1 \in ET$. Since $\langle P(T) \rangle_\Gamma$ is a complete graph, there exists a star St as a spanning tree of $\langle P(T) \rangle_\Gamma$ whose center is the vertex v_1 . Then the graph with the edge set $ESt \cup \{v_1 u_1\} \cup (ET \setminus E_1)$ is a spanning tree of Γ , and we put the spanning tree T' . By the hypothesis, T' is a complete graph. Now $\#P(T') = (\#St - 1) + (\#P(T_0) - 1) = \#St + \#P(T_0) - 2 \geq \#P(T) + 1$. But this contradicts that the size of $P(T)$ is a maximum.

Case 3. Suppose $\#P(T_0) = 2$, i.e., T_0 is a path. Let $P(T_0) = \{u_1, u_2\}$. Now suppose that there exist a vertex v in $P(T)$ and a vertex w in $V\Gamma \setminus (P(T_0) \cup P(T))$ such that $vw \in ET$. Since $\langle P(T) \rangle_\Gamma$ is a complete graph, there exists a star Sr' as a spanning tree of $\langle P(T) \rangle_\Gamma$ whose center is the vertex v . Then the graph with the edge set $ES'_r \cup \{vw\} \cup (ET \setminus E_1)$ is a spanning tree of Γ , and we put the spanning tree T'' . By the hypothesis, T'' is a complete

FIGURE 2



graph. Now $\#P(T'') = (\#S'_T - 1) + \#P(T_0) = \#P(T) + 1$. But this contradicts the hypothesis that the size of $P(T)$ is a maximum. Hence, in T , any vertex in $VT \setminus (P(T_0) \cup P(T))$ is adjacent to no vertex in $P(T)$.

If $\#P(T) \geq 3$, then either u_1 or u_2 is adjacent to at least two vertices of $P(T)$ in T . Without loss of generality, let u_1 be adjacent to at least two vertices of $P(T)$ in T , and let v_1, v_2 be vertices of $P(T)$ satisfying $v_1u_1, v_2u_1 \in ET$. Now there exists a star S as a spanning tree of $\langle P(T) \rangle_\Gamma$ whose center is the vertex v_1 . Then the graph with the edge set $ES \cup \{v_1u_1\} \cup (ET \setminus E_1)$ is a spanning tree of Γ . We put the spanning tree T^3 . Hence $P(T^3) = (P(T) \cup \{u_2\}) \setminus \{v_1\}$ by $\text{valency}(u_2)_{T^3} = 1$. Thus u_2 is adjacent to all vertices of $VP(T) \setminus \{v_1\}$ in Γ . By the similar way, we obtain the result that u_2 is adjacent to all vertices of $VP(T) \setminus \{v_2\}$ in Γ . Hence u_2 is adjacent to all vertices of $VP(T)$ in Γ . Then the graph with the edge set $\{xu_2 \mid x \in P(T)\} \cup ET_0$ is a spanning tree of Γ . We put the spanning tree T^4 . Then $\#P(T^4) = \#P(T) + \#\{u_2\}$. But this contradicts the hypothesis that the size of $P(T)$ is a maximum. By the above discussion, $\#P(T) = 2$.

Suppose that $E\Gamma_0 \setminus ET_0 \neq \emptyset$. Then there exists a spanning tree T^5 of Γ such that $\#P(T^5) > \#P(T)$, a contradiction.

Now $\langle P(T) \cup P(T_0) \rangle_\Gamma$ is a path by the hypothesis that the size of $P(T)$ is a maximum. Hence Γ is a cycle if $\#P(T_0) = 2$.

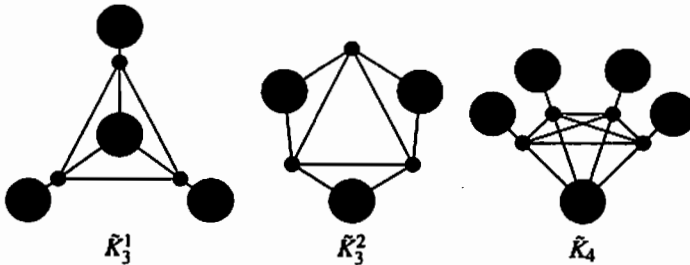
By the above discussion, we have completed the proof of Lemma. ■

Lemma 5.2. *Let Γ be a connected slim graph. If Γ is not either a complete graph or a cycle, then there exists a non-adjacent pair $\{x, y\}$ in $V\Gamma$ such that $\Gamma - xy$ is connected.*

Proof. From Lemma 5.1, there exists a spanning tree T of Γ such that $\langle P(T) \rangle_\Gamma$ is not a complete graph. Then there exists a non-adjacent pair $\{x, y\}$ in $\langle P(T) \rangle_\Gamma$. $T - xy$ is a connected graph by the definition of $P(T)$. Hence $\Gamma - xy$ is a connected graph since $T - xy$ is a spanning tree of $\Gamma - xy$. ■

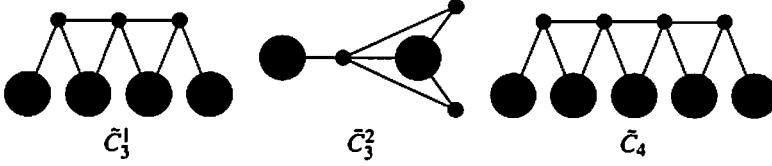
Lemma 5.3. *There exists one and only one \mathcal{H} -strict cover graph of the complete graph with at least four vertices.*

Proof. Without difficulty, we can show that an \mathcal{H} -strict cover graph of the complete graph with three vertices is isomorphic to either \tilde{K}_3^1 or \tilde{K}_3^2 . Hence an \mathcal{H} -strict cover graph of the complete graph with four vertices is only isomorphic to \tilde{K}_4 . By the inductive method, we have completed the proof of Lemma.



Lemma 5.4. *There exists one and only one \mathcal{H} -strict cover graph of the cycle with at least five vertices.* ■

Proof. Without difficulty, we can show that an \mathcal{H} -strict cover graph of the path with three vertices is isomorphic to either \tilde{C}_3^1 or \tilde{C}_3^2 . Now, for any sub-path with four vertices, an \mathcal{H} -strict cover graph of the path is only isomorphic to \tilde{C}_4 . Hence we have completed the proof of Lemma. ■



Theorem 5.5. *Let Γ be a connected slim \mathcal{H} -line graph with at least seven vertices. Then there exists one and only one \mathcal{H} -strict cover graph of Γ .*

Proof. Now $H - s$ is not always an \mathcal{H} -strict cover graph of itself for an \mathcal{H} -line graph H , only in this proof, we consider that $H - s$ is an \mathcal{H} -strict cover graph of itself by adding lack of fat vertices.

First, by Proposition 4.6, there exists one and only one \mathcal{H} -strict cover graph of Γ if $\#V\Gamma = 7, 8$ or 9 . In the next place, assume that there exists one and only one \mathcal{H} -strict cover graph of Γ when $\#V\Gamma = i$.

Suppose $\#V\Gamma = i + 1$. If Γ is either a complete graph or a cycle, then there exists one and only one \mathcal{H} -strict cover graph of Γ by Lemma 5.3 and Lemma 5.4. Thus we may assume that Γ is neither a complete graph nor a cycle. Then there exists a non-adjacent pair $\{x, y\}$ in $V\Gamma$ such that $\Gamma - xy$ is a connected graph by Lemma 5.2. Obviously, $\Gamma - x$ and $\Gamma - y$ are connected graphs.

Let K and L be \mathcal{H} -strict cover graphs of Γ . Then we can represent $K = K_1 \uplus K_2 \uplus \dots \uplus K_\alpha$ by all elements $K_1, K_2, \dots, K_\alpha$ of an \mathcal{H} -partition of K ; similarly $L = L_1 \uplus L_2 \uplus \dots \uplus L_\beta$.

Without loss of generality, we may consider the following three cases:

Case 1. Suppose that $x, y \in V_s K_1$, $x \in V_s L_1$ and $y \in V_s L_2$. Now there exists one and only one \mathcal{H} -strict cover graph of $\Gamma - x$ ($\Gamma - y$).

Hence

$$(1) \quad (K_1 - x) \uplus K_2 \uplus \dots \uplus K_\alpha = (L_1 - x) \uplus L_2 \uplus \dots \uplus L_\beta.$$

$$(2) \quad (K_1 - y) \uplus K_2 \uplus \dots \uplus K_\alpha = L_1 \uplus (L_2 - y) \uplus \dots \uplus L_\beta.$$

Now there exists a fat vertex $f \in V_f K_1$ such that $xf \in E(K_1 - y)$ and $yf \in E(K_1 - x)$. Hence $xf \in EL_1$ and $yf \in EL_2$. Thus $x \sim y$ in Γ , a contradiction.

Case 2. Suppose that $x \in V_s K_1 \cap V_s L_1$ and $y \in V_s K_2 \cap V_s L_2$. Now there exists one and only one \mathcal{H} -strict cover graph of $\Gamma - x$ ($\Gamma - y$).

Hence

$$(3) \quad (K_1 - x) \uplus K_2 \uplus \dots \uplus K_\alpha = (L_1 - x) \uplus L_2 \uplus \dots \uplus L_\beta.$$

$$(4) \quad K_1 \uplus (K_2 - y) \uplus \dots \uplus K_\alpha = L_1 \uplus (L_2 - y) \uplus \dots \uplus L_\beta.$$

By Definition 1.2-(v), $f \in V_f K_2 \Leftrightarrow fy \in EK_2 \Leftrightarrow fy \in EL_2 \Leftrightarrow f \in V_f L_2$.

Suppose $z \in V_s K_2$ satisfying $zy \notin E\Gamma$. Then there exists a fat vertex f such that $zf, yf \in EK_2$. Hence $zf \in EL_2$ by $z \not\sim y$ in Γ . Thus we obtain that $z \in V_s K_2 \Leftrightarrow z \in V_s L_2$ if $zy \notin E\Gamma$. In the next place, suppose $z \in V_s K_2$ satisfying $zy \in E\Gamma$. Then there exist a slim vertex v and a fat vertex f such that $EK_2 = \{vf, zf, gf, zy\}$. Hence $v \in L_2$ by $f \in V_f L_2$ and $v \not\sim y$ in Γ .

Since $f \in V_f L_2$ and $v \neq z$ in Γ , $z \in L_2$.

By the above discussion, we obtain that $K_2 = L_2$. By the similar way, we obtain that $K_1 = L_1$.

By $K_i = L_i$ ($i = 1, 2$),

$$((K_1 - x) \uplus K_2 \uplus \dots \uplus K_\alpha) \setminus V_s(K_1 \uplus K_2) = ((L_1 - x) \uplus L_2 \uplus \dots \uplus L_\beta) \setminus V_s(L_1 \uplus L_2).$$

Hence $K_3 \uplus \dots \uplus K_\alpha = L_3 \uplus \dots \uplus L_\beta$. Thus $K = L$.

Case 3. Suppose $x, y \in K_1 \cap L_1$. Now suppose $[K_1] \neq [L_1]$. Without loss of generality, let $[K_1] = H_3$ and let $[L_1] = H_5$. Since $K_1 - xy = \emptyset$, $K_2 \uplus \dots \uplus K_\alpha = (L_1 - xy) \uplus L_2 \uplus \dots \uplus L_\beta$. Hence

$$(5) \quad K = K_1 \uplus (L_1 - xy) \uplus L_2 \uplus \dots \uplus L_\beta.$$

Now there exists a slim vertex z different from x and y in L_1 . Without loss of generality, we may suppose that $x \neq z$ and $y \sim z$. Since $y \in V_s K_1$, $z \in L_1 - xy$ and $yz \in E\Gamma$, there exists one and only one common fat neighbour f of y and z in K by (5) as Definition 1.2-(ii). Hence $x \sim f$ by $[K_1] = H_3$. Thus $x \sim z$, a contradiction.

By the above discussion, $[K_1] = [L_1]$.

Let f be the unique fat vertex of K_1 . Then $xf \in K_1 - y \subset (K_1 - x) \uplus \dots \uplus K_\beta = (L_1 - x) \uplus \dots \uplus L_\alpha$. Hence $xf \in L_1 - y$ by $x \in L_1 - y$, i.e., $f \in L_1$. Thus $V_f K_1 = V_f L_1$.

When $[K_1] = H_3$,

$$(6) \quad \begin{aligned} K_2 \uplus \dots \uplus K_\alpha &= (K_1 - xy) \uplus K_2 \uplus \dots \uplus K_\alpha \\ &= (L_1 - xy) \uplus L_2 \uplus \dots \uplus L_\beta \\ &= L_2 \uplus \dots \uplus L_\beta. \end{aligned}$$

Hence when $[K_1] = H_3$, $K = L$ since $V_s K_1 = \{x, y\} = V_s L_1$

Suppose $[K_1] = H_5$. Let s be the unique slim vertex of $K_1 - xy$. Suppose that $V_s(K_1 - xy) \neq V_s(L_1 - xy)$. Then $s \in V_s(L_2 \uplus \dots \uplus L_\beta)$ by $s \notin V_s(L_1 - xy)$. Hence $sf \in L_2 \uplus \dots \uplus L_\alpha$. Thus $sx, sy \in EK_1$ by $f \in V_f L_1$, and the conclusion implies that $[K_1] \neq H_5$, a contradiction. By the above discussion, $V_s K_1 = V_s L_1$, i.e., $K = L$. ■

Lemma 5.6. *Let Γ be a slim \mathcal{H} -line graph with greater than seven vertices. Let S be the unique \mathcal{H} -strict cover graph of Γ given by Theorem 5.5. Let x be not a cut point of Γ , and let P be the \mathcal{H} -partition of the unique \mathcal{H} -strict cover graph of $\Gamma - x$. Then there exists a Hoffman graph H satisfying $[H] \in \mathcal{H}$ and $x \in V_s H$ such that $S = H \uplus \bigcup_{W \in A} W$, where $A = \{W \in P \mid V_s W \not\subset V_s H\}$.*

Proof. Let Q be an \mathcal{H} -partition of S . Now there exists the element H of Q such that $x \in VH$. Since $H - x$ is an \mathcal{H} -line graph, there exists an \mathcal{H} -partition R of an \mathcal{H} -strict cover graph of $H - x$.

Now $R \cup Q \setminus \{H\}$ is an \mathcal{H} -partition of an \mathcal{H} -strict cover graph of $\Gamma - x$. Hence $P = R \cup Q \setminus \{H\}$ without loss of generality. Since $V_s X \subset V_s H$ for all $X \in R$ and $V_s Y \not\subset V_s H$ for all $Y \in Q \setminus \{H\}$ by the definition 1.2, $S = H \uplus \bigcup_{W \in Q \setminus \{H\}} W = H \uplus \bigcup_{W \in A} W$. We have completed the proof of Lemma. ■

Lemma 5.7. *Let Γ be a connected slim graph which $\#V\Gamma \geq 9$, and is neither a complete graph nor a cycle. Let $\{x, y\}$ be a non-adjacent pair in $V\Gamma$ given by Lemma 5.2, and let P_0 be an \mathcal{H} -partition of the unique \mathcal{H} -strict cover graph (given by Theorem 5.5) of $\Gamma - xy$.*

Let $X \uplus \uplus_{W \in A_x} W$ be the unique \mathcal{H} -strict cover graph of $\Gamma - y$ given by Theorem 5.5; similarly, and let $Y \uplus \uplus_{W \in A_y} W$ be the unique \mathcal{H} -strict cover graph of $\Gamma - x$, where $A_x = \{W \in P_0 \mid V_s W \not\subset X\}$ and $A_y = \{W \in P_0 \mid V_s W \not\subset Y\}$. Then $Z \uplus \uplus_{W \in A_x \cap A_y} W$ is an $\mathcal{H} \cup \{[Z]\}$ -strict cover graph of Γ , where $Z = (X \uplus (Y - y)) \cup ((X - x) \uplus Y)$.

Proof. We put $W_0 = \uplus_{W \in A_x \cap A_y} W$.

$V_s X = \{x\} \cup \uplus_{W \notin A_x} V_s W$; similarly, $V_s Y = \{y\} \cup \uplus_{W \notin A_y} V_s W$. Now $V_s Z = V_s X \cup V_s Y$.

$$\begin{aligned} \text{Hence } V_s(Z \uplus W_0) &= \{x, y\} \cup \uplus_{W \notin A_x} V_s W \cup \uplus_{W \notin A_y} V_s W \cup \uplus_{W \in A_x \cap A_y} V_s W \\ &= \{x, y\} \cup \uplus_{W \in P_0} V_s W \\ &= V\Gamma. \end{aligned}$$

Since $P_0 \setminus A_x = A_y \setminus (A_x \cap A_y)$,

$E_s(X - x) = E_s \uplus_{W \in P_0 \setminus A_x} W = E_s \uplus_{W \in A_y \setminus (A_x \cap A_y)} W$.

Similarly $E_s(Y - y) = E_s \uplus_{W \in P_0 \setminus A_y} W = E_s \uplus_{W \in A_x \setminus (A_x \cap A_y)} W$.

$$\begin{aligned} \text{Hence } E_s(Z \uplus W_0) &= E_s(((X \uplus (Y - y)) \cup ((X - x) \uplus Y)) \uplus W_0) \\ &= E_s((X \uplus (Y - y) \uplus W_0) \cup E_s(((X - x) \uplus Y \uplus W_0)) \\ &= E_s(X \uplus \uplus_{W \in A_x} W) \cup E_s(Y \uplus \uplus_{W \in A_y} W) \\ &= E(\Gamma - y) \cup E(\Gamma - x) \\ &= E\Gamma \text{ (from } x \not\sim y). \end{aligned}$$

We have completed the proof of Lemma. ■

Proposition 5.8. *Let Γ be a connected slim graph with the smallest eigenvalue at least $-1 - \sqrt{2}$. If Γ is a minimal non \mathcal{H} -line graph without fat vertices, then $\#V\Gamma < 9$.*

Proof. Suppose $\#V\Gamma \geq 9$. By Proposition 4.7, $[\Gamma] \notin \mathcal{F}$ if $\#V\Gamma = 9$ a contradiction. Thus we may suppose $\#V\Gamma > 9$.

Since a complete graph and a cycle graph are \mathcal{H} -line graphs, Γ is neither a complete graph nor a cycle. Hence, by Lemma 5.2, there exists a non-adjacent pair $\{x, y\}$ in $V\Gamma$ such that $\Gamma - x$, $\Gamma - y$ and $\Gamma - xy$ are connected graphs. Since $\Gamma - xy$ is an \mathcal{H} -line graph, there exists an \mathcal{H} -partition P_0 of the unique \mathcal{H} -strict cover graph (given by Theorem 5.5) of $\Gamma - xy$. And then, by Lemma 5.6, there exists the unique \mathcal{H} -strict cover graph $Y \uplus \uplus_{W \in A_y} W$ of $\Gamma - x$, where $[Y] \in \mathcal{H}$, $y \in V_s Y$ and $A_y = \{W \in P_0 \mid V_s W \not\subset V_s Y\}$; similarly, there exists the unique \mathcal{H} -strict cover graph $X \uplus \uplus_{W \in A_x} W$ of $\Gamma - y$, where $[X] \in \mathcal{H}$, $x \in V_s X$ and $A_x = \{W \in P_0 \mid V_s W \not\subset V_s X\}$.

Hence, by Lemma 5.7, $Z \uplus \uplus_{W \in A_x \cap A_y} W$ is the unique $\mathcal{H} \cup \{[Z]\}$ -line graph of Γ , where $Z = (X \uplus (Y - y)) \cup ((X - x) \uplus Y)$.

Now suppose $V_f X \cap V_f Y = \emptyset$.

(i). Suppose $V_s X \cap V_s Y = \emptyset$. Since Z is an \mathcal{H} -line graph, $Z \uplus \uplus_{W \in A_x \cap A_y} W$ is an \mathcal{H} -line graph by Lemma 2.1. Hence Γ is an \mathcal{H} -line graph, a contradiction.

(ii). Suppose $V_s X \cap V_s Y \neq \emptyset$. Then $[X], [Y] \neq H_2$. Let u be a slim vertex in $V_s X \cap V_s Y$. Then, since u is adjacent to the unique fat vertex of X and the unique fat vertex of Y , X contains a subgraph isomorphic to F_6 in Figure 3 by Definition 1.2-(v), i.e., $F_6 \in \mathcal{H}$. But this contradicts. Hence $V_f X \cap V_f Y \neq \emptyset$.

If $[X] = H_2$ and $[Y] = H_3$, then there exists a slim vertex z in Y different from y . Since z is a slim vertex in the unique \mathcal{H} -strict cover graph of $\Gamma - y$ and $z \notin V_s X$, $x \sim z$ in Γ by $V_f X \cap V_f Y \neq \emptyset$. Hence Z is isomorphic to F_5 in Figure 3, i.e., Z contains a subgraph isomorphic to F_6 . In other cases, by using a similar technique, we can show that Z contains

a subgraph isomorphic to F_1, F_2, F_3 or F_6 in Figure 3. But the fact is that Z contains no subgraph isomorphic to F_1, F_2, F_3 or F_6 . This result is proved as follows.

Now all subgraphs of Γ are not isomorphic to every graph in \mathcal{F} . Let $S = \{P \in A_x \cap A_y \mid V_f P \cap V_f Z \neq \emptyset\}$. Clearly $S \neq \emptyset$ since $\#V\Gamma > 9$. Let $H' = G(A_x \cap A_y)$, and let $H = Z \cup H'$.

Case 1: $F_1 \not\subset Z$. Suppose $F_1 \subset Z$. If there exists an element $P \in S$ such that $[P] \in \{H_3, H_5\}$, then Γ contains a subgraph isomorphic to the complete bipartite graph $K_{3,2}$. Now $\lambda_{\min}(\Gamma) \leq \lambda_{\min}(K_{3,2}) < -1 - \sqrt{2}$. But this contradicts the hypothesis. Hence $[P] = H_2$ for all $P \in S$.

In the next place, suppose $\#S \geq 3$. Then $G_{6,22} \subset \Gamma$, a contradiction. Hence $0 < \#S \leq 2$.

(i). Suppose $\#S = 1$. Let P be the unique element of S . Since $\#V\Gamma > 9$, $(A_x \cap A_y) \setminus S \neq \emptyset$. Hence there exists an element Q of $(A_x \cap A_y) \setminus S$ such that $V_f Q \cap V_f P \neq \emptyset$. Since $G_{6,28} \not\subset \Gamma$, $[Q] = H_2$. Since $G_{6,26} \not\subset \Gamma$, $\{R \in (A_x \cap A_y) \setminus S \mid V_f R \cap V_f Q \neq \emptyset, V_f R \cap V_f P = \emptyset\} = \emptyset$. Now $\#V_s W = 1$ for all $W \in A_x \cap A_y$, $\#V_s Z \leq 6$, and $\#V\Gamma > 9$. Hence $\#\{Q \in (A_x \cap A_y) \setminus S \mid V_f A \cap V_f P \neq \emptyset\} \geq 3$. Thus $G_{7,3} \subset \Gamma$, a contradiction.

(ii). Suppose $\#S = 2$. Since $\#V\Gamma > 9$, there exists an element P of $(A_x \cap A_y) \setminus S$ such that $V_f G(S) \cap V_f P \neq \emptyset$. Then $G_{6,14}$ or $G_{6,19} \subset \Gamma$, a contradiction.

Case 2: $F_2 \not\subset Z$. Suppose $F_2 \subset Z$. If there exists an element $P \in S$ such that $[P] \in \{H_3, H_5\}$, then $G_{6,6} \subset \Gamma$. But this contradicts the hypothesis. Hence $[P] = H_2$ for all $P \in S$. If $\#S \geq 2$, then $G_{6,1} \subset \Gamma$. But this contradicts the hypothesis. Hence $\#S = 1$. Then $(A_x \cap A_y) \setminus S \neq \emptyset$ since $\#V\Gamma > 9$. Then $G_{6,16} \subset \Gamma$, a contradiction.

Case 3: $F_3 \not\subset Z$. Suppose $F_3 \subset Z$. Then $\#V_s Z = 2$ since $[X] = [Y] = H_2$. In the next place, suppose that there exists a fat vertex $f \in V_f Z$ such that $f \notin V_f G(A_x \cap A_y)$. Then, since $N_H^f(f) = \{x, y\}$ and $[Z - f] = H_3$, $H - f$ is the \mathcal{H} -strict cover graph of Γ , a contradiction. Hence $V_f Z \subset V_f G(A_x \cap A_y)$.

Since $K_{3,2} \not\subset \Gamma$, all graph in S are isomorphic to H_2 .

Suppose $(A_x \cap A_y) \setminus S \neq \emptyset$. Then $G_{5,1} \subset \Gamma$, a contradiction. Hence $A_x \cap A_y = S$.

Since $G_{6,21} \not\subset \Gamma$, $\#\{P \in S \mid f \in V_f P\} \leq 2$ for any $f \in V_f Z$. Hence $\#S \leq 4$, and therefore

$$\begin{aligned} \#V\Gamma &= \#V_s H &&= \#V_s Z + \#V_s G(A_x \cap A_y) \\ &= 2 + \#(A_x \cap A_y) &&= 2 + \#S < 7. \end{aligned}$$

But this contradicts the hypothesis.

Case 4: $F_6 \not\subset Z$. Suppose $F_6 \subset Z$. Without loss of generality, we can suppose that $[X] = H_2$. Let F be the subgraph of Z induced by X and the slim vertex y . Note that $[F] = [F_6]$. Let f be the fat vertex of F satisfying $y \sim f$, and let g be the fat vertex of F different from f . Then, since $f, g \in V_f X$ and $\Gamma - y$ is a connected graph, either f or g is a fat vertex in H' .

(i). Suppose that $f \notin V_f H'$ and $g \in V_f H'$. Then $Z - f$ is an $\{H_1\}$ -line graph. Hence $H - f$ is an \mathcal{H} -line graph of Γ from Lemma 2.2, a contradiction.

(ii). Suppose that $f, g \in V_f H'$. Then no graph in S contains both the fat vertices f and g by Definition 1.2-(ii). Let $S^f = \{P \in A_x \cap A_y \mid f \in V_f P\}$, and let $S^g = \{P \in A_x \cap A_y \mid g \in V_f P\}$. Note that $S^f \neq \emptyset$ and $S^g \neq \emptyset$. Since $G_{5,1} \not\subset \Gamma$, all elements of S^f are isomorphic to H_2 . Further we obtain the following results:

$$(7) \quad \#((V_f G(S^f) \setminus \{f\}) \setminus V_f G(S^g)) \leq 2.$$

Proof of (7). Suppose that $\#((V_f G(S^f) \setminus \{f\}) \setminus V_f G(S^g)) \geq 3$. Then $G_{6,9} \subset \Gamma$, a contradiction. ■

Suppose $V_f G(S^f) \cap V_f G(S^g) \neq \emptyset$. Then, since $G_{6,12} \not\subset \Gamma$, all elements of S^g are isomorphic

to H_2 , i.e., all elements of S are isomorphic to H_2 .

Further suppose $(V_f G(S^f) \setminus \{f\}) \setminus V_f G(S^g) \neq \emptyset$. Then, since $G_{6,5} \not\subset \Gamma$, $\#S^g = 1$, i.e., $[G(S^g)] = H_2$. If $\#((V_f G(S^f) \setminus \{f\}) \setminus V_f G(S^g)) = 2$ (i.e., $\#S^f = 3$), then $G_{6,7} \subset \Gamma$, a contradiction. Hence $\#((V_f G(S^f) \setminus \{f\}) \setminus V_f G(S^g)) = 1$, i.e., $\#S^f = 2$.

Now $\#V_3 Z \leq 4$, $\#V_3 G(S) = 3$. Hence $(A_x \cap A_y) \setminus S \neq \emptyset$. Thus $G_{5,1}$, $G_{6,13}$ or $G_{6,24} \subset \Gamma$, a contradiction. By the above discussion, $(V_f G(S^f) \setminus \{f\}) \setminus V_f G(S^g) = \emptyset$.

If $\#S^g \geq 3$, then $G_{6,11} \subset \Gamma$, a contradiction. Hence $\#V_3(Z \cup G(S)) = 4 + \#V_3 G(S^g) + \#V_3 G(S^f) \leq 4 + 2 \cdot \#V_3 G(S^g) \leq 8$. Hence $(A_x \cap A_y) \setminus S \neq \emptyset$. Now suppose $\#S^g = 2$. Then $G_{5,1}$, $G_{6,23}$ or $G_{6,24} \subset \Gamma$, a contradiction. Hence $\#S^g = \#S^f = 1$.

Let $R = \{P \in (A_x \cap A_y) \setminus S \mid V_f P \cap V_f G(S) \neq \emptyset\}$. Now $[P] = H_2$ for all $P \in R$ since $G_{6,19} \not\subset \Gamma$. Further $\#R \leq 2$ since $G_{7,6} \not\subset \Gamma$. Hence, since $\#V_3(Z \cup G(S \cup R)) \leq 4 + 2 + 2 = 8$, $(A_x \cap A_y) \setminus (S \cup R) \neq \emptyset$. Thus $G_{6,25} \subset \Gamma$, a contradiction. By the above discussion, $V_f G(S^g) \cap V_f G(S^f) = \emptyset$.

Let $R_0^f = \{P \in (A_x \cap A_y) \setminus S \mid V_f P \cap V_f G(S^f) \neq \emptyset\}$. Since $\Gamma - x$ is connected, $R_0^f \neq \emptyset$. $V_f G(R_0^f) \cap V_f G(S^g) = \emptyset$ from $G_{5,1} \not\subset \Gamma$.

Let $R_1^f = \{P \in (A_x \cap A_y) \setminus (S \cup R_0^f) \mid V_f P \cap V_f G(R_0^f) \neq \emptyset\}$. If $V_f G(S^g) \cap V_f G(R_1^f) \neq \emptyset$, then $G_{6,17} \subset \Gamma$, a contradiction. If $V_f G(S^g) \cap V_f G(R_1^f) = \emptyset$ and $R_1^f \neq \emptyset$, then $G_{6,27} \subset \Gamma$ a contradiction. Hence $R_1^f = \emptyset$. But this contradicts the hypothesis that $\Gamma - x$ is connected.

(iii). Suppose that $f \in V_f H'$ and $g \notin V_f H'$. Now $[Z - g] = F_2, F_6, F_7$ or H_5 . If $[Z - g] = H_5$, then $H - g$ is an \mathcal{H} -strict cover graph of Γ , and the conclusion implies that $H - g$ is an \mathcal{H} -line graph, a contradiction. Further, by the conclusion of Case 2, $[Z - g] \neq F_2$.

Suppose $[Z - g] = F_6$. If the fat vertex of $Z - g$ different from f belongs to H' , then this case is the same discussion of Case 4-(ii). If the fat vertex g' of $Z - g$ different from f does not belong to H' , then $H - gg'$ is isomorphic to H_3 , and is an \mathcal{H} -line graph of Γ by Lemma 2.2. Hence $[Z - g] = F_7$.

Since $G_{6,21} \not\subset \Gamma$, all elements of S are isomorphic to H_2 . Since $G_{7,7} \not\subset \Gamma$, $0 < \#S \leq 2$.

Suppose $\#S = 1$. Let P_0 be the unique graph of S , and let f_1 be the fat vertex of P_0 different from f . Further let $S^{f_1} = \{P \in (A_x \cap A_y) \setminus S \mid f_1 \in V_f P\}$.

If $V_f G(S^{f_1}) \cap V_f G((A_x \cap A_y) \setminus (S \cup S^{f_1})) \neq \emptyset$, then $G_{7,4} \subset \Gamma$, a contradiction. Since $G_{7,3} \not\subset \Gamma$, all elements of S^{f_1} are isomorphic to H_2 . Now $\#S^{f_1} > 4$ since $\#V\Gamma > 9$, and the conclusion implies $G_{8,1} \subset \Gamma$, a contradiction. Hence $\#S = 2$.

Let $S' = \{P \in (A_x \cap A_y) \setminus S \mid V_f P \cap V_f G(S) \neq \emptyset\}$. Since $\#V\Gamma > 9$, $S' \neq \emptyset$. Hence $G_{7,5}$ or $G_{7,6} \subset \Gamma$, a contradiction.

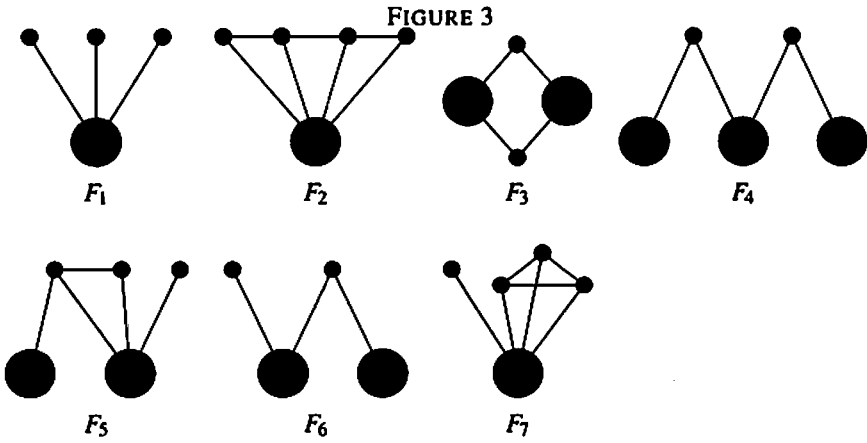
By the above discussion, we have completed the proof of Theorem. ■

From Proposition 5.8 and Proposition 4.7, we obtain the following result as the main theorem.

Theorem 5.9. *Let Γ be a minimal non \mathcal{H} -line graph without fat vertices. Then $[\Gamma] \in \mathcal{F}$ if $\lambda_{\min}(\Gamma) \geq -1 - \sqrt{2}$.*

REFERENCES

- [1] P. Cameron, J. M. Goethals, J. J. Seidel, and E. E. Shult, Line graphs, root systems and elliptic geometry, *J. Algebra* 43:305-327(1976).
- [2] R. Woo and A. Neumaier, On graphs whose smallest eigenvalue is at least $-1 - \sqrt{2}$, *Linear Algebra Appl.* 226-228:577-591(1995).



- [3] A. J. Hoffman, On graphs whose least eigenvalue exceeds $-1 - \sqrt{2}$, *Linear Algebra Appl.* 16:153-165(1977).
 [4] D. Cvetković, Generalized line graphs, *J. Graph Theory.* 5:385-399(1981).
 [5] D. Cvetković, P. Rowlinson, S. K. Simić, Constructions of the maximal exceptional graphs with largest degree 28, Department of Computing Science and Mathematics, University of Stirling, Scotland, Technical Report CSM-156, Stirling, 2000.
 [6] D. Cvetković, M. Lepović, P. Rowlinson and S. K. Simić, The maximal exceptional graphs, to appear.
 [7] L. Lovász, *Combinatorial problems and exercises*, North-Holland, 1979

(T. Taniguchi) GRADUATE SCHOOL OF MATHEMATICS, KYUSHU UNIVERSITY, FUKUOKA 812-81, JAPAN
E-mail address: tetsuzit@math.kyushu-u.ac.jp

Minimal Direct Summands

TAKASHI OKUYAMA

Oita University

1. INTRODUCTION

All groups considered are abelian groups. Throughout this article, P denotes the set of primes, N the set of all positive integers, and p a prime integer.

We pose the following problem.

Problem. For which subgroup A of a group G , is there a minimal direct summand containing A ?

Next we give several definitions.

Definition 1.1. Let G be a group. The subgroup

$$G[p] = \{g \in G \mid pg = 0\}$$

is called the p -socle of G .

Definition 1.2. A subgroup A of a group G is said to be almost-dense in G if, for all integers $n \geq 0$ and all $p \in P$,

$$p^n G[p] \subseteq A + p^{n+1} G.$$

Definition 1.3. A subgroup A of a group G is said to be pure in G if, for all $n \in N$,

$$A \cap nG = nA.$$

Definition 1.4. A subgroup A of a group G is said to be purifiable in G if, among the pure subgroups of G containing A , there exists a minimal one. Such a minimal pure subgroup is called a pure hull of A .

Not all subgroups are purifiable in given groups. T. Koyama gave a good example in [3, Remark, p.93]. The following result is useful.

Proposition 1.5. *Let A be a subgroup of a group G . Suppose that A is purifiable in G . Then the pure subgroup H of G containing A is a pure hull of A in G if and only if the following three conditions are satisfied:*

- (1) A is almost-dense in H ;
- (2) H/A is torsion;
- (3) for every $p \in \mathbf{P}$, there exists a nonnegative integer m_p such that

$$p^{m_p} H[p] \subseteq A.$$

Proposition 1.6. *Let G be a group and A a subgroup of G . Suppose that H is a minimal direct summand of G containing A . Then A is almost-dense in H .*

Note that direct summands are pure. Hence the subgroup H as in Proposition 1.6 is pure in G and A is almost-dense in H . If G is torsion, then H/A is torsion. Hence H satisfies the above conditions (1) and (2).

Now we give definition of quasi-purifiable subgroups.

Definition 1.7. *A subgroup A of a group G is said to be quasi-purifiable in G if there exists a pure subgroup H of G containing A such that*

- (1) A is almost-dense in H and
- (2) H/A is torsion.

Such a subgroup H is called a quasi-pure hull of A in G .

To solve the problem, we need to study quasi-purifiable subgroups. It is easy to see that purifiable subgroups are quasi-purifiable.

2. MAXIMAL QUASI-PURE HULLS

Lemma 2.1. *Let G be a group and A a subgroup of G . Suppose that A is quasi-purifiable in G . Then there exists a maximal quasi-pure hull of A in G .*

Example 2.2. *Let G be an unbounded p -group. Then there exists a proper basic subgroup B of G . Let $A = B[p]$. Then A is purifiable in G , B is a pure hull of A in G , and G is a quasi-pure hull of A in G . Hence B is not a maximal quasi-pure hull of A in G .*

In fact, the basic subgroup B is pure in G and $B[p]$ is almost-dense in G .

In general, by Example 2.2, pure hulls of purifiable subgroups are not necessarily maximal quasi-pure hulls of given subgroups. However, pure hulls of purifiable torsion-free subgroups A of groups G are maximal quasi-pure hulls of A in G as follows.

Theorem 2.3. *Let G be a group and A a torsion-free subgroup of G . If A is purifiable in G , then pure hulls of A in G are maximal quasi-pure hulls of A .*

3. QUASI-PURIFIABILITY

First, we give a basic property.

Proposition 3.1. *The set T of all elements of finite order in a group G is a subgroup of G . T is a torsion group and the quotient group G/T is torsion-free. Hence T is the maximal torsion subgroup of G . Moreover,*

$$T = \bigoplus_{p \in \mathbf{P}} G_p$$

where G_p is the maximal p -primary subgroup of G .

In general, if X is a group, $T(X)$ denotes the maximal torsion subgroup of X .

Definition 3.2. *A group G is said to be torsion-complete if G is the maximal torsion subgroup of a direct product of cyclic groups.*

We have an important property for torsion-complete groups as follows.

Proposition 3.3. *Let X be a torsion group and G a subgroup of X . If G is torsion-complete, then G is a direct summand of X .*

We used the previous Proposition to prove the following theorem.

Theorem 3.4. *Let G be a group whose maximal torsion subgroup is torsion-complete. Then the followings hold.*

- (1) *All subgroups of G are quasi-purifiable in G*
- (2) *Let A be a subgroup and $M/A = T(G/A)$. Then there exists a subgroup N of $T(G)$ such that $M = H \oplus N$ for every maximal quasi-pure hull H of A in G .*
- (3) *All maximal quasi-pure hulls of A are isomorphic and for all maximal quasi-pure hull H of A , the groups H/A are isomorphic.*

Corollary 3.5. *Let G be a group whose maximal torsion subgroup is torsion-complete and A a subgroup of G . Suppose that G/A is torsion. Then all maximal quasi-pure hulls of A in G are minimal direct summands of G containing A .*

4. APPLICATIONS

As an application of Theorem 3.4 for torsion groups, we have the following corollary.

Corollary 4.1. *Let G be a torsion-complete group and A any subgroup of G . Then the followings hold.*

- (1) A is quasi-purifiable in G .
- (2) For every subgroup A of G , there exists a minimal direct summand H of G containing A and the summand H is also a minimal pure torsion-complete subgroup of G containing A .
- (3) All minimal pure torsion-complete subgroups of G containing A are isomorphic and for all minimal pure torsion-complete subgroups H of G containing A , the groups H/A are isomorphic.

Before giving an application of Theorem 3.4 for mixed groups, we give the following definitions and basic properties. From now on, let $T = T(G)$.

Definition 4.2. *A subgroup A of a group G is said to be p -neat in G if*

$$A \cap pG = pA.$$

If A is p -neat in G for every $p \in \mathbf{P}$, then A is called neat in G .

Definition 4.3. *Let N be a subgroup of a group G . Then a subgroup A of G is said to be N -high in G if A is maximal with respect to the property of being disjoint from N .*

The existence of N -high subgroups is guaranteed by Zorn's lemma. We studied N -high subgroups in [2] and [1]. Summarizing them, we give the following characterization of N -high subgroups.

Proposition 4.4. *Let N be a subgroup of a group G . Then a subgroup A of G is N -high in G if and only if*

- (1) $A \cap N = 0$,
- (2) A is neat in G ,
- (3) $G[p] = A[p] \oplus N[p]$ for every $p \in \mathbf{P}$, and
- (4) $G/(A \oplus N)$ is torsion.

Corollary 4.5. *A torsion-free subgroup A of a group G is T -high in G if and only if*

- (1) A is neat in G and
- (2) G/A is torsion.

Definition 4.6. *A group G is said to be an ADE group if there exists a torsion-free subgroup A that is almost-dense and T -high in G . Such a subgroup A is called a moho subgroup of G .*

We already studied ADE groups of torsion-free rank 1 in [5] and [6].

Definition 4.7. A group G is said to be an ADE decomposable group if there exists an ADE subgroup H of G and a subgroup T' of T such that $G = H \oplus T'$.

Corollary 4.8. Let G be a group whose maximal torsion subgroup is torsion-complete. Then G is an ADE decomposable group.

Proof. Let N be a T -high subgroup of G . Then, Corollary 4.5(3), G/N is torsion. Let H be a maximal quasi-pure hull of N in G . By Corollary 3.5, N is a direct summand of G , i.e. $G = H \oplus K$ for some subgroup K of T . By Definition 1.7, N is almost-dense in H . Hence H is an ADE group with N as a moho subgroup and so G is an ADE decomposable group. \square

By Corollary 4.8, we have the following.

Corollary 4.9. Let G be a direct product G of cyclic groups. Then G is an ADE decomposable group.

REFERENCES

- [1] K. Benabdallah and J. Irwin. On N -High Subgroups of Abelian Groups, *Bull. Soc. Math. France*, 96:337–346, 1968.
- [2] J. Irwin and E. A. Walker. On N -High Subgroups of Abelian Groups, *Pacific J. Math.*, 11(4):1363–1374, 1961.
- [3] T. Koyama. On Quasi-Closed Groups and Torsion complete Groups, *Bull Soc. Math. France*, 95:89–94, 1967.
- [4] T. Okuyama On isomorphism of minimal direct summands, *Hokkaido Math. J.*, 23(2):229–240, 1994.
- [5] T. Okuyama. On Almost-Dense Extension Groups of Torsion-Free Groups, *J. Algebra*, 202:202–228, 1998.
- [6] T. Okuyama. Quasi-purifiable Subgroups and Height-matrices,, *Rocky Mountain J. Math.*, 32(4):1577–1595, 2002.

局所有限トポス上の Burnside 環の ベキ等元公式

The idempotent formula of the Burnside ring of a locally finite topos

吉田知行 (Tomoyuki YOSHIDA, 北大)

2004/06/30 09:30-10:30

1 はじめに

目標は「離散数学のカテゴリー化」である。カテゴリーというと抽象的で取っつきにくい感じがするが、必要なのはカテゴリーの考え方であって、カテゴリー論はそれほど必要としない。離散数学に限らず、すべての数学は集合と写像の概念を使って書いてあるとはよく言うが、それに対して、集合を第一線に出さず、集合の間の写像(つまり矢印)ですべてを書いてやろうというのがまずやるべき仕事である。集合を使っても良いが、元を表す記号 \in を使ってはいけない。カテゴリー論的に見ると、組合せ論は \mathbf{Set}_f (有限集合と写像のカテゴリー) の理論であり、有限群論は \mathbf{Grp} (有限群と準同型写像のカテゴリー) の理論、さらに有限群の表現論は \mathbf{Mod}_{kG} (有限群 G に対する kG -加群と kG -準同型写像のカテゴリー) の理論、あるいはいろいろな有限群 G に対するそのような \mathbf{Mod}_{kG} 達のなす高次元カテゴリーの理論と考えられる。

離散数学のカテゴリー化を考える上で問題になるのが、有限集合のカテゴリー \mathbf{Set}_f の代わりである。今のところ最適なのは局所有限トポスという種類のカテゴリーである。我々は局所有限トポスをひとつ固定し、そこで離散数学を構成したい。

例. グラフの概念を矢印で書いてみる.

(1) もっとも一般的なグラフ (各辺には向きがあり, 多重辺やループを許す) は, 写像の対 $\alpha, \beta: E \rightarrow V$ と同一視できる. $\alpha(e), \beta(e)$ は辺 e の始点と終点を表す. この表し方はグラフ理論できわめてよく使われる. グラフの準同型 $(f, g): (E_1 \rightarrow V_1) \rightarrow (E_2 \rightarrow V_2)$ は, 写像 $f: E_1 \rightarrow E_2$ と $g: V_1 \rightarrow V_2$ の対で, α, β と可換なものである. このようなグラフのカテゴリリーは局所有限トポスになっている.

(2) 単純グラフの概念を矢印で書くのはやっかいである. 普通は, 頂点集合 V と, その2点部分集合族 (V_2) の部分集合の対 (V, E) を単純グラフと定義するしかし, 2点集合の概念をカテゴリリー論的に定義するのは困難なので, この方法では単純グラフの良い定義はできない.

(3) 無向グラフの辺 $\{u, v\}$ をふたつの有効辺 $u \rightarrow v, v \rightarrow u$ の対と考えれば, 無向グラフも有効グラフとなる. すなわち, involution $\tau: E \rightarrow E$ があって, $\beta = \alpha \circ \tau$ であるような有向グラフ $\alpha, \beta: E \rightarrow V$ を無向グラフ定義すればよい. ループがないこと (すなわち $\alpha(e) \neq \beta(e)$) は, α と β のファイバー積が空集合であるとして定義できる. 多重辺がないことは, $\langle \alpha, \beta \rangle: E \rightarrow V \times V; e \rightarrow (\alpha(e), \beta(e))$ が単射であるとして定義できる. 連結性は, 直和分解ができないとして定義できる. 写像が単射であることや直和やファイバー積は, 「集合の元」の概念を使わずに完全に矢印だけで記述できる. これで単純グラフのカテゴリリー論的定義ができた. しかし単純グラフのカテゴリリーはトポスではない.

(4) 木とは, サイクルのない単純グラフのことである. 根付き木とは, 根と呼ばれる特別な頂点を指定した木である. 根付き森とは, 根付き木の disjoint union のことである. 高さ $\leq h$ の根付き森は, 写像の列 $F_h \rightarrow F_{h-1} \rightarrow \dots \rightarrow F_1 \rightarrow F_0$ と同一視できる. ここで F_k がレベル k の頂点の集合で, とくに F_0 が根の集合である. 与えられた高さ以下の根付き森のカテゴリリーは局所有限トポスになる.

例. ファンクターと絡めた方が実用的に便利なこともある. ブロックデザインの矢印化は, 次のようにしてなされる. 局所有限トポス \mathcal{E} と忠実なファンクター $\Phi: \mathcal{E} \rightarrow \mathbf{Set}_f$ を用意する. Φ によって同型射に移る射はもともと同型射であると仮定する. このとき \mathcal{E} におけるブロックデザイン $X \leftarrow F \rightarrow B$ とは, Φ によって \mathbf{Set}_f に飛ばしたとき普通のブロックデザインになるものとして定義する.

2 良いカテゴリーと悪いカテゴリー

離散数学に関係していろいろなカテゴリーが登場する。その中にカテゴリー論的に良いカテゴリーと悪いカテゴリーがある。良いカテゴリーとはたくさんの operator を持つカテゴリーである。基本的に、良いカテゴリーはふたつしかない。

- ・トポス，すなわち集合のカテゴリー **Set** とその一般化
- ・アーベルカテゴリー，すなわちアーベル群のカテゴリーとその一般化

これに対して，次のようなカテゴリーは悪いカテゴリーである。

・群 G . 対象はひとつ $*$ だけで， $\text{Hom}(*, *) = G$ ，合成は群の積。これでもカテゴリーになるが，operator はきわめて貧弱である。群が自明な場合を除けば直和も直積もない。同様に半群もカテゴリーと見なせるが，これはもっと悪いカテゴリーである。

・順序集合 P . 対象は P の元。ふたつの対象の間の射は高々ひとつ。 $x \rightarrow y$ が存在するのは $x \leq y$ のときに限る。

・ **Grp**. 対象は群，射は群準同型写像。このカテゴリーはあまり良くないこのカテゴリーは，直和 (自由積)，ファイバー和 (融合積)，始対象と終対象 (自明な群)，直積 (cartesian product)，ファイバー積，射の全単射分解，射の核や余等化の存在，準同型定理，生成素 (無限巡回群) などたくさんの良い性質を持つ。ただし有限群のカテゴリーは直和，ファイバー和を持たない。有限群のカテゴリーよりは，有限亜群 (有限群の直和集合) のカテゴリーの方が良い。後者はカテゴリー論的直和を持つ。

悪いカテゴリー \mathcal{C} を調べるにはどうすればよいのかというと，集合のカテゴリーや加群のカテゴリーへの (共変または反変) ファンクターカテゴリー $[\mathcal{C}, \text{Set}]$, $[\mathcal{C}, \text{Mod}_k]$ (さらには適当な Grothendieck トポロジーに対する層のカテゴリー) を考える。前者はトポスになり，後者はアーベルカテゴリーになる。群論的にみると，前者はカテゴリーの置換表現であり，後者は線形表現である。有限群のカテゴリーからの反変ファンクターカテゴリー $[\text{Grp}_f^{\text{op}}, \text{Set}_f]$, $[\text{Grp}_f^{\text{op}}, \text{Mod}_k]$ は研究の価値が十分あると思う。

カテゴリーを学ぶ人のための格言？

- ・良い猫 (cat) とはお金持ちの猫である。
- ・良い猫は基本的に二匹しかいない。白い猫と黒い猫である。
- ・悪い猫も表現すれば良い猫になる。

3 局所有限トポス

次の条件を満たすカテゴリー \mathcal{E} をトポスという：

(T1) 有限極限を持つ。したがって、直積 $X \times Y$ 、終対象 1 、ファイバー積 $X \times_Z Y$ などを持つ。

(T1') 有限余極限を持つ。したがって、直和 $X + Y$ 、始対象 \emptyset などを持つ。

(T2) ベキ Y^X を持つ。 $(-)^X$ は $X \times (-) : \mathcal{E} \rightarrow \mathcal{E}$ の右随伴である：

$$\text{Hom}(X \times Y, Z) \cong \text{Hom}(X, Z^Y).$$

(T3) 部分対象分類子 $t : 1 \rightarrow \Omega$ を持つ：

$$\text{Sub}(X) \longleftrightarrow \text{Hom}(X, \Omega); A \longmapsto \chi_A$$

たとえば、 Set はトポスである。ベキ Y^X は、 X から Y への写像全体の集合である。 Ω は 2 点集合 $\{0, 1\}$ である。 χ_A は部分集合の特性写像である。

局所有限トポスとは各 Hom-set $\text{Hom}(X, Y)$ が有限集合であるようなトポスのことをいう。

例. (1) Set_f : 有限集合のカテゴリー

$Y^X = \text{Map}(X, Y)$, $\Omega = \{0, 1\}$, $t : * (\in 1) \mapsto 1$.

(2) Set_f^G (G 群) : 有限 G -集合と G -写像のカテゴリー

Y^X, Ω は有限集合の場合と同様。

(3) Set_f^S (S 有限半群) : 有限 S -集合と S -写像のカテゴリー

$Y^X = \text{Map}_S(S \times X, Y)$, $\Omega = \{I \subseteq S \mid IS = I\}$ (右イデアルの集合)

(4) $\mathbf{RForest}_{\leq h}$: 高さ $\leq h$ の根付き森のカテゴリー

(注意：高さ h の根付き森は、長さ h の全順序集合から Set_f へのファンクター)

(5) Surj : 全射 $X \rightarrow Y$ と可換図式のカテゴリー

対象は $(X \rightarrow X')$, 射 $(f, f') : (X \rightarrow X') \rightarrow (Y \rightarrow Y')$ は写像の対で可換図式を作るもの。 Ω は 2 点集合から 1 点集合への自明な全射

これらの局所有限カテゴリーは、有限集合のカテゴリー Set_f に比べていくつかの違いがある。集合論的かつ論理的な取り扱いの困難さや易しさを示している。 G は自明でない有限または無限群、 S は群でない有限半群とする。

・ Set_f^G : 選択公理が成り立たない (全射 $X \rightarrow Y$ が分裂しない)。

- $\text{Set}_f^G, \text{Set}_f^S$: 連結対象の直積が必ずしも連結でない.
- $\text{RForest}_{\leq h}, \text{Surj}$: 連結対象の直積は連結.
- Set_f^G : 部分群束 $\text{Sub}(X)$ はブール代数.
- Set_f^S : 部分群束 $\text{Sub}(X)$ がブール代数でない.
- $\text{Set}_f^S : \Omega = \{S \text{ の左イデアル} \}$ は 2 点集合でない.
- $\text{Set}_f^G (G \text{ 無限群}), \text{Set}_f^S$: 直既約対象は無数個ある.

これに対して, 有限集合のカテゴリー Set_f は選択公理を満たし, 連結対象は 1 点集合だけでありしたがって連結対象の直積は連結, 連結対象の部分対象はふたつ (空集合と全体) しかない, 部分群束 $\text{Sub}(X)$ はブール代数である.

4 局所有限トポスのバーンサイド環

以下 \mathcal{E} を局所有限トポスとする. $\text{Con}(\mathcal{E})$ を \mathcal{E} の連結 (すなわち直既約) な対象のなす部分カテゴリーとする. $B^+(\mathcal{E}) := \mathcal{E}/\cong$ (\mathcal{E} の対象の同型類の集合) と置く. 対象 $X \in \mathcal{E}$ の同型類を $[X]$ と書く.

命題. (1) $B^+(\mathcal{E})$ は可換半環である. 和と積は直和と直積による:

$$[X] + [Y] := [X + Y], [X] \cdot [Y] := [X \times Y].$$

(2) $\text{Con}(\mathcal{E})/\cong$ (連結な対象の同型類の集合) を生成系とする自由可換半群である.

(1) は直和と直積に関する分配法則を意味する. (2) は Krull-Schmidt 型の一意的直既約分解定理を意味する.

局所有限トポスのバーンサイド環を, 半環 $B^+(\mathcal{E})$ の Grothendieck construction として定義する. したがって, $B(\mathcal{E})$ は $[X] - [Y]$ ($X, Y \in \mathcal{E}$) の形の記号からなり, 関係式

$$(i) [X] = [X'] \text{ if } X \cong X'$$

$$(ii) [X + Y] = [X] + [Y]$$

$$(iii) [X] \cdot [Y] = [X \times Y]$$

で定義される半環である.

5 バーンサイド環の基本定理

$I \in \text{Con}(\mathcal{E})$ なら

$$\begin{aligned}\text{Hom}(I, X + Y) &\cong \text{Hom}(I, X) + \text{Hom}(I, Y), \\ \text{Hom}(I, X \times Y) &\cong \text{Hom}(I, X) \times \text{Hom}(I, Y)\end{aligned}$$

である。したがって $[X] \mapsto |\text{Hom}(I, X)|$ は環準同型

$$\varphi_I : \mathbf{B}(\mathcal{E}) \longrightarrow \mathbf{Z}; [X] \mapsto |\text{Hom}(I, X)|$$

に拡張できる。これを束ねて、バーンサイド環準同型写像

$$\varphi := (\varphi_I) : \mathbf{B}(\mathcal{E}) \mapsto \tilde{\mathbf{B}}(\mathcal{E}) := \prod_I \mathbf{Z}$$

を得る。

命題. φ は単射環準同型写像である。

系. 局所有限トポスにおいて $X \cong Y$ であるための必要十分条件は、各連結対象 I に対して $|\text{Hom}(I, X)| = |\text{Hom}(I, Y)|$ が成り立つことである。

この系は、局所有限な一意的 epi-mono 分解カテゴリーで成り立つ。またこの系は米田の補題

$$X \cong Y \iff \text{Hom}(-, X) \cong |\text{Hom}(I, Y) : \mathcal{E}^{\text{op}} \rightarrow \text{Set}$$

の拡張である。

有限群のバーンサイド環の場合は、次の基本完全系列がある：

$$0 \longrightarrow \mathbf{B}(G) \xrightarrow{\varphi} \tilde{\mathbf{B}}(G) \xrightarrow{\psi} \text{Obs}(G) \longrightarrow 0.$$

ここで

$$\tilde{\mathbf{B}}(G) := \prod_{(H)} \mathbf{Z}, \quad \text{Obs}(G) := \prod_{(H)} (\mathbf{Z}/|WH|\mathbf{Z}), \quad WH := N_G(H)/H$$

$$\varphi = (\varphi_H), \quad \varphi_H([X]) = |X^H| \quad (X^H \text{ は } H\text{-固定点の集合})$$

$$\psi = (\psi_H), \quad \psi_H(\chi) = \sum_{gH \in WH} \chi(\langle g \rangle H) \bmod |WH|.$$

重要なのは ψ が具体的に表せることである。残念ながら、一般の局所有限トポスは連結対象の同型類が無数個あるためにそのままでうまく行

かない。基本完全系列を得るための対策はいくつか考えられる。それはバーンサイド環の定義を次のようなものに変えることである。

- (1) $\mathcal{I} \subseteq \text{Con}(\mathcal{E})$ に関する相対 Burnside 環 $B(\mathcal{E}, \mathcal{I})$.
- (2) $\mathcal{I} \subseteq \text{Con}(\mathcal{E})$ に関する部分 Burnside 環 $B(\mathcal{I})$.
- (3) 完備 Burnside 環 $\widehat{B}(\mathcal{E})$.
- (4) Hom を全射に制限した Burnside 環 $B(\mathcal{E}_{\text{epi}})$.
- (5) 有限個の既約対象の同型類 $\text{Irr}(\mathcal{E})/\cong$ を持つ場合は, G_0 環 $B(\mathcal{E}, \text{Irr})$.

ここではもっとも簡単な (1) の有限部分カテゴリー $\mathcal{I} \subseteq \text{Con}(\mathcal{E})$ に関する相対 Burnside 環 $B(\mathcal{E}, \mathcal{I})$ を考える。簡単のため, \mathcal{I} は $\text{Con}(\mathcal{E})$ の skeletal な有限充満部分カテゴリーとする。skeletal とは, $I \cong J \in \mathcal{I}$ なら $I = J$ を満たすことを意味する。さらに \mathcal{I} は全射像に関して閉じたものとする。すなわち $\mathcal{I} \ni I \rightarrow J \in \mathcal{E}$ なら, $J \in \mathcal{I}$ 。

相対バーンサイド環 $B(\mathcal{E}, \mathcal{I})$ を, 環準同型

$$\varphi' : B(\mathcal{E}) \xrightarrow{\varphi} \prod_C Z \xrightarrow{\text{pr}} \prod_{I \in \mathcal{I}} Z$$

(ここで C は $\text{Con}(\mathcal{E})/\cong$ 上を動く) を使って, $B(\mathcal{E}, \mathcal{I}) := B(\mathcal{E})/\text{Ker}(\varphi')$ として定義する。 $B(\mathcal{E}, \mathcal{I})$ は加群としては, \mathcal{I} 上の自由加群 $B(\mathcal{I}) := Z[\mathcal{I}]$ に同型で, $B(\mathcal{I})$ を環と考えるなら次のように具体的基本完全系列が構成できる。

$$B(\mathcal{I}) := Z[\mathcal{I}] := \left\{ \sum_{I \in \mathcal{I}} a_I [I] \mid a_I \in Z \right\} \subseteq B(\mathcal{E})$$

$$\widetilde{B}(\mathcal{I}) := Z^{\mathcal{I}} := \{ \chi : \mathcal{I} \rightarrow Z \} \quad (\text{ghost ring})$$

$$\text{pr} : \widetilde{B}(\mathcal{E}) \rightarrow \widetilde{B}(\mathcal{I}) \quad (\text{射影})$$

$$\varphi = (\varphi_I) : B(\mathcal{I}) \rightarrow \widetilde{B}(\mathcal{I}) = \prod_I Z$$

$$\varphi_I : \sum_J a_J [J] \mapsto \sum_J a_J \langle I, J \rangle, \quad \langle I, X \rangle := |\text{Hom}(I, X)|$$

$$\psi = (\psi_I)_I : \widetilde{B}(\mathcal{I}) \rightarrow \text{Obs}(\mathcal{I}) = \prod_I (Z/|\text{Aut}(I)|Z)$$

$$\psi_I : \chi \mapsto \sum_{\sigma \in \text{Aut}(I)} \chi(I/\sigma) \bmod |\text{Aut}(I)|.$$

ここで, I/σ は $1, \sigma : I \rightarrow I$ の coequalizer.

$$\therefore |\text{Hom}(I, X)^{(\sigma)}| = |\text{Hom}(I/\sigma, X)|.$$

定理

$$0 \longrightarrow B(\mathcal{I}) \xrightarrow{\varphi} \tilde{B}(\mathcal{I}) \xrightarrow{\psi} \mathbf{Obs}(\mathcal{I}) \longrightarrow 0 \quad (\text{exact}).$$

証明. $\mathcal{I} \times \mathcal{I}$ 型整数行列を次で定義する :

$$\begin{aligned} H &:= (\langle I, J \rangle), \\ L &:= (|\text{Quot}(I, J)|), \quad |\text{Quot}(I, J)| = |\text{Epi}(I, J)|/|\text{Aut}(J)| \in \mathbf{Z} \\ D &:= (|\text{Aut}(I, J)|\delta_{I, J}) \\ U &:= (|\text{Sub}(I, J)|), \quad |\text{Sub}(I, J)| = |\text{Mon}(I, J)|/|\text{Aut}(I)| \in \mathbf{Z} \end{aligned}$$

このとき $H = LDU$ であり, 適当な並べ替えにより L はベキ単下三角行列, D は対角行列, U はベキ単上三角行列になる. 対象の並べ替えとしては, $I \leftarrow \exists K (\in \mathcal{I}) \mapsto J$ のとき $I \leq J$ となるように小さい方から並べればよい.

$$\therefore \det H = \det L \det D \det U = \prod_I |\text{Aut}(I)| \neq 0$$

よって, H^{-1} が存在し, $\text{Ker} \varphi = 0$ かつ $|\text{Coker}(\varphi)| = |\mathbf{Obs}(\mathcal{I})|$. Cauchy-Frobenius の補題により, $\psi \circ \varphi = 0$. ψ の全射は明らかなので, 以上により完全性が言える.

系. $B(\mathcal{I})$ は, φ を環準同型とするただひとつの環構造を持つ.

有限部分カテゴリー $\mathcal{I} \subseteq \text{Con}(\mathcal{E})/\cong$ の部分カテゴリー \mathcal{I}_{epi} を, 対象は \mathcal{I} と同じで, 射は全射だけとして定義する.

このときふたつの Burnside 環 $B(\mathcal{I})$ と $B(\mathcal{I}_{\text{epi}})$ が得られる.

命題. \mathcal{I} が全射像に関して閉じているなら, 環同型 $B(\mathcal{I}_{\text{epi}}) \cong B(\mathcal{I})$ がある.

ある $G \in \mathcal{E}$ があって, G から任意の $I \in \mathcal{I}$ への全射が存在すると仮定する.

$$E : \mathcal{I} \longrightarrow \text{Set}; I \longmapsto \text{Epi}(G, I)$$

なるファンクターを取る. $\tilde{\mathcal{I}} := \text{Elem}(E)$ を E の elements のカテゴリーとする. すなわち $\tilde{\mathcal{I}}$ の対象は (I, λ) の形をしている. ここで $I \in \mathcal{I}, \lambda : G \rightarrow I$. また $\tilde{\mathcal{I}}$ における射 $f : (I, \lambda) \rightarrow (J, \mu)$ は $f : I \rightarrow J$ で $\mu = f \circ \lambda$ を満たすものとして定義する. このとき, $\tilde{\mathcal{I}}/\cong$ は半順序集合 (すなわち各 Hom-set がただひとつの元からなる) である.

$$f: \tilde{\mathcal{I}} \rightarrow \mathcal{I}; (I, \lambda) \mapsto I$$

このとき G に関する仮定から, f は objects 上全射である. f の選択関数を f' とすると,

$$f': \text{Obj}(\mathcal{I}) \rightarrow \text{Obj}(\tilde{\mathcal{I}})/\cong$$

で $f \circ f' = \text{id}_{\text{Obj}(\mathcal{I})}$. μ_e を $\tilde{\mathcal{I}}/\cong$ のメビウス関数とする.

定理. 上の仮定と記号のもとで

$$L_{I,J}^{-1} = \sum_{(J,\beta) \in f^{-1}(J)/\text{Aut}(J)} \mu_e(f'(I), (J,\beta)).$$

$K \in \mathcal{I}$ に対応する $QB(\mathcal{I})$ の原始ベキ等元は

$$e_K = \sum L_{I,K}^{-1}[I]$$

であることに注意しておく.

p -局所整数環上のベキ等元公式もあるが別の機会に述べたい.

置換群の可移拡大の組合せ論的計算法

宮本 泉
山梨大学

$X = \{0, 1, 2, \dots, n\}$ とし, G_0 は $X \setminus \{0\}$ 上に可移な置換群とする. ただし, G_0 は $X \setminus \{0\}$ 上に 2 重可移ではないとする. G_0 が $X \times X \times X$ に作用したときの orbit を

$$\{R_1, R_2, \dots, R_s\}.$$

G_0 は 群 G における点 0 の固定部分群とする. G は G_0 の可移拡大になる.

群の元は使わないで, $\{R_1, R_2, \dots, R_s\}$ を集めて結合を作ることによって, G の $X \times X \times X$ 上の orbit を構成することができるか? ----- かなり "Yes" らしい.

2 重可移群は対称群と同じアソシエーションスキームを定義してしまう。では, 2 重可移で, 3 重可移ではない群の 1 点固定群の作るアソシエーションスキームからもとの 2 重可移群を求めることができるか? ----- 答は "No"

Association schemes と Superschemes

定義. $(X, \{R_i\}_{0 \leq i \leq d})$ が Association scheme または (X, Π) が t -Superscheme であるとは, それぞれ \iff

A1. $\{R_0, R_1, \dots, R_d\}$ は $X \times X$ の分割, ただし, $R_0 = \{(x, x) | x \in X\}$,

S1. $\Pi = \{\Pi^1, \Pi^2, \dots, \Pi^t\}$, $t \geq 2$, で Π^l は $1 \leq l \leq t$ において X^l の分割,

A2. すべての R_i に対して, $R_{i'}$ が存在して, $R_{i'} = \{(y, x) | (x, y) \in R_i\}$ が成立,

S2. $\sigma \in \text{Sym}(l)$ について, $\sigma((y_1, y_2, \dots, y_l)) = (y_{\sigma(1)}, y_{\sigma(2)}, \dots, y_{\sigma(l)})$ とおき, $\Pi^l = \{R_0^l, R_1^l, \dots, R_{d_l}^l\}$, $1 \leq l \leq t$, とおくと, すべての R_k^l と $\sigma \in \text{Sym}(l)$, に対して, $\sigma(R_k^l) \in \Pi^l$... (symmetric)

A3. すべての R_i, R_j, R_k と, すべての $(x, y) \in R_k$ に対して, constant p_{ijk} が存在して, 次が成立

$$p_{i,j,k} = \#\{z \in X | (x, z) \in R_i, (z, y) \in R_j, (x, y) \in R_k\}.$$

S3. projection $\pi^l : X^l \rightarrow X^{l-1}$ を

$$\pi^l((y_1, y_2, \dots, y_{l-1}, y_l)) = (y_1, y_2, \dots, y_{l-1}),$$
 で定義すると, すべての $R_k^l \in \Pi^l$, $2 \leq l \leq t$ に対して, $\pi^l(R_k^l) \in \Pi^{l-1}$,

S4. すべての R_k^l , $2 \leq l \leq t$, と, すべての $y = (y_1, y_2, \dots, y_{l-1}) \in \pi^l(R_k^l)$ に対して, $\text{constant } p_k^l = |(\pi^l)^{-1}(y) \cap R_k^l|$ が存在. 特に, $p_k^l = |R_k^l|/|\pi^l(R_k^l)|$ (regular)

A3'. $R_{i,j,k}^3 = \{(x, y, z) | (x, z) \in R_i, (z, y) \in R_j, (x, y) \in R_k\}$ とおくと, すべての $(x, y) \in R_k$ に対して, $p_{i,j,k} = |(\pi^3)^{-1}((x, y)) \cap R_{i,j,k}^3|$ が成立.

注: $\pi_j^l((y_1, y_2, \dots, y_l)) = (y_1, y_2, \dots, y_{j-1}, y_{j+1}, \dots, y_l)$ とおくと, 対称性より,

$$\pi_j^l(R_k^l) \in R^{l-1}$$

G が X 上の置換群のとき, Π^l を G が X^l , $1 \leq l \leq t$ に作用したときの orbit とすると, (X, Π) は, $\Pi = (\Pi^1, \Pi^2, \dots, \Pi^t)$ において, *superscheme* になる.

$X^{(l)} = \{(x_1, x_2, \dots, x_l) | x_i \text{ 相異なる}\}$ とおく. もし G が X 上に可移なら, 重複成分は無視して, *superscheme* では G の $X^{(l)}$ 上の orbit を考えるだけで十分なので, *superscheme* (X, Π) , $\Pi = \{\Pi^1, \Pi^2, \dots, \Pi^t\}$, で下の様に定める.

$$\Pi^{(l)} = \{R_i^l | R_i^l \in \Pi^l \text{ and } R_i^l \subseteq X^{(l)}\}, \quad 1 \leq l \leq t.$$

一般に考える問題は次の様になる. G_0 は $X \setminus \{0\}$ 上に $(t-2)$ 重可移で, $(t-1)$ 重可移ではないとする. G_0 の X 上における可移拡大 G が存在するとする. (X, Π) を G の作る t -*superscheme* (X, Π') を G_0 の作る t -*superscheme* とする.

問題:

どうやって (X, Π') から (X, Π) をつくるか.

注: $\text{Aut}((X, \Pi))$ は G を含む $(t-1)$ -重可移で t -重可移ではない群になる.

可移拡大が無いときにも (X, Π) が得られることはある. そのときは, $\text{Aut}((X, \Pi))$ は可移にならない. (計算機による実験の結果)

G は X 上に $(t-1)$ 重可移なので, $\Pi^{(t-1)} = \{X^{(t-1)}\}$, $\Pi^{(t)} = \{R_1^t, R_2^t, \dots, R_r^t\}$ とする. つまり, G は $X^{(t)}$ 上, r 個の orbits をもつ. すると,

$$p_{k,j}^t = |R_k^t|/|X^{(t-1)}| \text{ for } 1 \leq k \leq r \text{ and } 1 \leq j \leq t.$$

Proposition.

G_0 は $(X \setminus \{0\})^{(t-1)}$ 上, r -orbits R_k^{t-1} , $1 \leq k \leq r$, をもつ. そして, $|R_k^t| = |X| \cdot |R_k^{t-1}|$. 特に,

$$p_{k,j}^t = |R_k^{t-1}|/|(X \setminus \{0\})^{(t-2)}| \text{ for } 1 \leq k \leq r \text{ and } 1 \leq j \leq t.$$

Proof.

適当な順序で下のようになることからわかる.

$$\{x = \pi_i^t((x_1, x_2, \dots, x_{t-1}, 0)) | x \in R_k^t\} = R_k^{t-1} \text{ for } 1 \leq k \leq r.$$

G_0 のつくる superscheme (X, Π') , $\Pi' = \{\Pi^1, \Pi^2, \dots, \Pi^t\}$, で、次の constant を定めて、下の図式を参照して条件をチェックする。

$$p_{i,j}^t = |R_i^t| / |\pi_j^t(R_i^t)| \quad (R_i^t \in \Pi^{(t)}).$$

$\Pi^{(t)}$	=	$\{R_1, R_2, \dots, R_r\}$	(未知)
$\begin{array}{ccc} & \Downarrow \pi_j^t & \swarrow \text{Sym}(t) \\ & p_{k,j}^t & \end{array}$			
$\Pi^{(t-1)}$	=	$\{X^{(t-1)}\}$	=
$\Pi^{(t-1)}$	=	$\{R_1^{t-1}, \dots, R_r^{t-1}, \dots, R_{r+t-1}^{t-1}\}$	
(既知)		\dots	$p_{i,j}^t \dots$
$\begin{array}{ccc} & \text{Sym}(t) \swarrow & \uparrow \pi_j^t \\ & & \end{array}$			
$\Pi^{(t)}$	=	$\{R'_1, R'_2, \dots, R'_{r'}, \dots, R'_{r'+rt}\}$	

性質 S2 の $\text{Sym}(t)$ は、 X^t の成分上に作用して、orbit 番号 $\{1, 2, \dots, r\}$ と $\{1, 2, \dots, r' + rt\}$ 上の置換群を誘導する。ただし、 $\Pi^{(t)} = \{R_1, R_2, \dots, R_r\} = G$ の $X^{(t)}$ 上の orbit, $\Pi^{(t)} = \{R'_1, R'_2, \dots, R'_{r'+rt}\} = G_0$ の $X^{(t)}$ 上の orbit であり、 $Y = \{1, 2, \dots, r' + rt\}$ とおく。

もし G が G_0 の可移拡大ならば、 Y の分割 $\{Y_1, Y_2, \dots, Y_k\}$ で、次が成立つものがある。

$$R_k = \bigcup_{l \in Y_k} R'_l, \quad 1 \leq k \leq r.$$

このとき、 $Y_{k,j,s} = \{l \in Y_k \mid R'_s{}^{(t-1)} = \pi_j^t(R'_l)\}$, $1 \leq s \leq r+t-1$, とおくと、

$$p_{k,j}^t = \sum_{l \in Y_{k,j,s}} p_{l,j}^t,$$

そして、 $\{Y_{k,j,1}, Y_{k,j,2}, \dots, Y_{k,j,r+t-1}\}$ は $1 \leq j \leq t$ で、 Y_k の分割になる。さらに、 $\text{Sym}(t)$ の 2 つの orbit 番号 $\{k\}$ と $\{l\}$ への作用は両立する。

以上の条件のもとに、上の図表を参照して、アルゴリズムがどの様に働くか、以下で、例を使って示す。

例: $PSL(m, q)$, $m \geq 3$

$G = PSL(m, q)$, $m \geq 3$, $X = P$ (q 元体上の $m-1$ 次元射影空間).

$G_0 = G$ における点 P_i の固定部分群 (stabilizer).

$t = 3$, $n = |P \setminus \{P_i\}| = q + q^2 + \dots + q^{m-1}$.

Table 1
 $PSL(m, q)$ における P_l の固定部分群の $P^{(2)}$ 上の orbit と
 $PSL(m, q)$ の $(P \cup \{P_0\})^{(3)}$ 上の orbit

No.	点 P_l の固定部分群		$PSL(m, q)$		property
	size	rep.	size	rep.	
1	$n(q-1)$	(P_i, P_j)	$(n+1)n(q-1)$	(P_i, P_j, P_l)	$P_j \in \langle P_i, P_l \rangle$
2	$n(n-q)$	(P_i, P_j)	$(n+1)n(n-q)$	(P_i, P_j, P_l)	$P_j \notin \langle P_i, P_l \rangle$
3	n	(P_l, P_i)	$(n+1)n$	(P_0, P_i, P_l)	
4	n	(P_i, P_l)	$(n+1)n$	(P_i, P_0, P_l)	
5			$(n+1)n$	(P_i, P_l, P_0)	

Table 1 の左部分から, G は $X^{(3)}$ 上に 2 個の orbit R_1 と R_2 をもち, その size は $(n+1)n(q-1)$ and $(n+1)n(n-q)$. 性質 S2 の $Sym(3)$ は $\Pi^{(3)} = \{R_1, R_2\}$ に自明に作用, (\therefore size が違うので, $|R_1| = (n+1)n(q-1) < (n+1)n(n-q) = |R_2|$).

Table 2
 $PSL(m, q)$ における P_l の固定部分群の $P^{(3)}$ 上の orbit

No.	size	rep.	property
1(1)	$n(q-1)$	(P_i, P_j, P_k)	$P_j, P_k \in \langle P_l, P_i \rangle$
\vdots	\vdots	\vdots	\vdots
1($q-2$)	$n(q-1)$	(P_i, P_j, P_k)	$P_j, P_k \in \langle P_l, P_i \rangle$
2	$n(q-1)(n-q)$	(P_i, P_j, P_k)	$P_j \in \langle P_l, P_i \rangle, P_k \notin \langle P_l, P_i \rangle$
3	$n(q-1)(n-q)$	(P_i, P_j, P_k)	$P_j \notin \langle P_l, P_i \rangle, P_k \in \langle P_l, P_i \rangle$
4	$n(q-1)(n-q)$	(P_i, P_j, P_k)	$P_j \notin \langle P_l, P_i \rangle, P_k \in \langle P_l, P_j \rangle$
5	$n(q-1)(n-q)$	(P_i, P_j, P_k)	$P_j \notin \langle P_l, P_i \rangle, P_k \in \langle P_i, P_j \rangle$
6	$n(q-1)^2(n-q)$	(P_i, P_j, P_k)	$P_k \in \langle P_l, P_i, P_j \rangle$, non collinear
6(1, 2, 3)	$n(q-1)^2(n-q)/3$	(P_i, P_j, P_k)	as above and $m = 3 q-1$
7	$n(n-q)(n-q-q^2)$	(P_i, P_j, P_k)	$P_k \notin \langle P_l, P_i, P_j \rangle$, non collinear
8	$n(q-1)$	(P_l, P_i, P_j)	$P_j \in \langle P_l, P_i \rangle$
9	$n(n-q)$	(P_l, P_i, P_j)	$P_j \notin \langle P_l, P_i \rangle$
10	$n(q-1)$	$\langle P_i, P_l, P_j \rangle$	$P_j \in \langle P_l, P_i \rangle$
11	$n(n-q)$	$\langle P_i, P_l, P_j \rangle$	$P_j \notin \langle P_l, P_i \rangle$
12	$n(q-1)$	(P_i, P_j, P_l)	$P_j \in \langle P_l, P_i \rangle$
13	$n(n-q)$	(P_i, P_j, P_l)	$P_j \notin \langle P_l, P_i \rangle$

$Sym(3)$ は $\{2, 3, 4\}$, $\{8, 10, 12\}$, $\{9, 11, 13\}$ へ可移に作用.

projection の性質

No.	π_1		π_2		π_3	
	im.	mult.	im.	mult.	im.	mult.
$1(1, \dots, q-2)$	1	1	1	1	1	1
2	2	$q-1$	2	$q-1$	1	$n-q$
3	2	$q-1$	1	$n-q$	2	$q-1$
4	1	$n-q$	2	$q-1$	2	$q-1$
5	2	$q-1$	2	$q-1$	2	$q-1$
6	2	$(q-1)^2$	2	$(q-1)^2$	2	$(q-1)^2$
$6(1, 2, 3)$	2	$(q-1)^2/3$	2	$(q-1)^2/3$	2	$(q-1)^2/3$
7	2	$n-q-q^2$	2	$n-q-q^2$	2	$n-q-q^2$
8	1	1	3	$q-1$	3	$q-1$
9	2	1	3	$n-q$	3	$n-q$
10	3	$q-1$	1	1	4	$q-1$
11	3	$n-q$	2	1	4	$n-q$
12	4	$q-1$	4	$q-1$	1	1
13	4	$n-q$	4	$n-q$	2	1

第 k 行: im. = orbit 番号 s で、次を満たす $R_s^{t-1} = \pi_j(R_k)$

mult. = $p_{k,j}^3 = |R_k'|/|R_s^{t-1}'|$ となっている。

答 (一般の場合): $Y_1 = \{1(1, \dots, q-2), 5, 8, 10, 12\}$, $Y_2 = \{2, 3, 4, 6, 7, 9, 11, 13\}$.

メモ: $p_{1,j}^3 = q-1$ and $p_{2,j}^3 = n-q$ for $1 \leq j \leq 3$.

$Y_{1,1,1} = \{1(1, \dots, q-2), 8\}$, $Y_{1,1,2} = \{5\}$, $Y_{1,1,3} = \{10\}$, $Y_{1,1,4} = \{12\}$, $Y_{2,1,1} = \{4\}$, $Y_{2,1,2} = \{2, 3, 6, 7, 9\}$, $Y_{2,1,3} = \{11\}$ and $Y_{2,1,4} = \{13\}$ となっている。

特別な場合の答:

$q=2$ の場合;

$Y_1 = \{5, 8, 10, 12\}$ or $Y_1 = \{6, 8, 10, 12\}$, $Y_2 = Y \setminus Y_1$.

$m=3$, かつ $q=4$ の場合;

$Y_1 = \{1(1, \dots, q-2), i, 8, 10, 12\}$, ここで、 i は $\{5, 6(1), 6(2), 6(3)\}$ の中の一つ、 $Y_2 = Y \setminus Y_1$. (このとき、 $\text{Aut}((X, \Pi)) = \text{PGL}(3, 4)$: 計算機実験)

Association scheme vs. Superscheme

第 5 と第 6 orbit は association scheme の 1 つの relation にはいる。(表の "im." の列からわかる。) しかし、上の拡大では $5 \in Y_1$, $6 \in Y_2$. association schemes では可移拡大を求められない場合がある。

$PSL(m, q)$ 自身の可移拡大

$t=4$, $Y = \{1, 2, \dots, 15\}$. (Table 3 を参照のこと)

答無し (一般の場合). 何故ならば表から $\{2, 3, 4, 5\} \subset Y_2$, そして $Y_{1,1,2} \subseteq \{6, 7, 9\}$ となる。しかし、これでは $p_{1,1}^3 = q-1 = \sum_{s \in Y_{1,1,2}} p_{s,1}^3$ にならない。

Table 3
 $PSL(m, q)$ の $(P \cup \{P_0\})^{(4)}$ 上の orbit

No.	size/(n+1)n	rep.	property
1(1)	(q-1)	(P_i, P_j, P_k, P_l)	$P_j, P_k \in \langle P_i, P_l \rangle$
⋮	⋮	⋮	⋮
1(q-2)	(q-1)	(P_i, P_j, P_k, P_l)	$P_j, P_k \in \langle P_i, P_l \rangle$
2	$(q-1)(n-q)$	(P_i, P_j, P_k, P_l)	$P_j \in \langle P_i, P_l \rangle, P_k \notin \langle P_i, P_l \rangle$
3	$(q-1)(n-q)$	(P_i, P_j, P_k, P_l)	$P_j \notin \langle P_i, P_l \rangle, P_k \in \langle P_i, P_l \rangle$
4	$(q-1)(n-q)$	(P_i, P_j, P_k, P_l)	$P_j \notin \langle P_i, P_l \rangle, P_k \in \langle P_i, P_j \rangle$
5	$(q-1)(n-q)$	(P_i, P_j, P_k, P_l)	$P_j \notin \langle P_i, P_l \rangle, P_k \in \langle P_i, P_j \rangle$
6	$(q-1)^2(n-q)$	(P_i, P_j, P_k, P_l)	$P_k \in \langle P_i, P_l, P_j \rangle$, non collinear
6(1,2,3)	$(q-1)^2(n-q)/3$	(P_i, P_j, P_k, P_l)	as above and $m = 3 q-1$
7	$(n-q)(n-q-q^2)$	(P_i, P_j, P_k, P_l)	$P_k \notin \langle P_i, P_l, P_j \rangle$, non collinear
8	(q-1)	(P_0, P_i, P_j, P_k)	$P_k \in \langle P_i, P_j \rangle$
9	(n-q)	(P_0, P_i, P_j, P_k)	$P_k \notin \langle P_i, P_j \rangle$
10	(q-1)	(P_i, P_0, P_j, P_k)	$P_k \in \langle P_i, P_j \rangle$
11	(n-q)	(P_i, P_0, P_j, P_k)	$P_k \notin \langle P_i, P_j \rangle$
12	(q-1)	(P_i, P_j, P_0, P_k)	$P_k \in \langle P_i, P_j \rangle$
13	(n-q)	(P_i, P_j, P_0, P_k)	$P_k \notin \langle P_i, P_j \rangle$
14	(q-1)	(P_i, P_j, P_k, P_0)	$P_k \in \langle P_i, P_j \rangle$
15	(n-q)	(P_i, P_j, P_k, P_0)	$P_k \notin \langle P_i, P_j \rangle$

Sym(4) は {2, 3, 4, 5}, {8, 10, 12, 14}, {9, 11, 13, 15} に可移に作用.

projection の性質

No.	π_1		π_2		π_3		π_4	
	im.	mult.	im.	mult.	im.	mult.	im.	mult.
1(1, ..., q-2)	1	1	1	1	1	1	1	1
2	2	q-1	2	q-1	1	n-q	2	q-1
3	2	q-1	1	n-q	2	q-1	2	q-1
4	1	n-q	2	q-1	2	q-1	2	q-1
5	2	q-1	2	q-1	2	q-1	1	n-q
6	2	$(q-1)^2$	2	$(q-1)^2$	2	$(q-1)^2$	2	$(q-1)^2$
6(1,2,3)	2	$(q-1)^2/3$	2	$(q-1)^2/3$	2	$(q-1)^2/3$	2	$(q-1)^2/3$
7	2	$n-q-q^2$	2	$n-q-q^2$	2	$n-q-q^2$	2	$n-q-q^2$
8	1	1	3	q-1	3	q-1	3	q-1
9	2	1	3	n-q	3	n-q	3	n-q
10	3	q-1	1	1	4	q-1	4	q-1
11	3	n-q	2	1	4	n-q	4	n-q
12	4	q-1	4	q-1	1	1	5	q-1
13	4	n-q	4	n-q	2	1	5	n-q
14	5	q-1	5	q-1	5	q-1	1	1
15	5	n-q	5	n-q	5	n-q	2	1

q = 2 の場合

$Y_1 = \{6, 8, 10, 12, 14\}$, $Y_2 = \{2, 3, 4, 5, 9, 11, 13, 15\}$.

可移拡大は $AGL(m, 2)$ になっているはず.

$m = 3$ かつ $q = 4$ の場合

$Y_1 = \{1(1, \dots, q-2), i, 8, 10, 12, 14\}$, ここで i は $\{6(1), 6(2), 6(3)\}$ の一つ. 可移拡大は M_{22} になっているはず. 計算実験では $\text{Aut}(M_{22})$.

$AGL(m, 2)$ の可移拡大

$t = 5, Y = \{2, \dots, 17\}$. (表無し)

答無し. なぜなら, 性質 S2 の $\text{Sym}(5)$ の作用から, $\{2, 3, 4, 5, 6\} \subset Y_2$ なので.

M_{22} の可移拡大

$t = 5, Y = \{1(1), 1(2), 2, \dots, 6(1), 6(2), 6(3), 8, \dots, 17\}$. (表無し)

$\{2, 3, 4, 5, 6(i)\} \subset Y_2$, ここで i は $\{1, 2, 3\}$ の一つ, が成立するはず. $6(3) \in Y_2$ と番号をつけることにする.

答は 2 つ, $Y_1 = \{1(1), 1(2), i, 8, 10, 12, 14, 16\}$, i は $\{6(1), 6(2)\}$ のいずれか.

M_{23} がでるはず.(未計算)

$\text{Aut}(M_{22})$ では $6(1) \cup 6(2)$ が orbit なので, 可移拡大は存在しない.

M_{23} の可移拡大, $t = 6, |Y| = 19$. 次が成立し, $Y_1 = \{1(1, \dots, q-2), 6(1), 8, 10, 12, 14, 16\}$, M_{24} がでるはず.

M_{24} の可移拡大, $t = 7, |Y| = 21$. 性質 S2 の $\text{Sym}(7)$ は $\{2, 3, 4, 5, 6(1), 6(2), 6(3)\}$ に可移作用して, それは Y_2 に入るしかない. そして, $Y_1 = \{1(1, \dots, q-2), 8, 10, 12, 14, 16, 18, 20\}$ となるが, それでは, $p_{k,j}^3$ についての条件が成立することは無い. 故に, M_{24} の可移拡大は無い.

$G = Sp(2m, 2)$ の $O^+(2m, 2)$ と $O^-(2m, 2)$ for $m \geq 3$ による coset 上への作用の場合も, 同様に, 可移拡大の計算に成功している.

計算機による実験には GAP を使用している.

References

- [1] G. Ivanyos. On the combinatorics of evdokimov's deterministic factorization. *Draft preprint*, 1997.
- [2] K. W. Johnson and J. D. H. Smith. Characters of finite quasigroups IV: products and superschemes. *European J. Combin.*, 10:257-263, 1989.
- [3] W. M. Kantor. Some consequences of the classification of finite simple groups. *Contemporary Math.*, 45:159-173, 1985.
- [4] 宮本泉: アソシエーションスキームの拡張と 2 重可移群の計算. 数理解析研究所講究録. *Computer Algebra - Algorithms, Implementations and Applications*, to appear .
- [5] J. D. H. Smith. Association schemes, superschemes, and relations invariant under permutation groups. *European J. Combin.*, 15(3):285-291, 1994.

Finite groups with small number of conjugacy lengths

千葉大学 石川 賢太

1 Notations and Results

G : finite group

$Irr(G)$: the set of ordinary irreducible characters of G

$Cl(G)$: the set of conjugacy classes of G

$cd(G) := \{\chi(1); \chi \in Irr(G)\} = \{1, n_1, n_2, \dots, n_s\}$ ($1 < n_1 < n_2 < \dots < n_s$)

$ccl(G) := \{|C|; C \in Cl(G)\} = \{1, m_1, m_2, \dots, m_t\}$ ($1 < m_1 < m_2 < \dots < m_t$)

$Z(G)$: the center of G

G' : the commutator subgroup of G ($:= [G, G]$)

私の知る限りでは 1950 年代頃から $cd(G), ccl(G)$ に対して条件を与え、それを満たす G の性質あるいは特徴付けをし、 $cd(G)$ と $ccl(G)$ のそれぞれの結果を比較するなどの研究が行われてきた。character degrees, conjugacy lengths と G の order の間には次のよく知られた関係がある。

$$\begin{aligned} \chi(1) \mid |G|, \quad |C| \mid |G|, \quad |Irr(G)| = |Cl(G)|, \\ |G| = \sum_{\chi \in Irr(G)} \chi(1)^2 = \sum_{C \in Cl(G)} |C| \end{aligned}$$

上の関係から $cd(G)$ よりも $ccl(G)$ のほうが自由度が高く、実際に $cd(G)$ へ条件を与えた結果より、 $ccl(G)$ へ条件を与えた結果のほうが強い結果が出る場合が多い。以下の結果及び例は多くを Huppert, 「Character Theory of Finite Groups」(de Gruyter 1998) から抜粋している。

Example

(1) (Ito, 1951 Michler, 1984 Okuyama) $p \nmid \chi(1)$ for all $\chi \in Irr(G)$

$\Leftrightarrow G$ は normal abelian Sylow p -subgroup を持つ。(単純群の分類を利用している)

(elementary proof) $p \nmid |C|$ for all $C \in Cl(G)$

$\Leftrightarrow G$ の Sylow p -subgroup は center に含まれる。

(2) (Thompson, 1970) $p \mid \chi(1)$ for all $\chi \in Irr(G)$ with $\chi(1) > 1$

$\Rightarrow G$ は p -nilpotent である。

(Huppert) $p \mid |C|$ for all $|C| \in Cl(G)$ with $|C| > 1$

\Rightarrow いくらでも大きい p -length の group がとれる。

(3) character degrees の prime divisors に関する次のような問題がある。

$\rho(G) := \{p; p \text{ prime}, p \mid \chi(1) \text{ for some } \chi \in Irr(G)\}$

自然数 n に対して $\sigma(n) := |\{p; p \text{ prime}, p \mid n\}|$

$\sigma(G) := \text{Max}\{\sigma(\chi(1)); \chi \in Irr(G)\}$ とすると、 G が solvable のとき

$$|\rho(G)| \leq 3\sigma(G) + 2 \quad (\text{Gluck, Manz, Wolf, 1993})$$

という結果があり、最終的には $|\rho(G)| \leq 2\sigma(G)$ ではないかと予想されている。また、一般の場合にもいくつか結果があり $|\rho(G)| \leq 3\sigma(G)$ と予想されている。

一方 conjugacy length に対しても同様な問題が考えられており

$$\rho^*(G) := \{p; p \text{ prime}, p \mid |C| \text{ for some } C \in Cl(G)\}$$

$\sigma^*(G) := \text{Max}\{\sigma(|C|); C \in Cl(G)\}$ とすると solvable の場合と一般の場合でそれぞれ次のような結果が示されている。

$$|\rho^*(G)| \leq 4\sigma^*(G) + 1$$

$$|\rho^*(G)| \leq 5\sigma^*(G) + 1$$

(Ferguson, Casolo, Dolfi, 1996)

同様に $|\rho^*(G)| \leq 2\sigma^*(G)$ と予想されていたが、Dolfi, Casolo(1996) によって否定的に示された。

(4) (character degree graph と conjugacy length graph)

character degree graph $\Gamma(G)$ とは vertices を $\rho(G)$ 、edges を異なる $p, q \in \rho(G)$ に対して

$$p \sim q \Leftrightarrow pq \mid \chi(1) \text{ for some } \chi \in Irr(G)$$

で表されたものとする。

(a) G が solvable のとき、 $\Gamma(G)$ は高々2つの components しか持たない。(Manz, 1985)

(b) 一般の場合には、高々3つの components しか持たず、best possible であることは $cd(SL(2, 2^f)) = \{1, 2^f - 1, 2^f, 2^f + 1\}$ からわかる。ただし (b) の結果には単純群の分類が使われている。(Manz, Staszewski, Willems, 1988)

一方で同様な仕方で conjugacy length version も存在する。conjugacy length graph $\Gamma^*(G)$ とは vertices を $\rho^*(G)$ 、edges を異なる $p, q \in \rho^*(G)$ に対して

$$p \sim q \Leftrightarrow pq \mid |C| \text{ for some } |C| \in Cl(G).$$

で表されたものとする。

(c) この場合も全ての G において $\Gamma^*(G)$ は components は高々2つであることが知られている。

(Kazarin, 1981)

(d) ここで非常に興味深い結果として、Example 1.1 より $\rho(G) \subseteq \rho^*(G)$ であり、

Theorem [Dolfi, 1995]

G が solvable のとき p, q を異なる素数とすると、ある $\chi \in Irr(G)$ に対して $pq \mid \chi(1)$ ならば $pq \mid |C|$ となる $|C| \in Cl(G)$ が存在する。

という結果から $\Gamma(G)$ は $\Gamma^*(G)$ の subgraph となる。nonsolvable の場合はまだ知られていない。

(3) そのほかにも $cd(G)$ や $ccl(G)$ が全て素数、全て素数べきあるいは全て square free などそれぞれの条件を満たす group の性質や特徴づけを行うなどの結果もある。

2 $|cd(G)|$ について

$cd(G)$ の研究においてもっとも基本的な問題として $|cd(G)|$ に対する研究があり、実際これらの研究の中で最初のものとなっている。次はそれらに関する結果である。

Theorem 2.1 [Isaacs-Passman, 1968]

G : finite group with $cd(G) = \{1, m\} (m > 1)$

$$\Rightarrow G'' = 1$$

Theorem 2.2 [Issacs,1968] G : finite group with $cd(G) = \{1, m\} (m > 1)$ \Rightarrow 次のうち一つは正しい。

- (1) G は index m を持つ abelian normal subgroup を持つ。
 (2) 素数 p が存在して $m = p^a (a > 0)$ であり G は nilpotent である。更に

$$G = P \times A$$

ここで P は nonabelian p -group、 A は abelian p' -group である。**Theorem 2.3 [Isaacs,1969]** G : finite group with $|cd(G)| = 3$ $\Rightarrow G$ は solvable であり $G''' = 1$ このことから自然な予想として G を solvable としたとき一般の group に対して

$$dl(G) \leq |cd(G)|$$

であるかという問題があり、monomial のとき満たされることが知られている。

Remark 2.4

- (1) $|cd(G)| = 4$ の場合には A_5 などの単純群が存在する。
 (2) $cd(G) = \{1, m\} (m > 1)$ の example として Frobenius group $G = C_7 \rtimes C_6$ がある。このとき $cd(G) = \{1, 6\}$ であり、nilpotent でなく Theorem 2.2 (2) を満たさない。
 (3) まず p, q を素数とし $K = GF(p^q)$ とおく。このとき

$$G = \left\{ \begin{pmatrix} x & \\ & ax^{p^j} + b \end{pmatrix}; a, b \in K, a \neq 0, 0 \leq j < q \right\}$$

は $G = \underbrace{(C_p \times C_p \times \cdots \times C_p)}_q \rtimes C_{p^q-1} \rtimes C_q$ と semidirect product で表される。このとき $cd(G) = \{1, q, p^q - 1\}$ かつ $dl(G) = 3$ となり、これは Theorem 2.3 が best possible であることを示している。

3 $|ccl(G)|$ について

一方 conjugacy lengths に関する同様の研究で $ccl(G) = \{1, m\} (m > 1)$ なる group G に対し $G''' = 1$ ではないかと予想するのは自然であり、前出の Huppert の本にも同様な予想が書かれている。この研究の初期の主な結果には次のようなものがある。**Theorem 3.1 [Ito,1953]** G : finite group with $ccl(G) = \{1, m\} (m > 1)$ \Rightarrow ある素数 p が存在し $m = p^a (a > 0)$ となり

$$G = P \times A$$

ここで P は nonabelian p -group、 A は abelian p' -group である。特に G は nilpotent である。

この結果は先の Isaacs-Passman の character degree の場合の 10 年以上前に示されていることは非常に興味深く、conjugacy length のほうがより強い結果になっている。この結果から $ccl(G) = \{1, m\} (m > 1)$ をもつ group の研究は p -group に帰着できる。

Theorem 3.2 [Isaacs,1970]

G : finite p -group with $ccl(G) = \{1, p^a\} (a > 0)$
 $\Rightarrow G/Z(G)$ は exponent p を持つ。

この結果から次のように $p = 2$ に対する結果が示される。

Corollary 3.3

G : finite 2-group with $ccl(G) = \{1, 2^a\} (a > 0)$
 $\Rightarrow G'' = 1$

これ以降、Verardi, Mann などの結果がありましたが予想は解決せず、このことがこの方向における conjugacy length に関する研究が少ないことの理由の一つともなっていました。そして次の結果を示しました。

Theorem 3.4 [Ishikawa,2002]

G : finite group with $ccl(G) = \{1, m\} (m > 1)$
 $\Rightarrow G$ の nilpotent class は高々 3 である。

Corollary 3.5 [Verardi,1988]

このとき $G'' = 1$ かつ、ある素数 p が存在し G' は elementary abelian p -group である。

この結果は conjugacy length の研究の次なる発展の一つの条件となっていたと考えられ、この結果を利用した Barnea-Isaacs の論文の中にもそういった主旨の文章が見られる。

Remark 3.6

- (1) $|ccl(G)| = 3$ なる finite group G は solvable であることが知られている。(Ito,1970)
- (2) extraspecial p -group は $ccl(G) = \{1, p\}$ であることが知られており、逆に $ccl(G) = \{1, p\}$ なる G は本質的に extraspecial p -group である。また G が Camina group であるとは、任意の $x \in G - G'$ に対し、 x を含む conjugacy class が $xG' = \{xz; z \in G'\}$ となるようなものである。このとき、 $|G'| = p^n$ である nilpotent 2 の Camina p -group G は $|ccl(G)| = \{1, p^n\}$ となり、これによってこの class の nilpotent class 2 の series を作る。(Camina)
- (3) 次も $ccl(G) = \{1, p^n\} (n > 0)$ なる group の nilpotent class 2 の series を作る。

$$G = \langle a_1, a_2, \dots, a_n, b_{12}, b_{13}, \dots, b_{n-1,n}; [a_i, a_j] = b_{ij}, a_i^p = a_n^p = b_{ij}^p = 1, (1 \leq i < j \leq n) \rangle$$

- (4) nilpotent class 3 を持つ group には次のようなものがある。

$$G = \langle a_1, a_2, b, c_1, c_2; [a_1, a_2] = b, [a_i, b] = c_i, a_i^p = b^p = c_i^p (i = 1, 2) \rangle$$

このとき $ccl(G) = \{1, p^2\}$ である。

Problem

- (1) 先の Theorem 3.4 は構造論により証明されており、いくらかの情報が含まれていることから class 3 の $|ccl(G)| = 2$ の group の構造はかなり分かっている。また $|ccl(G)| = \{1, p\}, \{1, p^2\}, \{1, p^3\}$ に関する分

類があることで、 $|ccl(G)| = \{1, p^a\}$ ($a > 1$) の分類に関する予想があり、それは Remark 3.6 の Camina group、(3) の groups の quotient の形を持つものと (4) の group を拡張してものできると思われる。

(2) $|ccl(G)|$ に関する研究において次にくるのが $ccl(G) = \{1, m_1, m_2\}$ を調べることとなる。

$(m_1, m_2) = 1$ においては Dolfi によって特徴づけが行われている。

(3) Mann's conjecture

この予想は Theorem 3.4 の結果を受けて Mann によって提出されたもので近々 Israel J. Math に掲載される予定である。

Conjecture

G を finite p -group とし $ccl(G) = \{1, m_1, m_2, \dots, m_t\}$ ($1 < m_1 < m_2 < \dots < m_t$) と書くとき、次のような $f(s)$, $g(p)$ が存在する。

(a) conjugacy lengths m_1, m_2, \dots, m_s の conjugacy classes 全体で生成される subgroup の derived length は高々 $f(s)$ である。

(b) conjugacy length m_1 の conjugacy classes 全体で生成される subgroup の nilpotent class は高々 $g(p)$ である。

この結果はかなり一般的に書かれているが $dl(G) \leq f(|ccl(G)|)$ などの予想も含まれている。

参考文献

- [1] Y. Barnea, I. M. Isaacs, Lie algebra with few centralizer dimensions, *J. Algebra*. **259** (2003), 284–299
- [2] A.R. Camina, Some conditions which almost characterize Frobenius groups, *Israel J. Math.* **31** (1978), 153–160.
- [3] C. Casolo, S. Dolfi, The diameter of a conjugacy class graph of finite groups, *Boll. London Math. Soc.* **28** (1996), 141–148.
- [4] C. Casolo, S. Dolfi, Conjugacy class lengths of metanilpotent groups, *Rend. Sem. Mat. Padova*. **96** (1996), 121–130.
- [5] S. Dolfi, Prime factors of conjugacy class lengths and irreducible character degrees in finite solvable groups, *J. Algebra*. **174** (1995), 749–752.
- [6] S. Dolfi, Arithmetical conditions of the lengths of the conjugacy classes of a finite group, *J. Algebra*. **174** (1996), 753–771.
- [7] P. A. Ferguson, Lengths of conjugacy classes of finite solvable groups II, *J. Algebra*. **154** (1993), 223–227
- [8] P. Hall, The classification of prime-power groups, *J. Reine Angew. Math.* **182** (1940), 130–141.
- [9] B. Huppert, “Character Theory of Finite Groups”, de Gruyter Expositions in Mathematics, 25, Walter de Gruyter and Co., Berlin, 1998.
- [10] I. M. Isaacs, Groups with many equal classes, *Duke Math. J.* **37** (1970), 501–506.
- [11] I. M. Isaacs, Groups having at most three irreducible character degrees, *Proc. Am. Math. Soc.* **21** (1969), 185–188.

- [12] I. M. Isaacs, D. Passman. A characterization of groups in terms of the degrees of their characters II, *Pacific J. Math.* **24** (1968), 467–510.
- [13] K. Ishikawa, Finite p -groups up to isoclinism, which have only two conjugacy lengths, *J. Algebra.* **220** (1999), 333–345.
- [14] K. Ishikawa, On finite p -groups which have only two conjugacy lengths, *Israel J. Math.* **129** (2002), 119–123
- [15] N. Ito, On finite groups with given conjugate types I, *Nagoya Math. J.* **8** (1953), 17–28.
- [16] N. Ito, On finite groups with given conjugate types II, *Osaka J. Math.* **7** (1970), 231–251.
- [17] R. James, The groups of order p^6 (p an odd prime), *Math. Comp.* **34** (1980), 613–637.
- [18] L. S. Kazarin, On groups with isolated conjugacy classes, (Russian) *Izv. Vyssh. Zaved. Mat.* **7** (1981), 40–45
- [19] G. Michler, Brauer's conjectures and the classification of finite simple groups, in Representation Theory II: Groups and Orders, Proc. Ottawa 1984, Springer Lecture Notes 1178, 129–142
- [20] O. Manz Endliche auflösbare Gruppen, deren sämtliche Charaktergrade Primzahlpotenzen sind, *J. Algebra.* **94** (1985), 211–255
- [21] O. Manz, R. Staszewski, W. Willems, On the number of components of a graph related to character degrees, *Proc. Am. Math. Soc.* **103** (1988), 31–37
- [22] O. Manz, T. Wolf, Arithmetically long orbits of solvable linear groups, *Illinois J. Math.* **37** (1993), 652–665.
- [23] O. Manz, T. Wolf, Representations of Solvable Groups, Cambridge U. Press, 1993
- [24] T. Okuyama, On a problem of Wallace, preprint
- [25] J. G. Thompson, Normal p -complements and irreducible characters, *J. Algebra.* **14** (1970), 129–134.
- [26] L. Verardi, On groups whose noncentral elements have the same finite number of conjugates, *Boll. Unione Mat. Italia.* (7), **2A** (1988), 391–400.

The W -graphs of the Hecke algebra of type E_7

吉田 憲秀

千葉大学大学院自然科学研究科

E-mail: nyoshida@g.math.s.chiba-u.ac.jp

宮地 兵衛氏 (名大多元数理) との共同研究

June 2004

1 序

有限 Coxeter system から定義される Hecke 環の (generic) 表現は, W -graph というグラフの言葉で記述することが出来ることが Kazhdan-Lusztig [14] において示されている. 後に行者氏 [10] により, 一般の有限 Coxeter system から作られる Hecke 環の既約表現には, 対応する W -graph が存在することが示されると, 多くの有限 Coxeter 群に対し, 対応する Hecke 環の既約表現を表す W -graph が求められていった (c.f. [9]). 現在までに既約 W -graph が決定されていないものとしては, B, D, E_7, E_8 型 Weyl 群から作られる Hecke 環が残されていた.

既約 W -graph を決定するという問題に対しては, Geck [6] の定理を用いれば, E_7 型 Hecke 環 $\mathcal{H}(E_7)$ の場合には解決出来る道具は揃っている事に気づいた. これらが決定できれば generic 既約表現行列が得られるので, 特殊化により modular 既約表現行列及び分解行列を得ることも出来る. Hecke 環の modular 表現を考え, その block 構造を調べる際には分解行列と呼ばれる通常既約表現と modular 既約表現の対応情報を得ることが重要である. 例えば, 考えている block に森田同値となる basic algebra を決定する為の重要な手掛かりとなるからである. さらに E_8 型 Hecke 環の modular 分解行列を考察する為の情報も得られるであろう.

また, E_7 型の研究によって古典型の B, D 型の場合について考察する際にも役立つ道具が得られれば, 既約 W -graph を完全に調べ尽くすことが可能となるかも知れない.

本報告では, 以上のような動機から以下の 2 つの定理を得た事を紹介するものである.

Theorem 1. E_7 型 generic Hecke 環の既約表現を全て構成し, それらを W -graph として書き表した.

Theorem 2. k を標数が 2, 3 ではない体, $q^{1/2} \in k^*$ とする. 特殊化された $\mathcal{H}_{k,q}$ の既約表現の次元は, k の標数には依らず q の位数のみにより決まる. (i.e. Hecke 環版の James 予想の解決)

Remark 1. (1) Dipper [2] の定理により, Theorem 2 で決定された分解行列は有限 Chevalley 群 $E_7(q)$ の主系列の部分分解行列を与えていることになる.

(2) Theorem 2 の内容自体は, Geck, Müller により E_8 型 Hecke 環の情報を用いて得られているが, 我々の構成の方が統一的である.

2 一般論からの準備

この節では E_7 に依存しない事柄についてまとめておく.

(W, S) を一般の有限 Coxeter system, $\mathcal{A} := \mathbb{Z}[u^{1/2}, u^{-1/2}]$ とする.

Definition 1. \mathcal{A} 上の generic Hecke 環 $\mathcal{H} = \mathcal{H}_{\mathcal{A}}(W, S)$ とは, $\{T_w \mid w \in W\}$ を基底にもつ \mathcal{A} -algebra であり, $s \in S, w \in W$ に対し

$$T_s T_w = \begin{cases} T_{sw} & \text{if } l(sw) > l(w) \\ T_{sw} + (u^{1/2} - u^{-1/2})T_w & \text{if } l(sw) < l(w) \end{cases}$$

により積が定義される. ここで l は length function である.

Theorem 3 ([14]). $\mathcal{H}_{\mathcal{A}}(W, S)$ 上の involution

$$\overline{\sum_{w \in W} a_w(u) T_w} = \sum_{w \in W} a_w(u^{-1}) T_w^{-1}, \quad (\text{for } a_w(u) \in \mathcal{A})$$

に関し, 以下の 2 条件を満たす (Kazhdan-Lusztig) 基底が一意に存在する.

- (1) $\overline{C_w} = C_w,$
- (2) $C_w = T_w + \sum_{\substack{y \in W \\ y < w}} P_{y,w}^* T_y.$

ここで $P_{y,w}^*$ は Kazhdan-Lusztig 多項式, “ $<$ ” は Bruhat order である.

Definition 2 ([14]). 3 つ組み (Γ, μ, I) が以下の 4 つの条件を満たすとき (W, S) の W -graph であるという.

- (1) $\Gamma = (X, Y)$: vertices X , edges Y を持つ有向グラフ
- (2) $\mu : X \times X \rightarrow \mathbb{Z}$ s.t. $(x, y) \notin Y \Rightarrow \mu(x, y) = 0$
- (3) $I : X \rightarrow 2^S$
- (4) X を basis とする \mathcal{A} -free module V が

$$T_s x = \begin{cases} -x & s \in I(x) \\ ux + u^{1/2} \sum_{\substack{y \in X \\ s \in I(y)}} \mu(x, y) y & s \notin I(x) \end{cases}$$

により $\mathcal{H}_{\mathcal{A}}(W, S)$ -module となる.

Remark 2. 本稿で考える W -graph は,

$$X := \{C_w\}_{w \in W' \subset W},$$

$$I(w) := L(w) := \{s \in S \mid sw < w\}$$

を仮定する.

講演では省略した left cell について定義だけ述べておく.

Definition 3 ([14]). The Kazhdan-Lusztig left preorder \leq_L is the relation on W generated by $y \leq_L w$ if there exists some $s \in S$ such that C_y appears with nonzero coefficient in $T_s C_w$.

The equivalence relation associated with \leq_L will be denoted \sim_L , and the corresponding equivalence classes are called the left cells of W .

次の Geck の定理は本研究の発端となったものである.

Theorem 4 ([6]). Let $W' \subset W$ be a standard parabolic subgroup, and let X' be the set of all $w \in W$ such that w has minimal length in the coset wW' . Let C be a left cell of W' . Then $X' \cdot C$ is a union of left cells of W .

3 構成の概略

Theorem 1, Theorem 2 を得るまでの概略を述べると次の様になる.

- (1) Weyl 群 $W(A_6)$, $W(D_6)$, $W(E_6)$ の left cells を用意する. [CHEVIE [7]]
- (2) 1 の left cells を $W(E_7)$ へ誘導して共通部分を取り, $W(E_7)$ の left cells を小さく捕まえる. [GAP [4]]
- (3) 2 の各 left cell に対し, Kazhdan-Lusztig 多項式を計算する. [Coxeter [3]]
- (4) 2, 3 から left cell 表現を作る. [CHEVIE]
- (5) 4 の表現を既約分解する. [MeatAxe[15]+GAP]
- (6) 5 の既約表現から W -graph を構成する. [GAP]
- (7) 特殊化した $\mathcal{M}_{k,q}$ の分解行列を計算する. [MeatAxe]

若干の補足をする. CHEVIE には与えられた Coxeter 群に対し, 全ての left cell 及び各々の left cell 表現を計算する機能があるが, 定義通りの計算の効率が非常に悪く, $W(E_7)$ に対して直接計算することは不可能であった. そもそも我々の目的にとって $W(E_7)$ の全ての left cell を求めることは無駄であり, 必要な left cell のみを効率よく得る方法を考える必要があった.

Parabolic subgroup から 1 つの left cell を誘導して得られるのは $W(E_7)$ の left cell たちの disjoint union であるが, 多くの場合この段階ではまだサイズが大きくなり step 3 の実行が困難である. その為, 異なる parabolic subgroup からの誘導の共通部分を取ることで left cell をできるだけ小さく取り出すことが計算上重要になる. これが step 1, 2 の意味である.

Step 2 で得られた left cell を \mathcal{L} とする。これは $W(E_7)$ の元の集合でしかないので、 \mathcal{L} の表現を得るためには $\mu(x, y), x, y \in \mathcal{L}$ の値が必要となる。これは Kazhdan-Lusztig 多項式を計算することにより得られる。この計算は一般に非常に複雑であるが、何とか $W(E_7)$ に関する Kazhdan-Lusztig 多項式を計算することが出来た。

これで left cell 表現が手に入ったので、表現のチェック及び既約表現への分解をすることになる。ここで Hecke 環の表現に現れる成分の特殊性を利用して GAP のデータ構造、行列演算を改良し、現実的な時間で処理が完了するようにした。

Step 5 の既約表現への分解については以下の 2 通りの方法がある。

- 有限体上での modular 表現を使う方法。
- $L(w)$ を用いて (primitive) idempotent を構成する方法。

第一の方法についての詳細は Geck-Lux [8] を参照して頂く事にして、第二の方法について紹介する。

3.1

Left cell の表現には special representation と呼ばれる規約表現が unique に含まれていることが知られている (c.f. Carter [1]). これは次のようにして取り出すことが出来るようである。

\mathcal{L} を left cell とする。

- (1) ラベル $\{L(w)\}_{w \in \mathcal{L}}$ を計算する。
- (2) 同じラベルを持つ元を同一視し \mathcal{L} を分割する。 (i.e. W -graph で同じラベルの点を張り合わせる.)
- (3) (2) での大きさ最小の coset \mathcal{L} に対し、 $D := \sum_{w \in \mathcal{L}} C_w$ を考える。
- (4) D で張られる \mathcal{H} -submodule を計算する。

このように作った (4) の \mathcal{H} -submodule は、 \mathcal{L} の表現に含まれる special 表現となっていた。

なぜ special になるのか分かっていないが、“(2) で得られる coset の個数 = special から同じ操作で得られる coset の個数” という事が $B_n (n \leq 5), D_n (n \leq 5), F_4, E_6, E_7$ では確認出来ている。

3.2 Example

$W(B_2)$ の left cell は全部で 4 つ;

$$\{1\}, \{s_1, s_2 s_1, s_1 s_2 s_1\}, \{s_2, s_1 s_2, s_2 s_1 s_2\}, \{s_1 s_2 s_1 s_2\}.$$

下線部の left cell に対し、 \mathcal{H} -表現を計算すると以下ようになる。

$$T_{s_1} \mapsto \begin{bmatrix} -1 & \sqrt{u} & 0 \\ 0 & u & 0 \\ 0 & \sqrt{u} & -1 \end{bmatrix} \cong \begin{bmatrix} -1 & 2\sqrt{u} \\ 0 & u \end{bmatrix} \oplus 1,$$

$$T_{s_2} \mapsto \begin{bmatrix} u & 0 & 0 \\ \sqrt{u} & -1 & \sqrt{u} \\ 0 & 0 & u \end{bmatrix} \cong \begin{bmatrix} u & 0 \\ \sqrt{u} & -1 \end{bmatrix} \oplus u.$$

Left cell 表現の W -graph: ①—②—①

既約表現の W -graphs: ①—²②, ①

Remark 3. (1) 一般に left cell 表現は既約ではない。

(2) 一般に $|2^S| < \text{degree of a special representation}$ なので、全ての基底が見つかるわけではない。

講演の際に紹介した $\mathcal{H}(E_7)$ の既約 W -graph は、以上のような計算を行い、dual を考慮した edge を付けたものである。実際の W -graph 30 個をここに載せることは不可能な為割愛します。

4 分解行列

$W(E_7)$ の Poincaré 多項式

$$\Phi_2^7 \Phi_3^3 \Phi_4^2 \Phi_5 \Phi_6^3 \Phi_7 \Phi_8 \Phi_9 \Phi_{10} \Phi_{12} \Phi_{14} \Phi_{18}$$

において、各 $e \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 18\}$ に対し $r \mid \Phi_e(q)$ を満たす素数 r と素数 q を考える。 k を標数 r の体とすると行者-宇野の定理 [11] により、 $\mathcal{H}_{k,q}(E_7)$ は non-semisimple algebra となることが分かる。

ところで、[5] において Geck は $e \in \{5, 7, 8, 9, 10, 12, 14, 18\}$ の場合の block の構造を Brauer tree として完全に決定している。したがって分解行列としては $e \in \{2, 3, 4, 6\}$ の場合だけが問題となる。

我々は既に $\mathcal{H}_{\mathbb{Z}}(E_7)$ の既約表現 (既約 W -graph) を得ているので、MeatAxe での簡単な応用として Φ_e -modular 分解行列を得ることが出来る。(c.f. [8])

計算した分解行列は講演では紹介したものの、かなり大きく多いので本稿での掲載は割愛します。

5 関連事項

2004 年 5 月 CHEVIE-beta に Howlett-Yin が 2003 年 11 月に提供したとある $\mathcal{H}(E_7)$ の W -graph データが追加されていた。彼らの実際の構成方法 [12], [13] も計算機に困ってはいるが、 W -graph データを求めるという点においては我々よりも遥かに軽い計算で取行出来るようで、 E_8 の W -graph の一部さえも構成している。

しかし、彼らの方法では Kazhdan-Lusztig 多項式を直接計算する必要は無い為、我々が得た Kazhdan-Lusztig 多項式までも得ているのかは不明である。

ともあれ、 W -graph を構成する問題としては事実上 B, D 型の古典型についてのみ残された事になるだろう。

今後の問題としては、block algebra の構造を詳しく調べることにより、Hecke 環版の local representation theory を考えてみたい。

参考文献

- [1] Roger W. Carter, *Finite groups of Lie type*, Pure and Applied Mathematics, John Wiley & Sons Inc., New York, 1985, Conjugacy classes and complex characters, A Wiley-Interscience Publication.
- [2] Richard Dipper, *Polynomial representations of finite general linear groups in nondefining characteristic*, Representation theory of finite groups and finite-dimensional algebras (Bielefeld, 1991), Progr. Math., vol. 95, Birkhäuser, Basel, 1991, pp. 343–370.
- [3] Fukko du Cloux, *Cozeter, Version 3.0*, 2004.
- [4] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004, (<http://www.gap-system.org>).
- [5] Meinolf Geck, *Brauer trees of Hecke algebras*, Comm. Algebra **20** (1992), no. 10, 2937–2973.
- [6] ———, *On the induction of Kazhdan-Lusztig cells*, Bull. London Math. Soc. **35** (2003), no. 5, 608–614.
- [7] Meinolf Geck, Gerhard Hiss, Frank Lübeck, Gunter Malle, and Götz Pfeiffer, *CHEVIE—a system for computing and processing generic character tables*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 3, 175–210.
- [8] Meinolf Geck and Klaus Lux, *The decomposition numbers of the Hecke algebra of type F_4* , Manuscripta Math. **70** (1991), no. 3, 285–306.
- [9] Meinolf Geck and Götz Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs. New Series, vol. 21, The Clarendon Press Oxford University Press, New York, 2000.
- [10] Akihiko Gyoja, *On the existence of a W -graph for an irreducible representation of a Coxeter group*, J. Algebra **86** (1984), no. 2, 422–438.
- [11] Akihiko Gyoja and Katsuhiko Uno, *On the semisimplicity of Hecke algebras*, J. Math. Soc. Japan **41** (1989), no. 1, 75–79.
- [12] Robert B. Howlett and Yunchuan Yin, *Induced W -graphs*, preprint (2003).
- [13] ———, *Inducing W -graphs*, Math. Z. **244** (2003), no. 2, 415–431.

- [14] David Kazhdan and George Lusztig, *Representations of Coxeter groups and Hecke algebras*, *Invent. Math.* **53** (1979), no. 2, 165–184.
- [15] Michel Ringe, *The C MatAze*, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, 2004.

Commutativity of Hecke algebras associated with p -nilpotent groups and their Sylow p -subgroups

二宮 晏 (信州大学理学部)

夫馬 道卓 (信州大学大学院工学系研究科)

1 序文

群環の自然な拡張となっているヘッケ環の可換性の判定は知られていない。そこで、複素数体 \mathbb{C} 上のヘッケ環の可換性を置換指標の multiplicity-free 性を考察する事により考える。有限群 G とその部分群 H に対して、 \mathbb{C}_H を自明な H -加群、 $(\mathbb{C}_H)^G$ をその誘導加群としたとき、ヘッケ環 $\text{End}_{\mathbb{C}[G]}((\mathbb{C}_H)^G)$ は半単純環である事が知られている。よってヘッケ環 $\text{End}_{\mathbb{C}[G]}((\mathbb{C}_H)^G)$ が可換である事と $(\mathbb{C}_H)^G$ に対応する置換指標 $(1_H)^G$ が multiplicity-free であることが同値である。ここでは、有限群 G が半直積の場合の置換指標の multiplicity-free 性を考察し、とくに G が p -べき零群でシロー p -部分群 H の位数が p である場合の置換指標 $(1_H)^G$ が multiplicity-free になる G の構造を決定する。

2 定義と準備

ここでは G は有限群とし、考える体はすべて複素数体 \mathbb{C} であるとする。

定義 2.1 群 G の部分群 H に対して、 1_H で自明な H -指標を表し、 $(1_H)^G$ で 1_H の G への誘導指標を表す。この $(1_H)^G$ を置換指標と言う。

定義 2.2 G -指標が multiplicity-free であるとは、その指標を既約な G -指標へと分解したときの既約指標がすべて異なることである。

複素数体上ではヘッケ環は半単純環になるので、ヘッケ環 $\text{End}_{\mathbb{C}[G]}((\mathbb{C}_H)^G)$ が可換になることと置換指標 $(1_H)^G$ が multiplicity-free になることが同値である。ここでは $G = N \rtimes H$ となっている場合を考察する。 $G = N \rtimes H$ のときヘッケ環 $\text{End}_{\mathbb{C}[G]}((\mathbb{C}_H)^G)$ は群環 $\mathbb{C}[N]$ と同型になっているので、 H の N への作用は非自明であるとする。 N がアーベル群のときヘッケ環は可換になっている ([7], 補題 6.4) ので N は非アーベル群であるとする。

3 $G = N \rtimes H$ のとき

N の部分群と H の部分群に対して、 $(1_H)^G$ の multiplicity-free 性に関して次の補題が得られる。

補題 3.1 $G = N \rtimes H$ とする。

- (1) K を H -不変な N の正規部分群とする。 $X = KH$, $Y = (N/K)H$ とする。このとき $(1_H)^G$ が multiplicity-free ならば $(1_H)^X$ と $(1_H)^Y$ は multiplicity-free である。
- (2) T を H の部分群とする。このとき $(1_T)^{NT}$ が multiplicity-free ならば $(1_H)^G$ も multiplicity-free である。

N が中心積に分解されているときに, $(1_H)^G$ の multiplicity-free 性に関して次の補題が得られる.

補題 3.2 C を H が自明に作用するアーベル群とし, $G = (C * N) \rtimes H$ とする. このとき N が H -不変で $(1_H)^{NH}$ が multiplicity-free ならば $(1_H)^G$ も multiplicity-free である.

4 $G = N \rtimes H$, H がアーベル群のとき

H がアーベル群のとき, 次の補題が得られる. この補題はさらに $(1_H)^G$ の multiplicity-free 性を考えていく上で重要であり, また, 指標表が与えられたときに $(1_H)^G$ が multiplicity-free であるかを容易に判定するのを可能にする.

補題 4.1 $G = N \rtimes H$, H がアーベル群であるとする. このとき次は同値である.

- (1) $(1_H)^G$ は multiplicity-free である.
- (2) すべての既約な G -指標 χ に対して, $\chi|_H$ は multiplicity-free である.
- (3) すべての既約な H -指標 λ に対して, $(\lambda)^G$ は multiplicity-free である.

特に, このとき, すべての既約な G -指標 χ に対して, $\chi(1) \leq |H|$ である.

5 $G = N \rtimes H$, $|H| = p$ のとき

$|H| = p$ のとき, 既約な G -指標は, 既約な N -指標の G への拡張か誘導指標として得られる. その事に関して次の補題が得られる.

補題 5.1 $G = N \rtimes H$, $|H| = p$ とする. このとき $(1_H)^G$ が multiplicity-free ならばすべての 1 次でない既約な N -指標は G へ拡張可能である.

この補題から次のように degree set に関する条件が得られる.

系 5.2 $G = N \rtimes H$, $|H| = p$ とし N を非アーベル群とする. $(1_H)^G$ が multiplicity-free のとき, $\text{cd } G \subseteq \text{cd } N \cup \{p\}$ かつ, すべての $\text{cd } N$ の元は p 以下である. さらに $(|N|, |H|) = 1$ ならば $\text{cd } G = \text{cd } N \cup \{p\}$ かつ, すべての $\text{cd } N$ の元は p より小さい.

この系から $|H| = 2$ のときの同値な条件が得られる.

系 5.3 $G = N \rtimes H$, $|H| = 2$ で $(|N|, 2) = 1$ のとき, $(1_H)^G$ が multiplicity-free であることと N がアーベル群であることは同値である.

6 $G = N \rtimes H$, $|H| = p$, $(|N|, p) = 1$ のとき

以下では, $(|N|, p) = 1$ とする. すなわち G は p -べき零群でシロー p -部分群 H は位数 p の巡回群であるとする.

注意 6.1 I. M. Isaacs は論文 [6] において, $G = N \rtimes H$ で H は非自明に N に作用し, $(|N|, |H|) = 1$ とする. このとき H の作用ですべての 1 次でない既約な N -指標を固定するならば N はべき零群である事を示している. したがって補題 5.1 より $(1_H)^G$ が multiplicity-free のとき N はべき零群, とくに G は可解群である.

まず, 伊藤の定理と Glauberman 対応を紹介する.

定理 6.2 (伊藤の定理, [5]) G を可解な n 次の線形群とし, $p \geq n+1$ を素数とする. G のシロー p -部分群が正規部分群でないとき, $p = n+1$ となり n は 2 べきである.

定理 6.3 (Glauberman 対応, [5]) $G = N \rtimes H$ で H が可解で $(|N|, |H|) = 1$ とする. このとき, 自然な全単射

$$\pi(N, H) : \text{Irr}_H(N) \longrightarrow \text{Irr}(C_N(H))$$

が一意的に定まる. ここで, $\text{Irr}_H(N)$ は $\{\chi \in \text{Irr}(N) \mid \chi^h = \chi, \forall h \in H\}$ である.

まず, 伊藤の定理を用いる事により N の degree set の条件が得られる.

補題 6.4 $G = N \rtimes H$, $|H| = p$, $(|N|, p) = 1$ とする. このとき $(1_H)^G$ が multiplicity-free ならば $\text{cd } N = \{1, p-1\}$ であり, $p-1$ は 2 べきである. とくに p はフェルマー素数である.

この補題と Glauberman 対応を用いて N の構造を決定する事ができる.

補題 6.5 $G = N \rtimes H$, $|H| = p$, $(|N|, p) = 1$ とする. このとき $(1_H)^G$ が multiplicity-free ならば $C_N(H) = Z(N) = Z(G)$ で $N/Z(N)$ は位数 $(p-1)^2$ のアーベル 2-群である.

これらから, p -べき零群でシロー p -部分群 H の位数が p のときの multiplicity-free になる群の構造を決定づけることができる.

定理 6.6 群 G が p -べき零群で, そのシロー p -部分群 H が位数 p の巡回群であるとする. すなわち $G = N \rtimes H$ で $|H| = p$ かつ $(|N|, p) = 1$. このとき次の 2 つの条件は同値になる.

- (1) $(1_H)^G$ は multiplicity-free である.
- (2) p はフェルマー素数であり, N は semi-extraspecial 2-群 M で $|M/Z(M)| = (p-1)^2$ となるものとアーベル群 C との中心積になる. H は $M/Z(M)$ に正則に作用し, かつ $Z(M)$ と C には自明に作用する.

ここにできた semi-extraspecial p -群とは次のようなものである.

定義 6.7 G が semi-extraspecial p -群とは, 任意の $Z(G)$ の極大部分群 K に対して, G/K が extraspecial p -群になる群のことである ([1]).

注意 6.8 上の定理の (2) から (1) の証明は, [3] の定理 17.13 において, N を extraspecial p -群とし, H を位数が $|N|$ と互いに素な N の自己同型群の巡回部分群とする. このとき $G = N \rtimes H$ としたときの既約指標を決定していることからわかる.

$p = 3$ と $p = 5$ のときの例を紹介する.

例 6.9 $G = N \rtimes H$ で $|H| = 3$ かつ $(|N|, 3) = 1$. このとき, 定理 6.6 より M は位数 8 の extraspecial 2-群であり, そのうち位数 3 の非自明な作用が存在するのは Q_8 のみである. よって $G = (C \rtimes Q_8) \rtimes H$, C は H が自明に作用するアーベル群となる. 逆に, この群が multiplicity-free であることは指標表 ([4], 例 7.9) と補題 4.1 からわかる.

定理では semi-extraspecial 2-群である事を示したが, 実際に semi-extraspecial 2-群で multiplicity-free になる例を紹介する.

例 6.10

$$\begin{aligned}
 M &= \langle g_1, g_2, g_3, g_4 \rangle : \\
 g_1^4 &= g_2^4 = 1, g_1^2 = g_4^2, g_2^2 = g_3^2, g_1^{-1} g_2 g_1 = g_2 g_1^2, \\
 g_1^{-1} g_3 g_1 &= g_3 g_2^2, g_1^{-1} g_4 g_1 = g_4 g_1^2 g_2^2, g_2^{-1} g_3 g_2 = g_3 g_1^2 g_2^2, \\
 g_2^{-1} g_4 g_2 &= g_4 g_1^2, g_3^{-1} g_4 g_3 = g_4
 \end{aligned}$$

とすると, $Z(M) = \langle g_1^2, g_2^2 \rangle$ で $Z(M)$ の極大部分群 $\langle g_1^2 \rangle$, $\langle g_2^2 \rangle$, $\langle g_1^2 g_2^2 \rangle$ に対して

$$M / \langle g_1^2 \rangle \cong M / \langle g_2^2 \rangle \cong M / \langle g_1^2 g_2^2 \rangle \cong Q_8 * D_8$$

となっている. よって M は semi-extraspecial 2-群である. $H = \langle \sigma \mid \sigma^5 = 1 \rangle$ とし, $G = M \rtimes H$ を次のように定義する:

$$\begin{aligned}
 \sigma^{-1} g_1 \sigma &= g_1 g_3, & \sigma^{-1} g_2 \sigma &= g_1 g_2 g_3 g_4, \\
 \sigma^{-1} g_3 \sigma &= g_2, & \sigma^{-1} g_4 \sigma &= g_1 g_2 g_4.
 \end{aligned}$$

このとき G は 15 個の 1 次でない既約な指標を持ちそれらの degree はすべて 4 である. これらの H 上での指標の値は次の 5 つのタイプである.

	1	σ	σ^2	σ^3	σ^4
4	-1	-1	-1	-1	-1
4	- ζ	- ζ^2	- ζ^3	- ζ^4	
4	- ζ^2	- ζ^4	- ζ	- ζ^3	
4	- ζ^3	- ζ	- ζ^4	- ζ^2	
4	- ζ^4	- ζ^3	- ζ^2	- ζ	

ζ は 1 の原始 5 乗根. 補題 4.1 より $(1_H)^G$ が multiplicity-free であることがわかる.

参考文献

- [1] B. Beisiegel, Semi-Extraspezielle p -Gruppen, *Math. Z.* **156** (1977) 247-254.
- [2] M. Fuma and Y. Ninomiya, Finite groups with multiplicity-free permutation characters, to appear.
- [3] B. Huppert, *Endliche Gruppen I* (Springer-Verlag, Berlin, Heidelberg, New York, 1967).
- [4] B. Huppert, *Character Theory of Finite Groups* (Walter de Gruyter, Berlin, New York, 1998).

- [5] I. M. Isaacs, *Character Theory of Finite Groups* (Academic Press, 1976).
- [6] I. M. Isaacs, Coprime group actions fixing all nonlinear irreducible characters, *Can. J. Math.* 41 (1989) 68–82.
- [7] A. Krieg, *Hecke Algebras* (Mem. Amer. Math. Soc. 435, 1990).

