# 第 22 回代数的組合せ論シンポジウム 報告集

2005 年 6 月 27 日 ～ 29 日
於 愛媛大学 総合情報メディアセンター

平成 17 年度文部科学省科学研究費基盤研究 (B)
課題番号 16340010　研究代表者 坂内英一

# まえがき

この報告集は 2005 年 6 月 27 日から 6 月 29 日にわたり, 愛媛大学総合情報メディアセンターで行なわれた「第 22 回代数的組合せ論シンポジウム」の講演記録です。25 名の講演者によって 21 の講演が行なわれ, 約 60 名の参加者があり盛会でした。

この報告集の作成と一部講演者の旅費は

平成 17 年度文部科学省科学研究費基盤研究 (B)
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。講演者の方々, 参加者の方々, 会場設営を手伝ってくれた愛媛大学の学生諸君, そしてこの研究集会にご協力いただいたすべての方々に, この場を借りてお礼を申し上げます。

2006 年 1 月　愛媛大学理学部
佐々木洋城, 安部利之, 庭崎隆

# 第 22 回代数的組合せ論シンポジウム

日程　2005 年 6 月 27 日 (月) - 6 月 29 日 (水)
会場　愛媛大学総合情報メディアセンター 1 階 メディアホール

## プログラム

### 6 月 27 日 (月)

9:30–10:00　野崎寛 (九州大学大学院数理学府)
A note on odd unimodular Euclidean lattices

10:10–10:40　坂内英一 (九州大学大学院数理学研究院)
A note on integral Euclidean lattices in dimension 3

11:00–11:40　坂内悦子 (九州大学大学院数理学研究院)
On antipodal Euclidean tight $(2e+1)$-designs

11:50–12:20　奥山京 (大分大学工学部)
Purifiability in pure subgroups

13:50–14:50　松尾厚 (東京大学大学院数理科学研究科)
企画講演「Quasi-finiteness of vertex operator algebras」

15:10–15:40　安部利之 (愛媛大学理学部)
A $Z_2$-orbifold model of symplectic fermionic vertex operator superalgebra

15:50–16:20　田辺顕一朗 (筑波大学大学院数理物質科学研究科),
山田裕理 (一橋大学大学院経済学研究科)
The fixed point subalgebra of a lattice vertex operator algebra by an automorphism of order three

16:30–17:00　山内 博 (東京大学大学院数理科学研究科・学振特別研究員)
McKay's observation and vertex operator algebras generated by two conformal vectors of central charge 1/2

### 6 月 28 日 (火)

9:30–10:00　芦原崇裕 (筑波大学大学院数理物質科学研究科)
ジョルダン代数と頂点作用素代数

10:10–11:10　宮本雅彦 (筑波大学数学系)
企画講演「On the order of a group of even order」

11:30–12:10　北詰正顕 (千葉大学理学部), 千吉良直紀 (室蘭工業大学),
原田昌晃 (山形大学理学部)
有限置換群と自己直交符号

12:20–12:50　原田昌晃 (山形大学理学部)
On a 5-design related to an extremal doubly-even self-dual code

14:10–14:40 Sejeong Bang (九州大学大学院数理学研究院)
Delsarte clique graphs

14:50–15:20 秋山献之 (福岡大学理学部), 末竹千博 (大分大学工学部)
$STD_{\frac{k}{3}}[k;3]'s$

15:40–16:10 平峰豊 (熊本大学教育学部)
位数 $p^4$ の可換 $p$-群における半正則相対差集合について

16:20–17:00 木村浩 (上武大学ビジネス情報学部)
アダマール行列について

18:00–20:00 懇親会

**6 月 29 日 (水)**

10:00–11:00 吉荒聡 (東京女子大学文理学部)
企画講演「高次元の双対弧 — 平面上の二次曲線の高次元化」

11:10–11:40 南部奈緒 (東京女子大学大学院理学研究科)
Examples of dimensional dual hyperovals of polar type

11:50–12:20 谷口浩朗 (詫間電波工業高等専門学校)
On dimensional dual hyperoval $S^{d+1}_{\sigma,\phi}$

13:50–14:20 川原行人 (東京都立大学理学研究科・学振特別研究員)
Arrangements of hyperplanes constructed from Latin hypercubes

14:30–15:00 縫田光司 (東京大学大学院数理科学研究科・学振特別研究員)
Coxeter 群の同型問題, 直既約性と自己同型群について

## 懇親会

日時　2005 年 6 月 28 日 (火) 18:00 – 20:00
会場　愛媛大学 大学会館 2 階 生協食堂リーセス
会費　5000 円 (学生 2000 円)

ご参加いただける方は 6 月 21 日 (火) までに下記世話人のいずれかへご連絡下さい。

その他, 会場施設などの詳細は第 22 回代数的組合せ論シンポジウムのホームページをご覧下さい : http://www.math.sci.ehime-u.ac.jp/ac2005/

世話人・連絡先

〒 790-8577　松山市文京町 2-5 愛媛大学理学部数学科

佐々木洋城　(sasaki@math.sci.ehime-u.ac.jp)
安部利之　(abe@math.sci.ehime-u.ac.jp)
庭崎隆　(niwasaki@dpc.ehime-u.ac.jp)

# A note on odd unimodular Euclidean lattices

野崎　寛

九州大学数理学府
ma204018@math.kyushu-u.ac.jp

**概要**

任意の奇素数 $p$ に対して、任意の odd unimodular Euclidean lattice のテータ級数が $p$ を法として 1 と合同にならないことを示す。

## 1 Introduction

$R^n$ の even unimodular lattice については、そのテータ級数が奇素数 $p$ を法として 1 と合同になる多くの例が知られている。例えば Bayer-Fluckiger [1]、Dummigan and Tiep [2] などを参照されたい。次の問題は、坂内英一先生を通して、田口雄一郎先生から頂いた問題である。

**Problem 1.1.** $n$ を奇数、$p$ を奇素数とする。$\Lambda \subset R^n$ を *unimodular lattice* とする。次の条件を満たす $\Lambda$ が存在するか。

$$\Theta_\Lambda \equiv 1 \pmod{p}$$

この条件を満たす lattice が存在すれば、良いガロア表現が見つかる。しかし、田口先生は Koblitz [5, pages 202-203] の論文により、そのような lattice は存在しないということを確かめられている。しかし、その証明は Katz と Kohnen の深い結果に依存しているため非常に難しい。ここでは、この問題について、非常に単純で初等的な証明を与えることを目的とする。

$n$ が 8 の倍数のときのみ even unimodular lattice が存在するという有名な結果があるから、$n$ が奇数のときは、unimodular lattice は odd になる。よって problem　1.1. は次のように一般的に簡単に書き直される。

**Theorem 1.1.** $p$ を任意の奇素数とする。そのとき、$p$ を法として 1 と合同になるテータ級数を持つ *odd unimodular lattice* は存在しない。

## 2 Preliminaries

まず最初に、いくつかの定義を述べる。

lattice $\Lambda \subset R^n$ の dual とは、$\Lambda^\#$ と表し次の様なものである。

$$\Lambda^\# := \{y \in R^n \mid \langle y \mid x\rangle \in \mathbb{Z}, \forall x \in \Lambda\}$$

$(* \mid *)$ は標準の内積を表す。lattice $\Lambda$ が integral と呼ばれるのは、$\Lambda$ の任意の二つの元の内積が整数になるときであり、つまり $\Lambda \subset \Lambda^\#$ を満たすときである。integral lattice $\Lambda$ が even と呼ばれるのは、$\Lambda$ の任意の元 $x$ について、$\langle x \mid x\rangle$ が偶数になるときである。それ以外は odd と呼ばれる。つまり、自身との内積が偶数になるものと、奇数になるものが入り混じった場合も odd と呼ばれる。integral lattice が selfdual (もしくは unimodular) と呼ばれるのは、$\Lambda^\# = \Lambda$ を満たすときである。selfdual lattice $\Lambda$ の shadow $S(\Lambda)$ は次のように定義される。

$$S(\Lambda) = \begin{cases} \Lambda, & \Lambda \text{ が even} \\ \Lambda_0^\# \setminus \Lambda, & \Lambda \text{ が odd} \end{cases}$$

このとき、$\Lambda_0 = \{x \in \Lambda \mid \langle x \mid x\rangle \equiv 0 \bmod 2\}$。
$q := e^{\pi i z}$ とおく。

$$\theta_3(z) := \sum_{m\in\mathbb{Z}} q^{m^2} = 1 + 2q + 2q^4 \cdots$$

$$\theta_2(z) := \sum_{m\in\mathbb{Z}+\frac{1}{2}} q^{m^2} = 2q^{\frac{1}{4}}(1 + q^2 + \cdots)$$

$$\theta_4(z) := \sum_{m\in\mathbb{Z}} (-q)^{m^2} = 1 - 2q + 2q^4 - \cdots$$

lattice $\Lambda$ のテータ級数は次のように定義される。

$$\Theta_\Lambda(z) := \sum_{x\in\Lambda} q^{\langle x|x\rangle}$$

次に、必要な定理をいくつかあげる。

**Theorem 2.1.** (*Dummigan-Tiep [2, Theorem 3.2]*)
$p$ を素数、$\varphi$ をオイラー関数とする。$M = l\varphi(p)$ は次のように定義される。
(1) $p \equiv 1 \pmod 4$ のとき、$M = 2\varphi(p)$
(2) $p \equiv 3 \pmod 4$ のとき、$M = 4\varphi(p)$
そのとき、$\Theta_\Lambda \equiv 1 \pmod p$ を満たす、ランク $M$ の *even unimodular lattice* $\Lambda$ が存在する。

**Theorem 2.2.** (*Hecke, Conway-Sloane [4, pages 187-188]* 参照 )
$\Lambda$ がランク $n$ の *unimodular lattice* であるとき、そのテータ級数は

$$\Theta_\Lambda = \theta_3^n + c_1\theta_3^{n-8}\Delta_8 + \cdots + c_{\lfloor n/8\rfloor}\theta_3^{n-8\lfloor n/8\rfloor}\Delta_8^{\lfloor n/8\rfloor}$$

と書き表せる。このとき $c_i$ は整数で、$\Delta_8(z)$ は次の様なものである。

$$\Delta_8(z)=\frac{1}{16}\theta_2(z)^4\theta_4(z)^4=q\prod_{m=1}^{\infty}\{(1-q^{2m-1})(1-q^{4m})\}^8$$

**Theorem 2.3.** (*Pache [3, Proposition 13]*)
*Theorem 2.2.* をさらに詳しくし、

$$\Theta_\Lambda=\theta_3^n+c_1\theta_3^{n-8}\Delta_8+\cdots+c_k\theta_3^{n-8k}\Delta_8^k$$

このとき $k=\frac{1}{8}(n-\sigma(\Lambda))$ $(\sigma(\Lambda):=4\min\{(x\,|\,x\rangle\mid x\in S(\Lambda)\})$。さらに $c_k=(-1)^k2^{-n+12k}|S(\Lambda)_{(n-8k)/4}|$ であり、$S(\Lambda)_m:=\{x\in S(\Lambda)\mid (x\,|\,x\rangle=m\}$。

これらの結果を、Theorem1.1. の証明に使いやすいように、ひとつの proposition にまとめる。

Theorem 2.1. において、$\varphi(p)=p-1$ であるから、

$$M=\begin{cases}8t, & p=4t+1\text{ のとき},t\in\mathbb{N}\\ 8(2t-1), & p=4t-1\text{ のとき},t\in\mathbb{N}\end{cases}$$

任意の $p$ について、$\Theta_\Lambda\equiv 1\pmod p$ となるようなランク $M$ の even unimodular lattice $\Lambda$ が存在する。$\Lambda$ は unimodular lattice であるから、整数 $c_i$ が存在し、

$$\Theta_\Lambda=\theta_3^M+c_1\theta_3^{M-8}\Delta_8+\cdots+c_k\theta_3^{M-8k}\Delta_8^k$$

と書ける。このとき、Theorem 2.3. により $\sigma(\Lambda)=M-8k$。また、
$c_k=(-1)^k2^{-M+12k}|S(\Lambda)_{(M-8k)/4}|$。
さらに $\Lambda$ は even であるから、$S(\Lambda)=\Lambda$ であり、$\sigma(\Lambda)=0$。ゆえに、
$c_k=(-1)^k2^{-M+12k}|\Lambda_0|=(-1)^k2^{-M+12k}$。
(1)$p=4t+1$ のとき、$M=8t$。$\sigma(\Lambda)=M-8k=0$ だから、$k=t$ である。
よって、 $c_k=(-1)^t2^{4t}=(-1)^t2^{p-1}\equiv(-1)^t\pmod p$。
(2)$p=4t-1$ のとき、$M=8(2t-1)$。$\sigma(\Lambda)=M-8k=0$ だから、$k=2t-1$ である。よって、
$c_k=(-1)^{2t-1}2^{8t-4}=-2^{2(p-1)}\equiv-1\pmod p$。
以上をまとめると、次の proposition が得られる。

**Proposition 2.1.** $p$ を奇素数とし、その $p$ に対して、$M:=4\varphi(p)$ と定義する。

$$\Theta_\Lambda=\theta_3^M+c_1\theta_3^{M-8}\Delta_8+\cdots+c_{M/8}\Delta_8^{M/8}\equiv 1\pmod p$$

を満たすランク $M$ の *even unimodular lattice* $\Lambda$ が存在する。このとき、$c_i$ は整数であり、特に $c_{M/8}\not\equiv 0\pmod p$。$M/8$ も整数。

ここでは、$M := 4\varphi(p)$ と定義されているが、Theorem 2.1. では、$p = 4n+1$ のとき、$\Lambda$ のランクは $2\varphi(p)$ であった。このとき、$\Theta_{\Lambda\oplus\Lambda} = {\Theta_\Lambda}^2 \equiv 1 \pmod p$ であり、$\Lambda \oplus \Lambda$ はランク $4\varphi(p)$ の even unimodular lattice である。 よって、proposition のように、まとめることができる。

## 3 Proof of Theorem 1.1.

Theorem 1.1. を証明するために、以下の2つの結果を証明する。Theorem 3.1. はランク $n$ が8で割り切れない場合であり、Theorem 3.2. はランク $n$ が8で割り切れる場合である。Theorem 3.1. は lattice の存在に依存しない。

**Theorem 3.1.** *$n$ を8で割り切れない整数とし、$p$ を奇素数とする。$a_0 = 1$、$a_i$ を整数とするとき、*

$$\sum_{i=0}^{[n/8]} a_i\, \theta_3^{n-8i} \Delta_8^i \equiv 1 \pmod p$$

*となるような、$\{a_0, a_1, \cdots, a_{[n/8]}\}$ は存在しない。*

*Proof.* 背理法により示す。

$$\Theta_\Lambda = \theta_3^n + a_1\, \theta_3^{n-8}\Delta_8 + \cdots + a_{[n/8]}\, \theta_3^{n-8[n/8]} \Delta_8^{[n/8]} \equiv 1 \pmod p$$

となるような $\{a_1, \cdots, a_{[n/8]}\}$ が存在すると仮定する。$n$ は8で割り切れるから、$n - 8[n/8] \neq 0$。

Proposition 2.1 より、

$$\Theta_{\Lambda'} = \theta_3^M + c_1\, \theta_3^{M-8}\Delta_8 + \cdots + c_{M/8}\, \Delta_8^{M/8} \equiv 1 \pmod p$$

となるようなランク $M$ の even unimodular lattice $\Lambda'$ が存在する。このとき、$c_i$ は整数であり、$c_{M/8} \not\equiv 0 \pmod p$。そして次のような計算をする。

$${\Theta_{\Lambda'}}^n - {\Theta_\Lambda}^M = b_1\, \theta_3^{Mn-8}\Delta_8 + b_2\, \theta_3^{Mn-16}\Delta_8^2 + \cdots + b_{Mn/8}\, \Delta_8^{Mn/8} \equiv 0 \pmod p$$

このとき $b_i$ は整数。$\theta_3^{Mn-8i}\Delta_8^i = q^i(1 + \cdots)$ だから、まず $q$ の係数を0と合同にしようとすると、$b_1 \equiv 0$ でなければならない。同様に、順に考えていくと、$b_2 \equiv 0, \cdots, b_{Mn/8} \equiv 0 \pmod p$ でなければならい。しかし、これは $b_{Mn/8} = (c_{M/8})^n \not\equiv 0 \pmod p$ に矛盾している。 □

**Theorem 3.2.** *$n$ を8で割り切れる整数とし、$p$ を奇素数とする。ランク $n$ の任意の odd unimodular lattice $\Lambda$ に対して、*

$$\Theta_\Lambda = \sum_{i=0}^{k} a_i\, \theta_3^{n-8i} \Delta_8^i \not\equiv 1 \pmod p$$

*このとき $a_0 = 1$、$a_i$ は整数であり、$k = \frac{1}{8}(n - \sigma(\Lambda))$。*

*Proof.* $\sigma(\Lambda)=0$ となるのは、$\Lambda$ が even のときのみである。それゆえ、$\Lambda$ が odd のときは $\sigma(\Lambda)=n-8k\neq 0$。残りの証明は Theorem 3.1. と同様。 □

**Acknowledgements.** この問題を与えてくださり、たくさんの情報を与えて下さった、坂内英一先生に感謝します。また、坂内先生を通してこの問題がテータ級数のレベルで解けないかと、提案してくださった Boris Venkov 氏にも感謝いたします。

## 参考文献

[1] E. Bayer-Fluckiger: "Definite unimodular lattices having an automorphism of given characteristic polynomial ", Comment. Math. Helvetici **59** (1984), 509-538

[2] Neil Dummigan and Pham Huu Tiep: "Congruences for Certain Theta Series", Journal of Number Theory **71**,86-105(1998).

[3] Claude Pache: "Shells of selfdual lattices viewed as spherical designs", (2004), preprint.

[4] J.H.Conway, N.J.A.Sloane: "Sphere Packings, Lattices and Groups", third edition, (1999).

[5] Neal Koblitz: "$p$-Adic Congruences and Modular Forms of Half Integer Weight", Math. Annalen **274** (1986), 199-220.

# A note on integral Euclidean lattices of dimension 3

Eiichi Bannai （坂内英一・九大数理）

Faculty of Mathematics, Graduate School,
Kyushu University

## 1 Introduction

この原稿は愛媛での第２２回代数的組合せ論シンポジウムの報告集のための原稿です。講演のOHPシートをほぼ忠実にTex化したものです。講演の時にOHPシートに書いた図はうまくTex化できなかったので省略してしまいましたが。詳細は4ページの短い論文[1]としてArch. Math. で印刷中ですので、そちらを参照して下さい。

格子 $\Lambda$ が integral であるとは、$(x,y) \in \mathbb{Z}, \forall x,y \in \Lambda$ であることと定義されます。このとき、$\Lambda$ のテーター級数は

$$\Theta_\Lambda = \sum_{i=0}^{\infty} a_i q^i$$

$$a_i = |\{x \in \Lambda | (x,x) = i\}|$$

で定義されます。
奇素数 $p$ に対して、$\Theta_\Lambda \equiv 1 \pmod p$ であるとは、$p|a_i$ $(i = 1,2,\cdots)$ であることと定義されます。($a_0 = 1$ に注意。)

今回の講演の主結果は次の定理です。

**定理 1** 任意の奇素数 $p$ に対して、$\Lambda$ を $\mathbb{R}^3$ の任意の integral lattice とすると、$\Theta_\Lambda \not\equiv 1 \pmod p$ である。

この定理の背景は次の通りです。この愛媛のシンポジウムで野崎寛君が次の結果について講演しました。[3] 参照。

**Theorem** （野崎寛） 任意の奇素数 $p$ と任意の奇数 $n$ に対して、$\Lambda$ を $\mathbb{R}^n$ の任意の unimodular lattice とすると、$\Theta_\Lambda \not\equiv 1 \pmod p$ である。
(さらに強く、任意の $n$ に対して $\mathbb{R}^n$ の任意の odd unimodular lattice に対して $\Theta_\Lambda \not\equiv 1 \pmod p$ が成立つことも示されている。)

この問題は、もともとは田口雄一郎（九大数理）氏による「奇素数 $p$ と奇数 $n$ に対して、$\Theta_\Lambda \equiv 1 \pmod p$ となる unimodular lattice $\Lambda$ in $\mathbb{R}^n$ は存在するか？」という質問

から発生しました。そのようなことは起きないというのがその解答でした。それならば、「unimodular の条件を弱めて、integral に置き換えたらどうなるか?」というのが田口氏の次の質問でした。$n=3$ の場合にはそのようなことは起きないというのが、この講演の主結果（定理1）です。$n \geq 5$ の場合にはまだ未解決であることに注意して下さい。

## 2 定理1の証明の概略

以下、次の記号を用いることにします。

$\Lambda$ = integral lattice in $\mathbb{R}^n$
$S_i = S_i(\Lambda) = \{x \in \Lambda | (x,x) = i\}$,
$s_i = \frac{1}{2}|S_i(\Lambda)| (= \frac{1}{2}a_i)$,
$m = \text{Min}\ \{(x,x) | x \in \Lambda \backslash \{0\}\}$.
So, $S_m$ = the set of min. vectors in $\Lambda$.

J. Martinet [2] は $\Lambda/2\Lambda$ (および $\Lambda/3\Lambda$), の representatives について考察し、次の定理を得た。

**Theorem (Martinet, Theorem 2.1 in [2])**

$$\sum_{0<k<2m} s_k + \sum_{x \in S_{2m} \bmod 2\Lambda} \frac{1}{l(x)} \leq 2^n - 1.$$

ここで $l(x)$ = the number of lines containing a vector $y \in S_{2m}$ with $y \equiv x \bmod 2\Lambda$ で与えられ、$1 \leq l(x) \leq n$ である。

更に、ここで、norm $N \leq 2m$ の ベクトル達が $\Lambda/2\Lambda$ において異なるクラスを表すのは、$(x,-x)$ の場合、あるいは $x,y$ がお互いに直交する norm $2m$ のベクトルである場合に限る。(Martinet [2, Theorem 3.1].)

**Corollary (Martinet, Theorem 2.3 in [2])**

$$\sum_{0<k<2m} s_k + \frac{1}{n} s_{2m} \leq 2^n - 1.$$

ここで等号のなりたつのは、
norm $2m$ のベクトル達が $2n$ 個あって、$n$ 本のお互いに直交する直線上にのっているようになっている場合に限る。

以上の準備のもとに、定理1の証明に入る。まず、
$\Lambda$ が $\mathbb{R}$ 3 の integral lattice で, $\Theta_\Lambda \equiv 1 \pmod p$ ならば $p=3$ となることを示す。
証明。$p \geq 5$ ならば $p | s_m$ であり、$|S_m| \geq 10$ である、従って、$\exists x, y \in S_{2m}$ with $(x,y) > 0$ (and $(x,y) \neq m'$.) 従って、$x-y \in S_m$ with $m < m' < 2m$. このとき、$s_m + s_{m'} + \frac{s_{2m}}{3} \leq 2^n - 1 (= 7, \text{if } n=3)$ がなりたたないので、上の Corollary (Martinet, Theorem 2.3 in [2])

に矛盾する。従って、$p=3$ でなければならない。従って、以下では常に $p=3$ を仮定する。

**定理 1 の証明の概略.** 次のように場合分けをする（$s_m=\frac{1}{2}|S_m|$ に注意。）
Case 1 ($s_m=6$)
Case 2 ($s_m=3$) (これは次の 2 つの Subcases 2A と 2B に分ける。)
Subcase 2A (The case $S_m$ generates $\mathbb{R}^2$.)
Subcase 2B (The case $S_m$ generates $\mathbb{R}^3$.)　(これは次の 3 つの Subcases (i), (ii), (iii) に分けられる。)
Subcase 2B(i) (The case $A(\Lambda)=\{m'\}$ with $m'\neq 2m$.)
Subcase 2B(ii) (The case $A(\Lambda)=\{2m\}$.)
Subcase 2B(iii) (The case $A(\Lambda)=\{m',2m\}$ with $m'\neq 2m$.)
ここで　$A(\Lambda)=\{(x-y,x-y)|x,y\in S_m, x\neq y,(x,y)\geq 0\}$ と定義する。Case 2B の場合には、$s_m=3$ なので、$m\notin A(\Lambda)$ であることに注意。)
　Case 1 ($s_m=6$)
この場合、kissing number $|S_m|=12$ となる。このような lattice は一意的に決まり、fcc lattice (face centred cubic lattice=$A_3$ 型ルート格子) となる。この格子 $\Lambda$ に対して $\Theta_\Lambda\not\equiv 1 \pmod p$ となる。

Case 2A　($s_m=3$, で $S_m$ が $\mathbb{R}^2$ を生成する場合.)
この場合、$S_m$ は hexagonal lattice $H(\subset\mathbb{R}^2)$ を生成するとして良い。$z\in\Lambda$ を $H$ に含まれていない、norm 最小 ($>m$) の元とする。このとき、この最小の norm の ($H$ の片側にある) ベクトルは、$z(=z_1), z_2, z_3$ の丁度 3 つであり、これらは $H$ を平行移動した $H+z$ の上に位置しなければならない、なぜならばそうでないとすると $\Theta_\Lambda\not\equiv 1 \pmod 3$ となるからである。このとき、 2 つの平面 $<H>, <H+z>$ の間に $\Lambda$ の元は存在しなくて、さらに、$H+z$ の norm 一定のベクトルの個数は 3 の倍数でなければならないことも示される。この議論は $H$ を平行移動した $H+z_1+z_2$ に対しても成立つ。このとき、$H\pm z_1, H\pm(z_1+z_2)$ の上にない norm $z_1+z_2+z_3$ を持つ ($H$ で切った空間の一方の半分にある) 元は一意的に決まり、$z_1+z_2+z_3$ と一致しなければいけないことがわかる。従って、$s_{(z_1+z_2+z_3, z_1+z_2+z_3)}$ は modulo 3 で 0 と合同にならないので、矛盾である。

Case 2B(i). ($s_m=3$ で $S_m$ は $\mathbb{R}^3$ を生成し、かつ $A(\Lambda)=\{m'\}$ with $m'\neq 2m$. の場合。)
今、$x_1,x_2,x_3$ を $S_m$ の代表元とする。必要なら $x_i$ を $-x_i$ で取り替えて、

$$(x_1,x_2)=(x_1,x_3)=(x_2,x_3)=\alpha,\ (m>|\alpha|>0)$$

と取ることが出来る。このとき、格子 $<x_1, x_1-x_2, x_1-x_3>=<x_1,x_2,x_3>$ は初等幾何的議論を用いて、saturated であることが示される。ここで saturated とは、格子の最小距離を減らすことなしに格子に元を付け加えることが出来ないことを意味する。このとき、$H=<x_1-x_2, x_1-x_3>$ は hexagonal lattice である。ここで、$z_i=x_i (i=1,2,3)$ と置いて Case2A と同様の議論を繰り返すと、$\Theta_\Lambda\not\equiv 1 \pmod 3$ となり、矛盾が得られる。

Case 2B(ii). ($s_m=3$ で $S_m$ は $\mathbb{R}^3$ を生成し、かつ $A(\Lambda)=\{2m\}$ の場合。)
このとき、representatives $x_1,x_2,x_3$ 達はお互いに直交している。従って $<x_1,x_3,x_3>\cong\mathbb{Z}^3$ saturated なので、$\Gamma=\mathbb{Z}^3$ である。このとき、$\Theta_\Lambda\not\equiv 1 \pmod 3$ となり、矛盾が得られる。

Case 2B(iii). ($s_m = 3$ で $S_m$ は $\mathbb{R}^3$ を生成し、かつ $A(\Lambda) = \{m', 2m\}$ with $m' \neq 2m$ の場合。)
今、$x_1, x_2, x_3$ を $S_m$ の代表元とする。このとき、次の2つの可能性のどちらかが起こらなければならない。
Case(a) $(x_1, x_2) = 0, (x_1, x_3) = (x_2, x_3) = \alpha > 0$,
Case(b) $(x_1, x_2) = (x_2, x_3) = 0$, $(x_1, x_3) = \alpha > 0$.

Case(a) の場合。
このとき、$s_m = s_{m'} = 3$ でなければならない。$3|s_{2m}$ なので、Martinet の系により、$s_{2m} = 3$ でなければならない。このとき、$y \in S_{2m}$ で $x_1, x_2$ (従って $x_1 - x_2, x_1 + x_2$ の)両方に直交するものが存在する。今、$x_3 \in < x_1 + x_2, y >$ だから、$x_3 = \frac{1}{2}(x_1 + x_2 + y)$ でなければならない。このとき、$\frac{1}{2}(x_1 + x_2 + y) - y \in S_m$ となり、これは $s_m > 3$ となり $s_m = 3$ に矛盾する。

Case(b) の場合。
$(x_1, x_2) = (x_2, x_3) = 0$ なので、$y \in S_{2m}$ で $x_1, x_2$ 両方に直交するものが存在する。従って、$x_3 \in < x_1, y >$ である。このことは、格子 $\Lambda$ の最小距離が減ってしまうことを意味し、矛盾が得られる。

以上から定理1の証明は完成した。

# References


[1] E. Bannai, A note on integral Euclidean lattices in dimension 3, to appear in Arch. Math. (2005).

[2] J. Martinet, Reduction modulo 2 and 3 of Euclidean lattices, J. of Algebra, 251 (2002), 864-887.

[3] H. Nozaki, A note on odd unimodular Euclidean lattices, to appear in Arch. Math.

# On antipodal Euclidean tight $(2e+1)$-designs

坂内悦子 (Etsuko Bannai)

九大・数理
(Faculty of Mathematics, Graduate School
Kyushu University)

Neumaier-Seidel の論文 (1988) において球面上の design の概念はユークリッド空間の design として一般化された. そして Delsarte-Seidel の論文 (1989) 等ユークリッド空間の design に関する論文がいくつか発表された. しばらく組合せ論的な発展があまりなっかったのであるが, 最近, 坂内英一との共同研究で Euclidean tight $2e$-design についていくつかの結果を得ることが出来 Euclidean designs の研究の手がかりが得られた. 講演では antipodal Euclidean tight $(2e+1)$-designs について最近得た結果を解説した.

## 球面上の $s$-distance sets

球面 $S^{n-1}=\{x=(x_1,\ldots,x_n)\in\mathbb{R}^n \mid \|x\|=\sum_{i=1}^n x_i^2=1\}$ 上の有限部分集合 $X$ に対して $A(X)=\{\|x-y\| \mid x,\, y\in X,\, x\neq y\}$ とする. $|A(X)|=s$ が成立つ時に $X$ を $S^{n-1}$ 上の $s$-距離集合と言う.

次の定理が知られている.

**定理 1. (Delsarte-Goethals-Seidel, 1977)**
$X$ を $S^{n-1}$ 上の $s$-距離集合とすると

$$|X|\leq \binom{n+s-1}{s}+\binom{n+s-2}{s-1}$$

が成立つ. さらに, $X$ が antipodal であれば

$$|X|\leq 2\binom{n+s-2}{s-1}$$

が成立つ. ここで, $-x\in X$ が全ての $x\in X$ に対して成立つ時に $X$ は antipodal であると言う.

## Spherical $t$-designs

Delsarte-Goethals-Seidel は spherical $t$-design の定義を次の様に与えた.

**定義 (Spherical $t$-design)**
有限部分集合 $X \subset S^{n-1}$ が $n$ 変数の高々$t$ 次の全ての多項式 $f(x)$ に対して次の等式を満たすならば $X$ を *spherical $t$-design* と呼ぶ.

$$\frac{1}{|S^{n-1}|}\int_{S^{n-1}} f(x)d\sigma(x) = \frac{1}{|X|}\sum_{x\in X} f(x).$$

ここで $\sigma$ は $S^{n-1}$ 上の Haar measure, そして $|S^{n-1}| = \int_{S^{n-1}} d\sigma(x)$ とする.

さらに彼等は spherical $t$-design $X$ に含まれる点の個数の下界について次の様な定理を証明している.

**定理 2. (Delsarte-Goethals-Seidel, 1977)**
(1) $X$ が spherical $2e$-design であれば

$$|X| \geq \binom{n+e-1}{e} + \binom{n+e-2}{e-1}$$

が成立つ.
(2) $X$ が spherical $(2e+1)$-design であれば

$$|X| \geq 2\binom{n+e-1}{e}$$

が成立つ.

**Note:**
(1) の不等式の右辺は定理 1 で示された球面上の $e$-distance set の点の個数の上界と等しい.
(2) の不等式の右辺は定理 1 で示された球面上の antipodal な $e$-distance set の点の個数の上界と等しい.

## Spherical tight designs

Spherical $2e$-design と spherical $(2e+1)$-design に対して不等式 (1) と 不等式 (2) において等式が成立っている時に, それぞれ tight spherical $2e$-design および tight spherical $(2e+1)$-design と呼ばれる.

Tight な designs と $s$-distance sets の間には次の定理が成立っている.

**定理 3 (Delsarte-Goethals-Seidel, 1977)**
(1) $|X| = \binom{n+e-1}{e} + \binom{n+e-2}{e-1}$ であれば $X$ が $e$-distance set である事と $X$ が $2e$-design である事は同値である.
(2) $|X| = 2\binom{n+e-1}{e}$ であれば $X$ が antipodal な $(e+1)$-distance set である事と $(2e+1)$-design である事は同値である.

球面 $S^{n-1}$ 上の spherical $t$-design は Seymour-Zaslavsky (1984) によって点の個数が十分大きければ任意の $n$ と $t$ に対して存在する事が証明されている. 彼等の証明は一般的な存在

定理であり具体的に構成する一般的な方法は知られていない．個々の特定な方法により色々な $t$-design の例が知られている．

次にユークリッド空間 $\mathbb{R}^n$ における $s$-distance sets と Euclidean $t$-deisgns の話に入りたいのだがその前に記号等の定義を少し与えておこう．

**Notation**

$X$ を $\mathbb{R}^n$ の有限部分集合とする．原点を中心とし $X$ と交わる球面が丁度 $p$ 個あるとし，それらを $\{S_1, S_2, \ldots, S_p\}$ とし $S = S_1 \cup S_2 \cup \cdots \cup S_p$ と置く．この時 $X$ は 同心球面 $S$ にサポートされていると言い同心球面 $S$ は $X$ のサポートと呼ぶ．以下にこれから使う記号を与える．ここで $\{0\}$ も球面の特別な場合として考える．すなわち $S_i = \{0\}$ となる可能性もあるとする．

- $r_i$ は $S_i$ の半径 $(1 \leq i \leq p)$．($r_i = 0$ も球面の特別な場合として含む．)
- $X_i := X \cap S_i$ $(1 \leq i \leq p)$ $(X = \cup_{i=1}^{p} X_i)$．
- $w$ は $X$ 上の正値 weight function $(w : X \longrightarrow \mathbb{R}_{>0})$．
- $w(X_i) := \sum_{x \in X_i} w(x)$.
- $\sigma_i$ は $S_i$ の Haar measure とし

$$|S_i| = \int_{S_i} d\sigma_i(x) = {r_i}^{n-1} |S^{n-1}|$$

が成立っているとする．
- $S_i = \{0\}$ に対しては積分は次の様に定義する．

$$\frac{1}{|S_i|} \int_{S_i} f(x) d\sigma_i(x) = f(0).$$

**Vector spaces of polynomials**

$\mathcal{P}(\mathbb{R}^n)$ を実数体上の $n$ 変数の全ての多項式が作るベクトル空間とする．

$$\begin{aligned}
&\mathcal{P}_e(\mathbb{R}^n) := \{f \in \mathcal{P}(\mathbb{R}^n) \mid \deg f \leq e\} \\
&\mathcal{P}_e(Y) := \{f|_Y \mid f \in \mathcal{P}_e(\mathbb{R}^n)\} \\
&\mathcal{P}_e^*(\mathbb{R}^n) := \{f \in \mathcal{P}_e(\mathbb{R}^n) \mid \deg f \equiv e \pmod 2\} \\
&\mathcal{P}_e^*(Y) := \{f|_Y \mid f \in \mathcal{P}_e^*(\mathbb{R}^n)\}
\end{aligned}$$

ただし $Y \subset \mathbb{R}^n$ とする．

上記多項式空間の次元については次の様な事が知られている．

**Dimensions of vector spaces of polynomials**

$$\dim(\mathcal{P}_e(S^{n-1})) = \binom{n+e-1}{e} + \binom{n+e-2}{e-1}$$

$$\dim(\mathcal{P}_e^*(S^{n-1})) = \binom{n+e-1}{e}$$
$$\dim(\mathcal{P}_e(\mathbb{R}^n) = \binom{n+e}{e} = \sum_{i=0}^{e} \binom{n+e-i-1}{e-i}$$

$S = S_1 \cup \cdots \cup S_p$ を $p$ 個の原点中心の同心球面の和集合とする．$0 \notin S$ であれば

$$\dim(\mathcal{P}_e(S)) = \sum_{i=0}^{2p-1} \binom{n+e-i-1}{e-i},$$
$$\dim(\mathcal{P}_e^*(S)) = \sum_{i=0}^{p-1} \binom{n+e-2i-1}{e-2i}$$

が成立つ．

**$\mathbb{R}^n$ の $s$-distance set**

$\mathbb{R}^n$ の $s$-distance set に含まれる点の個数の上界については下記の様な結果が知られている．

**定理 4 (Bannai-Bannai-Stanton, Blokhuis, 1983)**
$X \subset \mathbb{R}^n$ を $s$-distance set とすると

$$|X| \leq \binom{n+s}{s} = \dim(\mathcal{P}_s(\mathbb{R}^n))$$

が成立つ．

**定理 5 (Bannai-Kawasaki-Nitamizu-Sato, 2003)**
$X$ を $p$ 個の同心球面 $S_1, \ldots, S_p$ でサポートされた $s$-distance set で，$0 \notin X$ とする．この時

$$|X| \leq \sum_{i=0}^{2p-1} \binom{n+s-i-1}{s-i} = \dim(\mathcal{P}_s(S))$$

が成立つ．さらに $X$ が antipodal とすると

$$|X| \leq 2\sum_{i=0}^{p-1} \binom{n+s-2i-1}{s-2i} = 2\dim(\mathcal{P}_s^*(S))$$

が成立つ．ここで $S = S_1 \cup \cdots \cup S_p$ である．

**定義 (Euclidean $t$-designs, Neumaier-Seidel, 1988)**
$X$ をユークリッド空間 $\mathbb{R}^n$ の有限部分集合とする． $X$ 上には正値 weight 関数 $w$ が定義さ

れているとする．この時高々 $t$ 次の任意の多項式 $f(x)$ に対して次の等式が成立つならば $X$ を Euclidean $t$-design と呼ぶ．

$$\sum_{i=1}^{p} \frac{w(X_i)}{|S_i|} \int_{S_i} f(x) d\sigma_i(x) = \sum_{x \in X} w(x) f(x).$$

**Note:**
Euclidean $t$-design の定義においてもし $X$ をサポートする球面の個数が丁度 1 個で $S \neq \{0\}$ でありかつ weight 関数が $X$ 上で定数関数（$w(x) \equiv a$, $^\forall x \in X$, $a$ は正の実数）であれば $X$ は spherical $t$-design に相似である．

Euclidean $t$-design の点の $|X|$ 下界については次の結果が知られている．

**定理 6 (Delsarte-Seidel, 1989)**
(1) $X$ を Euclidean $2e$-design とすると

$$|X| \geq \dim(\mathcal{P}_e(S))$$

が成立つ．
(2) $X$ を Euclidean $(2e+1)$-design とする．さらに $X$ が antipodal かつ weight 関数が $w(x) = w(-x)$, $^\forall x \in X$ を満たすならば

$$|X^*| \geq \dim(\mathcal{P}_e^*(S))$$

が成立つ．ただし $X^*$ は次の様に定義される $X$ の “antipodal half part” である：
$X = X^* \cup (-X^*)$, $X^* \cap (-X^*) = \emptyset$ or $\{0\}$.

**Note:**
定理 6 (2) において $X$ が antipodal であると言うことを仮定しないと点の個数のより良い下界は知られていない．(もちろん Euclidean $(2e+1)$-design は Euclidean $2e$-design であるからその意味では下界は知られている．)

**Tight designs**

Delsarte-Seidel は定理 6 の不等式 (1) および (2) において等号が成立つ時にそれぞれ tight Euclidean $2e$-design, antipodal tight Euclidean $(2e+1)$-design と呼んだ．Delsarte-Seidel による tightness の定義を見直してより精密に次の様な定義を与える．

**定義**
$X$ が Euclidean $2e$-design でかつ $|X| = \dim(\mathcal{P}_e(S))$ が成立つならば $X$ を $S$ 上の tight $2e$-design であると言う．さらに $\dim(\mathcal{P}_e(S)) = \dim(\mathcal{P}_e(\mathbb{R}^n))$ が成立つならば $X$ を Euclidean tight $2e$-design と呼ぶ．

**定義**
$X$ が antipodal な Euclidean $(2e+1)$-design でかつ $w(x) = w(-x)$, $^\forall x \in X$ および $|X^*| = \dim(\mathcal{P}_e^*(S))$ が成立つならば $X$ を $S$ 上の antipodal な tight $(2e+1)$-design であると言う．

さらに $\dim(\mathcal{P}_e^*(S)) = \dim(\mathcal{P}_e^*(\mathbb{R}^n))$ が成立つならば $X$ を antipodal な Euclidean tight $(2e+1)$-design と呼ぶ.

$S$ 上の tight $2e$-design について次の補題が知られている.

**補題 7 (Bannai-Bannai)**
$X$ を $S$ 上の tight $2e$-design とする. 次の (1), (2) および (3) が成立つ.
(1) $w$ は各 $X_i(1 \le i \le p)$ 上で定数である.
(2) 各 $X_i(1 \le i \le p)$ は高々 $e$-distance set である.
(3) $w$ が $X\backslash\{0\}$ 上で定数関数であるならば $X\backslash\{0\}$ は高々$e$ 個の同心球面でサポートされている.

次の定理は補題 7 および 2-distance set に関する Larman-Rogers -Seidel の定理を用いて証明された.

**定理 8 (Bannai-Bannai)**
$X$ を Euclidean tight 4-design とする. weight 関数 $w$ が $X\backslash\{0\}$ 上で定数関数になっているならば $0 \in X$ であり, さらに $X\backslash\{0\}$ は spherical tight 4-design に相似である.

ここでもう少し言葉と記号を導入する.
集合 $Y \subset \mathbb{R}^n$ に対して $A(Y) = \{\|x-y\| \mid x, y \in Y, x \neq y\}$ と置く. $y \in Y$ と $\alpha \in A(Y)$ に対して $v_\alpha(y) = |\{x \in Y \mid \|x-y\| = \alpha\}|$ とおく. 任意の $\alpha \in A(Y)$ に対して $v_\alpha(y)$ が $y$ に依存しない定数である時に集合 $Y$ は distance invariant と呼ばれる.
原点を中心とする有限個の同心球面の和集合 $S$ に対して $\varepsilon_S$ を次のように定義する.

$$\varepsilon_S = \begin{cases} 1 & , 0 \in S \text{ の時,} \\ 0 & , 0 \notin S \text{ の時.} \end{cases}$$

この時次の定理が成り立つ.

**定理 9.** (1) $X$ を $S$ 上の tight $2e$-design とする. もし $e-p+\varepsilon_S \ge 0$ が成り立てば任意の $X_i \neq \{0\}$ は spherical $2(e-p+\varepsilon_S+1)$-design である. さらに $p \le [\frac{e+2\varepsilon+3}{2}]$ であれば任意の $X_i \neq \{0\}$ は distance invariant である.
(2) $X$ を $S$ 上の antipodal な tight $(2e+1)$-design とする. もし $e-p+\varepsilon_S \ge 0$ が成り立てば任意の $X_i \neq \{0\}$ は spherical $(2(e-p+\varepsilon_S+1)+1)$-design である. さらに $p \le [\frac{e+2\varepsilon+3}{2}]$ であれば任意の $X_i \neq \{0\}$ は distance invariant である.

antipodal な $(2e+1)$-design についても補題 7 と同様に次の補題が成り立つ.

**補題 10.** $X$ を $S$ 上の antipodal tight $(2e+1)$-design とする. 次の (1)〜(4) が成り立つ.
(1) $w$ は各 $X_i(1 \le i \le p)$ 上で定数である.
(2) 各 $X_i^* = X_i \cap X^*(1 \le i \le p)$ は高々 $e$-distance set である.
(3) 各 $X_i(1 \le i \le p)$ は高々 $(e+1)$-distance set である.
(4) $w$ が $X\backslash\{0\}$ 上で定数関数であるならば $X\backslash\{0\}$ は高々$e$ 個の同心球面でサポートされている.

## Antipodal tight Euclidean 3-designs

**定理 I.** $\mathbb{R}^n$ の antipodal tight Euclidean 3-design は次の $X$ antipodal tight Euclidean 3-design のどれかと相似である.

$$X = \{\pm r_i \mathbf{e}_i \mid 1 \le i \le n\}, \quad w(\pm r_i \mathbf{e}_i) = \frac{1}{n{r_i}^2},\ 1 \le i \le n.$$

ただし $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ は $\mathbb{R}^n$ の標準基底であり $r_1, \ldots, r_n$ は正の実数である.

定理 I の antipodal Euclidean tight 3-designs は Bajnok が構成したものである.

## Antipodal tight Euclidean 5-designs

**定理 II.** 二つの同心球面にサポートされている antipodal tight Euclidean 5-design は次にあげる antipodal tight Euclidean 5-designs のどれかと相似である.

(1) $X$ は原点 0 を含み $X\backslash\{0\}$ は spherical tight 5-design である.

(2) $n=2$ で $X = X_1 \cup X_2$, $|X| = 8$,

$$X_1 = \{\pm \mathbf{e}_i \mid i = 1,\ 2\},$$
$$X_2 = \{\frac{r}{\sqrt{2}}(\varepsilon_1, \varepsilon_2) \mid \varepsilon_1,\ \varepsilon_2 = \pm 1\}$$

ただし $r > 0$, $r \neq 1$, $w(x) = \begin{cases} 1, & x \in X_1 \\ r^{-4}, & x \in X_2. \end{cases}$

(3) $n=3$ で $X = X_1 \cup X_2$, $|X| = 14$,

$$X_1 = \{\pm \mathbf{e}_i \mid i = 1,\ 2,\ 3\},$$
$$X_2 = \{\frac{r}{\sqrt{3}}(\varepsilon_1, \varepsilon_2, \varepsilon_3) \mid \varepsilon_i = \pm 1,\ 1 \le i \le 3\}$$

ただし $r > 0$, $r \neq 1$, $w(x) = \begin{cases} 1, & x \in X_1 \\ \frac{9}{8}r^{-4}, & x \in X_2. \end{cases}$

(4) n=5 で $X = X_1 \cup X_2 \subset \{(x_1, \ldots, x_6) \mid \sum_{i=1}^{6} x_i = 0\} \cong \mathbb{R}^5$, $|X| = 32$,

$$X_1 = \{\pm \mathbf{u}_i \mid 1 \le i \le 6\},$$
$$\mathbf{u}_i = \frac{1}{\sqrt{30}}(u_{i,1}, \ldots, u_{i,6}), u_{i,j} = 1, \text{ for } i \neq j,\ u_{i,i} = -5,$$
$$X_2 = \{\frac{r}{\sqrt{6}}(\varepsilon_1, \ldots, \varepsilon_6) \mid \varepsilon_i = \pm 1,\ 1 \le i \le 6,\ \sum_{i=1}^{6} \varepsilon_i = 0\}$$

ただし $r > 0$, $r \neq 1$, $w(x) = \begin{cases} 1, & x \in X_1 \\ \frac{27}{25}r^{-4}, & x \in X_2. \end{cases}$

(5) n=6 で $X = X_1 \cup X_2$, $|X| = 44$,

$$X_1 = \{\pm \mathbf{e}_i \mid 1 \le i \le 6\},$$
$$X_2 = \{\frac{r}{\sqrt{6}}(\varepsilon_1, \ldots, \varepsilon_6) \mid \varepsilon_i = \pm 1,\ 1 \le i \le 6,\ \sharp\{i \mid \varepsilon_i > 0\} \text{ is even}\}$$

ただし $r > 0$, $r \neq 1$, $w(x) = \begin{cases} 1, & x \in X_1 \\ \frac{8}{8}r^{-4}, & x \in X_2. \end{cases}$

注意 定理 II の (2) と (3) は Bajnok によって構成された.
定理 II において $n$ が大きい値の時に二つの同心球面にサポートされている antipodal tight Euclidean 5-design が存在しない事は Larman-Rogers-Seidel の 2-distance set の距離の比に関する定理を用いて証明された.

最後に予想を 1 つ書いておく.

予想 $X$ を Euclidean $(2e+1)$-design とする. この時 $|X^*| \ge \dim(\mathcal{P}_e^*(S))$, $X^*$ は $X$ の部分集合 $Y^* \subset X$ で $Y^* \cap (-Y^*) = \emptyset$ or $\{0\}$ を満たす極大集合 (?). さらにもし $|X^*| \ge \dim(\mathcal{P}_e^*(S))$ が成立つならば $X$ は antipodal で $w$ は各 $X_i$ 上で一定である.

# References


[1] B. Bajnok, *On Euclidean t-designs*, to appear in Advances in Geometry.

[2] E. Bannai and E. Bannai, *Algebraic Combinatorics on Spheres* (in Japanese) Springer Tokyo 1999.

[3] E. Bannai and E. Bannai, *On Euclidean tight 4-designs*, preprint

[4] E. Bannai and D. Suprijanto, *On the strongly non-rigidity of certain Euclidean designs*, in preparation.

[5] P. Delsarte, J.-M. Goethals and J. J. Seidel, *Spherical codes and designs*, Geom. Dedicata 6 (1977) 363-388.

[6] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t-designs*, Lin. Algebra and its Appl. 114-115 (1989) 213-230.

[7] A. Erdélyi et al. *Higher transcendental Functions, Vol II, (Bateman Manuscript Project)*, MacGraw-Hill (1953).

[8] D. G. Larman, C. A. Rogers and J. J. Seidel, *On two-distance sets in Euclidean space*, Bull London Math. Soc. 9 (1977) 261-267.

[9] A. Neumaier and J. J. Seidel, *Discrete measures for spherical designs, eutactic stars and lattices*, Nederl. Akad. Wetensch. Proc. Ser. A 91=Indag. Math. 50 (1988) 321-334.

# Purifiability in Pure Subgroups

奥山　京

大分大学工学部

すべての群はアーベル群とし, 演算はすべて加法で書く。さらに $p$ を素数とする。

**定義 1**　$G$ を群とし, $A$ をその部分群とする。そこですべての非負整数 $n$ に対して

$$A \cap nG = nA$$

が成り立つとき, $A$ を $G$ の**純粋部分群 (pure subgroup)** という。

**定義 2**　$G$ を群とし, $A$ をその部分群とする. そこで $A$ を含む極小な純粋部分群 $H$ が存在するとき, $A$ を $G$ の**純粋包をもつ部分群 (purifiable subgroup)** という。また, この $H$ を $A$ の $G$ の中での**純粋包 (pure hull)** という。

すべての部分群がその部分群を含む群の中で, 純粋包をもつとは限らない。すべての素数 $p$ に対して $A \cap pG = pA$ が成り立つとき, $A$ を $G$ の粋部分群 (neat subgroup) という。群 $G$ において, 任意の部分群 $A$ に対して, $A$ を含む $G$ の極小な粋部分群 (粋包) は必ず存在することは知られている。元立教大学教授で日本のアーベル群研究の草分けでもある本田欣哉先生が, 上記の「すべての部分群には粋包が必ず存在する」ことのエレガントな証明を彼の著書「アーベル群・代数群」(共立出版) の中で与えている。

そこで次のような問題が提起される。

**問題 1**　群 $G$ の中で, どのような部分群が純粋包をもつか。

問題 1 から次のような問題も提起される。

**問題 2**　群 $G$ の中で, 部分群 $A$ が純粋包をもつとき, それらの純粋包はすべて同型か。もし同型でないなら, いかなる条件のもとで同型となるか。

$p$ 群の中で, すべての純粋包が同型にならない部分群が存在することはすでに知られている。

次にこれらの問題に対する歴史的背景を少し述べることにする。その前に 1 つ定義を与える。

**定義 3**　群 $G$ が $p$ 群であるとは, $G$ の各元の位数が $p$ ベキである群をいう。

まず $p$ 群の中でこれらの問題は次のように考察されてきた。

(1) $p$ 群において, すべての純粋包が同型にならない部分群を発見 (Hill and Megibben 1963 [5], [8])
(2) $p$ 群における純粋包の構造を決定 (Hill and Megibben 1964 [6])
(3) $p$ 群において almost-dense の概念を導入して, 純粋包の構造についての研究を深めた (Irwin and Benabdallah 1976 [2])
(4) $p$ 群において, overhang の概念を導入して, 群 $G$ の部分群 $A$ が純粋包をもつための必要条件を見つけた (Benabdallah and Okuyama 1991 [3])
(5) Quasi-complete 群においては, (3) で見つけたの条件は必要十分になることを証明 (Mader, Charles, and Benabdallah 1991 [1])

しかし一般の群についての結果はこの時点では皆無であった。次に一般の群における純粋包問題の歴史的経緯を述べる前に 1 つ定義を与える。

**定義 4**　$G$ を群とし, $A$ をその部分群とする. そこですべての非負整数 $n$ に対して

$$A \cap p^n G = p^n A$$

が成り立つとき, $A$ を $G$ の $p$ **純粋部分群** ($p$–**pure subgroup**) という。そこで $A$ を含む極小な $p$ 純粋部分群 $H$ が存在するとき, $A$ を $G$ の $p$ 純粋包をもつ部分群 (**p–purifiable subgroup**) という. また, この $H$ を $A$ の $G$ の中での $p$ **純粋包** (**p–pure hull**) という。

(1) $p$純粋包をもつ部分群から, 一般のアーベル群における純粋包をもつ部分群に入り, $p$純粋包をもつ部分群と純粋包をもつ部分群との関係, 前記の必要条件の拡張 (Okuyama 2000 [10])
(2) 一般の群において, トーションフリーランク 1 の部分群が純粋包をもつための必要十分条件を見つける (Okuyama 2001 [11])
(3) 一般の群において, トーションフリー部分群の純粋包はすべて同型の証明 (Okuyama 2001 [12])
(4) 一般の群において, トーションフリーランクが有限の部分群が純粋包をもつための必要十分条件を見つける (Okuyama 2004 [14])

群 $G$ において任意の部分群に粋包が存在することは, いろいろな証明の中で使われ, 非常に便利な道具となっている。従って純粋包をもつ部分群が特徴付けされれば, 同様に便利な道具になる。さらに一般の群における純粋包をもつ部分群の研究は次のような発展性をもっている。

(1) 分解問題への手掛かり [11], [14]
(2) 群のトーションフリーな元の高度行列の決定 [13]
(3) ADE 群への応用 [9]
(4) 混合基部分群の存在 [15]

以下, 上記の事項について少し説明を与える。その前に少しコメントを挟むことにする。

**命題 1** 群 $G$ において位数が有限の元をトーション元といい, トーション元全体のなす集合 $T$ は $G$ の部分群となり, $G/T$ はトーションフリー群となる。また上記の $T$ は最大トーション部分群となり, ただ 1 つ存在する。なお, トーションフリー群とは, 0 を除く各元の位数が無限となる群をいう。

**定義 5** トーションフリーランク $k$ の群 $G$ とは, 基底 $\{b_i \mid 1 \leqq i \leqq k\}$ があって, 任意の $g \in G$ に対して,

$$ng = n_1 b_1 + \cdots + n_k b_k$$

と書ける群である。ただし, $n_i (1 \leqq i \leqq k)$ は整数である。従って, $G$ は $k$ 個の $\mathbf{Z}$ の直和とは必ずしも同型ではない。

トーションフリーランク 1 の群は, 次のように特徴付けされている。しかし, ランク 2 以上の群についての特徴付けはまだなされていない。

**命題 2**　トーションフリーランク 1 の群は, 有理数体 $\mathbf{Q}$ を加法群とみたときの部分群と同型である。

(1) $G$ を群とし, $T$ をその最大トーション部分群とする。このとき $T$ が $G$ の直和因子となれば, $G = T \oplus F$ となるトーションフリー部分群 $F$ が存在することになる。このように分解される群を分解群と呼ぶ。しかし分解しない群の存在は, 1917 年に Levi が発見している。以後, 分解群の特徴付け問題についていろいろな研究がなされてきたが, まだ完全解答は与えられていない。ただ, トーションフリーランク 1 の群については, Stratton によって 1971 年に完全解答が与えられた。近年, 純粋包を持つ部分群の研究からその別証明を奥山が与えている。トーションフリーランク有限の群についても, Stratton は Module を使って結果を出しているが使い勝手の悪いものである。これについても, 純粋包を持つ部分群の研究から奥山が別の結果を出している。

(2) 高度行列は加算濃度のトーションフリーランク 1 の群の分類で使われているのがよく知られている。即ち, 加算濃度のトーションフリーランク 1 の群 $G, H$ が同型となるための必要十分条件は, それぞれの最大トーション部分群が同型で, それぞれの群の任意のトーションフリー元の高度行列が同値である。(3) の ADE 群の構造を調べるときも, その群のトーションフリー元の高度行列が重要な役割を果たすことがわかってきた。

(3) 純粋包が ADE 群の 1 つの例である。有名な L.Fuchs 著「Infinite Abelian Groups」[4] 第 2 巻, p.186 例 2 も 1 つの例で, この例から ADE 群の研究は多くの可能性を秘めていることがわかる。現在は純粋包をもつ部分群の概念を弱めた, 準純粋包をもつ部分群の概念を導入してこの方面の研究を奥山が行っている。

(4) $p$ 群には基部分群というのが必ず存在し, それらはすべて同型であることはよく知られている。そこでこの概念を一般の群に拡張したのが, 混合基部分群で定義は以下の通りである。

**定義 6**　群 $G$ が, すべての自然数 $n$ に対して $G = nG$ をみたすとき, $G$ を**可除群 (divisible group)** という。

**定義 7**　$G$ を群とし, その部分群 $L$ が次の 3 つの条件を満たすとき, $L$ を $G$ の**混合基部分群 (mixed basic subgroup)** という.

(1) $L$ の最大トーション部分群は巡回群の直和
(2) $L$ は $G$ の純粋部分群

(3) $G/L$はトーションな可除群

混合基部分群は必ずしも同型でない。しかし, いろいろな問題が混合基部分群の中まで縮小できる可能性がある。そこで上記の純粋包問題がそのようにならないかを考察した。

群$G$において, 任意のトーションフリー部分群$A$を与えたとき, $A$を含む混合基部分群$L$が存在する。もし$A$が$G$で純粋包をもつとき, $L$では純粋包をもたないか。必ずもてば$L$で考えればいいことになる。しかし答えは「no」である。その例を次に示す。これは[7, Remark, p.93]から引用したものである。この例を考えられたのも日本では数少ないアーベル群研究者である元お茶の水大学教授小山敏子先生である。先生はこの例で純粋包をもたない部分群の存在を示された。

例　群$G$を$\prod_{n=1}^{\infty}\langle x_n\rangle$の最大トーション部分群とし, $B=\bigoplus_{n=1}^{\infty}\langle x_n\rangle$とする. ただし$|x|=p^n$. また

$$y_i = x_{2i} + p^2x_{2i+1} - p^2x_{2i+2}.$$

とし, $H=\langle y_i \mid i=1,2,\ldots\rangle$とおき$\overline{H}$を $p$-adic closure of $H$ in $B$とする. このとき$H$は$G$の純粋部分群となり, $\overline{H}=\langle px_2\rangle\oplus H$は$G$の純粋部分群とならない. さらに$\overline{H}$は$G$で純粋包をもつが, $B$では純粋包をもたない。

そこで次のような問題が生じる。

**問題 3**　$G$を群とし, $H$をその純粋部分群とする. そこで, $H$の部分群$A$が$G$で純粋包をもつとき$H$でも純粋包をもつのはどのようなときか。

なお, 逆は必ず成り立つ。即ち,

**命題 3**　$G$を群とし, $A$をその部分群, $H$を$A$を含む$G$の純粋部分群とする. そこで$A$は$H$で純粋包をもつならば$G$で純粋包をもつ。

$A$がトーションフリーで$H$が$G$の直和因子のときは成り立つ。 即ち

**定理 1** $G$ を群とし, $A$ をそのトーションフリー部分群, $H$ を $A$ を含む $G$ の直和因子とする。このとき $A$ は $G$ で純粋包をもつならば $H$ で純粋包をもつ。

以下において, $A$ をトーションフリーランク有限としてこの問題を考える。まず定義と事実を少し記載する。

**命題 4** 群 $G$ には最大可除部分群 $D$ がただ 1 つあって, $G = R \oplus D$ と書ける。このとき $R$ には 0 以外可除部分群は存在しない。このような群 $R$ を被約群 (reduced group) という。

**定義 8** $G$ を群とするとき, その部分群

$$G[p] = \{g \in G \mid pg = 0\}$$

を $G$ の $p$ 台部分群 ($p$–socle) という。従ってこの部分群は標数 $p$ の体上のベクトル空間である。また, $G$ の最大 $p$ 部分群を $G_p$ と書く。

$G$ を群とし $A$ をそのトーションフリー部分群とする。$E$ を $G_p$ の最大可除部分群とすると $G_p = R \oplus E$ と書ける。このとき $R$ は被約群になる。そこで剰余群 $G/A$ の最大トーション部分群 $T(G/A)$ を考える。このとき $(G_p \oplus A)/A \subset T(G/A)$ であるから, $(E \oplus A)/A$ は $T(G/A)$ の可除部分群となる。そこで, $T(G/A)$ の最大可除部分群を $D/A$ とすると $(E \oplus A)/A \subset D/A$ となる。可除部分群が直和因子になることはよく知られている。従って,

$$D/A = M/A \oplus (E \oplus A)/A \tag{0.1}$$

と書ける。

**定義 9** $G$ を群とし, $A$ をそのトーションフリー部分群とする. さらに $D/A$ を $(G/A)_p$ の最大可除部分群, $E$ を $G_p$ の最大可除部分群とする. このとき次のように定義する.

$$\dim(G, A, p) = \dim(D/(E \oplus A))[p].$$

上記のコメントと (0.1) から $\dim(G, A, p) = \dim(M/A)[p]$ となる。

$G$ を群, $A$ をそのトーションフリー部分群, $E$ を $G_p$ の最大加除部分群とする。$A$ は $G$ で純粋包をもつと仮定する。このとき $E$ は $G$ の絶対直和因子となるので,

$$G = H \oplus E, \quad H < G, \quad A \subseteq H \tag{0.2}$$

となる。すると $\dim(G,A,p) = \dim(H,A,p) = \dim(D'/A)[p]$ となる。ただし, $D'/A$ は $H/A$ の最大トーション部分群 $T(H/A)$ の最大可除部分群である。また, (0.2) と定理 1 より $A$ は $H$ で純粋包をもつことになる。従って, はじめから $G_p$ は被約群であると仮定してよい。さらに, $A$ をトーションフリーランク有限の部分群と仮定すると, $D$ がトーションフリーであることがわかる。そこで

**補題** $F$ をトーションフリー群, $B$ をその部分群とする。そして $F/B$ は $p$ 群であると仮定する。このとき

$$\dim(F/B)[p] \leqq rank(F)$$

を使うと, $\dim(G,A,p)$ は有限で $A$ のランク以下になることがわかる。これらのことを念頭において下記の結果を得た。

**定理 2** $G$ を群とし, $A$ をそのトーションフリーランク有限の部分群, $H$ を $A$ を含む $G$ の純粋部分群とする. そこで $A$ は $G$ で純粋包をもつと仮定する. このとき $A$ が $H$ で純粋包をもつための必要十分条件は, すべての素数 $p$ に対して, 次の式が成り立つことである.

$$\dim(G,A,p) = \dim(H,A,p)$$

証明はトーションフリーランク有限の部分群が純粋包をもつための必要十分条件を使っている。

## REFERENCES


[1] K. Benabdallah, B. Charles, and A. Mader. Vertical Subgroups of Primary Abelian Groups, *Can. J. Math.*, 43:3–18, 1991.

[2] K. Benabdallah and I. Irwin. On minimal pure subgroups, *Publ. Math.* Debrecen, 23:111-114, 1976.

[3] K. Benabdallah and T. Okuyama. On purifiable subgroups of primary abelian groups, *Comm. Algebra* 19(1):85–96, 1991.

[4] L. Fuchs. *Infinite Abelian Groups, Vol. I, II.* Academic Press, 1970 and 1973.

[5] P. Hill. Certain pure subgroups of primary groups, *Topics in Abelian Groups* Chicago, Illinois, 311–314, 1963.
[6] P. Hill and C. Megibben. Minimal pure subgroups in primary abelian groups, *Bull Soc. Math.* France, 92:251–257, 1964.
[7] T. Koyama. On Quasi–Closed Groups and Torsion complete Groups, *Bull Soc. Math.* France, 95:89–94, 1967.
[8] C. Megibben. A note of a paper of Bernard Charles, *Bull Soc. Math.* France, 91:453–454, 1963.
[9] T. Okuyama. On Almost–Dense Extension Groups of Torsion–Free Groups, *J. Algebra*, 202:202–228, 1998.
[10] T. Okuyama. On Purifiable Subgroups in Arbitrary Abelian Groups, *Comm. Algebra*, 28(1):121–139, 2000.
[11] T. Okuyama. On Purifiable Torsion–Free Rank–One Subgroups, *Hokkaido Math. J.*, 30(2):373–404, 2001.
[12] T. Okuyama. On isomorphy of pure hulls of purifiable torsion–free subgroups, *Hokkaido Math. J.*, 30(3):671–677, 2001.
[13] T. Okuyama. Quasi–Purifiable Subgroups and Height–Matrices, *Rocky Mountain J. Math.*, 32(4):1577–1595, 2002.
[14] T. Okuyama. Splitting mixed groups of finite torsion–free rank, *Comm. Algebra*, 32(4):1587–1601, 2004.
[15] T. Okuyama. Mixed Basic Subgroups, *to appear in Hokkaido Math, J.*.

# 頂点作用素代数の有限性について

東京大学大学院数理科学研究科

松尾　厚

## はじめに

本稿では，頂点作用素代数に対するある種の有限性条件を定式化し，その帰結について考察する。

頂点作用素代数の理論にはいくつかの側面があり，大雑把に言って組合せ的ないし代数的な側面と解析的ないし幾何的な側面に分けることができる。これらの側面は，例えば分割数が母函数を通してモジュラー形式と関連しているのと同様の意味で，互いに関連している。物理の用語で言えば，状態の数え上げの問題が分配函数を通して幾何学的な問題と関連しているというわけである。

ところで，整格子 $L$ を与えると，双対格子 $L^*$ が定まるが，商集合 $L^*/L$ に属する各コセットに対して，対応するテータ函数を考えることができる。カイラルな共形場理論において，格子 $L$ に相当するのが頂点作用素代数 $V$ であり，各コセットに相当するのが既約 $V$-加群である。そして，コセットに附随して定まるテータ函数に相当するのが，既約加群の分配函数すなわち指標と呼ばれるものである。

そこで，頂点作用素代数を与えたときに，その上の既約加群を分類し，その分配函数を計算することは重要な問題であるが，定量的な計算もさることながら，ある程度一般的な枠組みのもとで，定性的な結論を得ることが大切であると考えられる。そのような型の結論としては，例えば有名な Verlinde の公式などがその典型であるが，この種の性質を突き詰めていくと，Riemann 面上のカイラルな共形場理論を構成せよという問題に行き着くことになる。

これに関しては，特にアフィン Kac-Moody 代数の最高ウェイト可積分表現に附随する場合について，土屋昭博・上野健爾・山田泰彦による有名な研究 [TUY] がある。この研究を一般化するためには，アフィン Kac-Moody 代数の最高ウェイト可積分表現の性質の中から本質的な部分を抜き出し，そのような性質を満たすような頂点作用素代数について一般論を展開するのが良いと考えられる。

本稿では，このような立場から，特に表現あるいは加群のなす圏の有限性に関わる性質に注目し，それを一般的にとらえる方法について述べる。

本稿は，永友清和・土屋昭博両氏との共同研究 [MNT] の内容の一部とその背景の紹介である。代数的組合せ論シンポジウムでの講演を薦めてくださった安部利之氏ならびに組織委員各位に感謝する。

第 22 回代数的組合せ論シンポジウム報告集原稿

# 第1章 可積分表現の圏

アフィン Kac-Moody 代数の可積分表現に関する最高ウェイトの理論の概略を回顧し，本稿の研究の動機を説明する。

### 有限次元単純 Lie 代数

有限次元複素単純 Lie 代数 $\mathfrak{g}$ を考える。Cartan 部分代数 $\mathfrak{h}$ をとり，標準的な定義関係式を持つ生成元 $e_1,\dots,e_\ell,h_1,\dots,h_\ell,f_1,\dots,f_\ell$ をとる。このとき，Lie 代数 $\mathfrak{g}$ の有限次元表現は以下の条件 (F1), (F2), (F3) で特徴付けられる。

(F1) Cartan 部分代数 $\mathfrak{h}$ は半単純に作用し，各ウェイト空間は有限次元である。

(F2) 元 $f_1,\dots,f_\ell$ は巾零に作用する。

(F3) ある有限個のウェイトがあって，任意のウェイトはこれらに負ルートを繰り返し加えた形をしている。

ただし，Cartan 部分代数 $\mathfrak{h}$ の作用の固有値のなすベクトルをウェイトと呼び，特に随伴表現 $\mathfrak{g}$ のウェイトをルートと呼ぶのであった。

考える有限次元表現が既約である場合には，条件 (F3) に言う有限個のウェイトとして一個の最高ウェイトを取ることができ，これを通して有限次元既約表現の同型類の全体が支配的整ウェイトの集合 $\mathrm{P}_+$ によってパラメトライズされる。

### アフィン Kac-Moody 代数

さて，$\mathfrak{g}$ に附随するアフィン Kac-Moody 代数は，$\hat{\mathfrak{g}}=\mathfrak{g}\otimes\mathbb{C}[t,t^{-1}]\oplus\mathbb{C}K\oplus\mathbb{C}D$ なるベクトル空間に括弧積を

$$\begin{aligned}&[X\otimes t^m,Y\otimes t^n]=[X,Y]\otimes t^{m+n}+m\delta_{m+n,0}K,\\&[D,X\otimes t^m]=mX\otimes t^m,\ [K,X\otimes t^m]=[K,D]=0\end{aligned}\tag{1.1}$$

で与えて得られる Lie代数である。

アフィン Kac-Moody 代数は一般に Kac-Moody 代数と呼ばれる Lie 代数の特別なクラスであり，$\mathfrak{g}\otimes t^0$ を $\mathfrak{g}$ と同一視するとき，これに標準的な元 $e_0,h_0,f_0$ を加え，さらに元 $D$ を合わせて $\hat{\mathfrak{g}}$ を生成するようにできる。(註1)

さて，無限次元の Kac-Moody 代数に対して有限次元表現を考えることは，有限次元単純 Lie 代数に対して有限次元表現を考えることの類似ではない。むしろ，条件 (F1), (F2), (F3) に相当する条件を満たす表現を考えることによって，最高ウェイト理論に基づく正しい類似が得られる。

正確には，以下の条件を考える。

(I1) Cartan 部分代数 $\hat{\mathfrak{h}}$ は半単純に作用し，各ウェイト空間は有限次元である。

(I2) 元 $f_0,f_1,\dots,f_\ell$ は局所巾零に作用する。

(I3) ある有限個のウェイトがあって，任意のウェイトはこれらに負ルートを繰り返し加えた形をしている。

---

1. 詳しくは [Kac] を参照のこと。

すなわち，条件 (I1), (I2), (I3) を満たす表現を考えることによって，有限次元単純 Lie 代数 $\mathfrak{g}$ に対する有限次元表現のアフィン Kac-Moody 代数における類似が得られるというわけである。

### レベル $k$ の可積分表現のなす圏の構造

ここで，正整数 $k$ を一つ固定し，アフィン Kac-Moody 代数 $\hat{\mathfrak{g}}$ の表現に対する次の条件を考える。

(I4)$_k$ 中心 $K$ はスカラー $k$ で作用する。

Lie 代数 $\hat{\mathfrak{g}}$ の表現であって，条件 (I1), (I2), (I3) に加えて条件 (I4)$_k$ を満たすもののなす圏を $\mathcal{O}_k^{\mathrm{int}}$ と表し，本稿ではレベル $k$ の可積分表現の圏と呼ぶことにする。(註2)

Kac-Moody 代数の一般論によれば，圏 $\mathcal{O}_k^{\mathrm{int}}$ に属する表現は完全可約であって，既約表現の同型類の全体は，レベル $k$ の支配的整ウェイトの集合 (註3)

$$\mathrm{P}_k = \{\lambda \in \mathrm{P}_+ \mid 0 \le (\lambda \mid \theta) \le k\} \tag{1.2}$$

でパラメトライズされる。ウェイト $\lambda \in \mathrm{P}_k$ に対応するレベル $k$ の最高ウェイト既約表現を $L(k,\lambda)$ と表す。

ここで，支配的整ウェイトの集合 $\mathrm{P}_+$ が無限集合であるのに対し，各正整数 $k$ に対して，集合 $\mathrm{P}_k$ は有限集合であることに注意する。かくして，圏 $\mathcal{O}_k^{\mathrm{int}}$ は単純対象が有限集合 $\mathrm{P}_k$ でパラメトライズされるような半単純圏となることが分かった。特に，この圏はある有限次元半単純環上の有限生成加群の圏と圏同値になる。(註4)

### 頂点作用素代数による解釈と問題設定

さて，可積分な最高ウェイト既約表現 $L(k,\lambda)$ のうち特にウェイトが $\lambda = 0$ であるもの，すなわち $L(k,0)$ を考えよう。これをレベル $k$ の（可積分な）真空表現という。

論文 [FrZ] において，Frenkel と Zhu は，真空表現 $L(k,0)$ が自然な頂点作用素代数の構造を持つことを示した。さらに，各 $\lambda \in P_k$ に対して $L(k,\lambda)$ は既約な通常 $L(k,0)$-加群であり，それらの全体が既約な通常 $L(k,0)$-加群の同型類を尽くすこと (註5) を示した。すなわち，通常 $L(k,0)$-加群の圏は圏 $\mathcal{O}_k^{\mathrm{int}}$ と等しい。このようにして，アフィン Kac-Moody 代数 $\hat{\mathfrak{g}}$ に対して，圏 $\mathcal{O}_k^{\mathrm{int}}$ は頂点作用素代数の枠組みで理解することができる。

さらに，Dong 他の結果 ([DLM]) と前節で述べたことを合わせれば，次のことが (註6) 分かる。

**事実 1.1** 頂点作用素代数 $L(k,0)$ に対し，$L(k,0)$-加群の圏はある有限次元半単純環上の加群の圏と圏同値である。

我々は，この事実のうち，圏の半単純性を忘れて，有限次元環上の加群の圏と圏 (註7) 同値になるという部分に着目する。この種の条件を単に有限性条件と呼ぶことにしよう。そして，そのような頂点作用素代数を特徴付けることと，圏同値関手を標準的に構成することに関心がある。

---

2. 可積分表現という用語のここでの用法は正当なものではないので注意されたい。
3. ここに $\theta$ は最高ルートであり，$(\ |\ )$ は $\mathfrak{h}^*$ 上の正規化された内積である。
4. 環とは一般には非可換な $\mathbb{C}$ 上の単位的結合的代数のことを意味するものとする。
5. 通常加群については，後で用いないので，これ以上述べない。文献 [DLM] を参照のこと。
6. 論文 [DLM] の結果を用いれば，可積分表現の圏そのものについてもすっきりと説明できる。
7. その理由は，実際に $V$-加群の圏が半単純でないような重要な例が考察されているからである。

すなわち，我々の問題は次の通りである。

**問題 1.2** 頂点作用素代数 $V$ 上の加群の圏が有限次元環上の加群の圏と圏同値になるための条件を求めよ。また，そのような有限次元環および圏同値関手の標準的な構成法を与えよ。 (注8)

究極的には，$V$-加群の圏が有限次元環上の加群の圏と圏同値になるために $V$ が満たすべき必要十分条件を求めたいところであるが，これは難しい問題であると思われる。圏同値の標準的な構成方法について第2章で論じ，その結果を利用する形で，$V$ に対する有限性条件を第3章で述べる。

### 普遍展開環の利用

ところで，一般に Lie 代数 $L$ に対しては，その普遍展開環 $\mathrm{U}(L)$ の概念があって，$L$ の表現を $\mathrm{U}(L)$-加群とみなすことができた。また $\mathrm{U}(L)$ を積極的に利用して $L$ の表現論を調べることができた。そこでは，Lie 代数 $L$ 自体は非結合的な代数系であるが，$\mathrm{U}(L)$ は結合的な代数系であるという点が重要である。同様に，頂点作用素代数という非結合的な代数系の表現を調べるためにも，その普遍展開環の概念を利用するのが良いと考えられる。 (注9)

そこで，頂点作用素代数 $V$ に対して，その普遍展開環 $\mathbf{U}(V)$ を用いて $V$-加群の圏を有限次元環上の加群の圏を結び付けることを考えよう。

実は，頂点作用素代数 $V$ の普遍展開環 $\mathbf{U}(V)$ の概念もまた Frenkel と Zhu ([FrZ]) によって既に導入されている。実際には，普遍展開環 $\mathbf{U}(V)$ は単なる環ではなく，整数で次数付けられた次数環であって，各斉次部分空間に完備な線型位相が与えられているようなものである。 (注10) (注11)

ともあれ，$V$-加群の圏が有限次元環上の加群の圏と圏同値になるための条件を，まずは $\mathbf{U}(V)$ の性質として求め，次に $\mathbf{U}(V)$ がその性質を満たすような $V$ の性質を求めようというのである。

## 第2章 擬有限な環とその性質

普遍展開環 $\mathbf{U}(V)$ に対する有限性条件については，$\mathbf{U}(V)$ が $V$ の普遍展開環であるという事実を離れ，$\mathbf{U}(V)$ の持つ一般的な性質のみで定式化される。そこで，普遍展開環 $\mathbf{U}(V)$ をモデルとする環の一般的な性質を述べ，そのような環に対する有限性条件とその帰結について述べる。

### 環に関する設定

環 $\mathbf{U}$ が与えられたとし，その乗法を $a,b \in \mathbf{U}$ に対して $a \cdot b$ と表すことにする。環 $\mathbf{U}$ に関する以下の性質を考える。

---

8. $V = L(k,0)$ の場合には，圏同値を与える有限次元環として，いわゆる Zhu 代数をとることができるが，一般にはそうではない。
9. それどころか，可算個の二項演算を持っているような代数系である。
10. こまかいことを言えば，論文 [FrZ] の構成には若干の瑕疵がある。なお，普遍展開環 $\mathbf{U}(V)$ やそのフィルターごとの完備化のことを，論文 [NaT] および [MNT] ではカレント代数と呼んでいる。
11. 位相を考える必要があるのは，加群の定義関係式 (A.7) の右辺が無限和を含んでいるからである。右辺は加群 $M$ の一つの元に作用させれば有限和であるが，作用素としては無限和なのである。一方，左辺はいつでも有限和である。

(U1) 整数による次数付け $\mathbf{U}=\bigoplus_d \mathbf{U}(d)$ が与えられ，$\mathbf{U}$ は次数環である。

(U2) 各斉次部分空間に線型位相が与えられている。

(U3) 乗法 $\mathbf{U}(d)\times\mathbf{U}(e)\to\mathbf{U}(d+e)$ は連続である。

ここで $\mathbf{F}_n\mathbf{U}=\bigoplus_{d\le n}\mathbf{U}(d)$ とおく。各 $d$ について部分空間 $\mathbf{U}(d)\cap(\mathbf{U}\cdot\mathbf{F}_{-n-1}\mathbf{U})$ を考え，$\mathbf{U}(d)$ の線型位相に関するその閉包を $\mathbf{I}_n(d)$ とおく。 (註12)

$$\mathbf{I}_n(d)=\overline{\mathbf{U}(d)\cap(\mathbf{U}\cdot\mathbf{F}_{-n-1}\mathbf{U})}. \tag{2.1}$$

これについて，次の性質を考える。

(U4) 部分空間の族 $\{\mathbf{I}_n(d)\}$ は，$\mathbf{U}(d)$ の原点の基本近傍系をなす。

(U5) 各斉次部分空間 $\mathbf{U}(d)$ は完備である。

ここで，条件 (U5) は，$\mathbf{U}(d)=\varprojlim_n \mathbf{U}(d)/\mathbf{I}_n(d)$ を意味する。

### Hamiltonian を持つ擬有限環

以下では，環 $\mathbf{U}$ は条件 (U1)-(U5) を満たすものとする。そのような環 $\mathbf{U}$ に対して，部分空間 $\mathbf{I}_n(d)$ を考え，

$$\mathbf{Q}_n(d)=\mathbf{U}(d)/\mathbf{I}_n(d) \tag{2.2}$$

とおく。このとき，$\mathbf{I}_n=\bigoplus_d \mathbf{I}_n(d)$ は $\mathbf{U}$ の左イデアルとなるから，$\mathbf{Q}_n=\bigoplus_d \mathbf{Q}_n(d)$ は左 $\mathbf{U}$-加群となる。

以上の考察に基づき，環 $\mathbf{U}$ に対して次のように定義する。

**定義 2.1（擬有限性）** 環 $\mathbf{U}$ が擬有限（quasi-finite）であるとは，すべての非負整数 $n$ およびすべての整数 $d$ に対して，$\mathbf{U}(d)/\mathbf{I}_n(d)$ が有限次元となることである。

すなわち，環 $\mathbf{U}$ に対する擬有限性は，左 $\mathbf{U}$-加群 $\mathbf{Q}_n$ の斉次部分空間が有限次元であることを意味している。なお，$d\le -n-1$ であれば，$\mathbf{U}(d)=\mathbf{I}_n(d)$ であるので， (註13)

$$\mathbf{Q}_n=\bigoplus_{d=-n}^{\infty}\mathbf{Q}_n(d) \tag{2.3}$$

となっていることを注意しておく。

擬有限性は重要な性質であるが，特別な性質を持つ元 $h$ が $\mathbf{U}$ の中に存在することによって威力を発揮する。

**定義 2.2（Hamiltonian）** 次数環 $\mathbf{U}=\bigoplus_{d=-\infty}^{\infty}\mathbf{U}(d)$ の元 $h$ が $\mathbf{U}$ の Hamiltonian であるとは，$a\in\mathbf{U}(d)\Leftrightarrow h\cdot a-a\cdot h=da$ となることである。 (註14)

条件 (U1)-(U5) を満たす擬有限な $\mathbf{U}$ であって，Hamiltonian $h$ の与えられたものを，Hamiltonian を持つ擬有限環と呼ぶことにする。

---

12. ここで $\mathbf{U}(d)$ があたかも次数を $d$ だけシフトする作用素からなるものと考えると，部分空間 $\mathbf{U}\cdot\mathbf{F}_{-n-1}\mathbf{U}$ はいったん次数を $n+1$ 以上下げるような作用素全体であると考えることができる。
13. 擬有限という用語は，Kac-Radul [KaR] に倣い，これに基づいて名付けたものである。
14. 特に $\mathbf{U}=\mathbf{U}(V)$ の場合には，$h$ として Virasoro の $L_0$ の像をとることができる。Hamiltonian という用語はこれに由来して付けたものであって，ここに与えた定義自体は物理で言うところの Hamiltonian とは特に関係がない。

### 広義固有空間

Hamiltonian を持つ擬有限環 $\mathbf{U}$ を考える。これに対して，空間 $\mathbf{Q}_0(0) = \mathbf{U}(0)/\mathbf{I}_0(0)$ を考えると，これは有限次元の環となり，Hamiltonian $h$ の $\mathbf{Q}_0(0)$ における最小多項式を考えることができる。その根の集合を $\Omega_0$ とおくと，これは有限集合である。

複素数体 $\mathbb{C}$ 上の順序 $\leq$ を $\alpha \leq \beta$ であるとは $\beta - \alpha \in \mathbb{Z}_{\geq 0}$ となることであると定義する。この順序に関して，集合 $\Omega_0$ の極小元の全体を $\Gamma_0$ とおく。従って，$\Gamma_0$ に属する複素数は整数差を持たない。

各自然数 $n$ に対して次のようにおく。

$$\Gamma_n = \Gamma_0 + \{0, 1, \ldots, n\} = \{\gamma + k \,|\, \gamma \in \Gamma_0,\ k = 0, 1, \ldots, n\}. \tag{2.4}$$

また，次のようにおく。

$$\Gamma_\infty = \Gamma_0 + \{0, 1, \ldots\} = \{\gamma + k \,|\, \gamma \in \Gamma_0,\ k = 0, 1 \ldots\}. \tag{2.5}$$

すると $\Gamma_0 \subset \Gamma_1 \subset \Gamma_2 \subset \cdots$ かつ $\Gamma_\infty = \bigcup_n \Gamma_n$ となっている。集合 $\Omega_0$ の元の間の整数差の最大値を $g$ とおくと，$\Gamma_0 \subseteq \Omega_0 \subseteq \Gamma_g$ が成立することに注意しておく。

さて，Hamiltonian を左および右から掛けるという作用に関する広義固有空間を考え，それを次のようにおく。

$$\mathbf{U}[\lambda, \mu] = \left\{ a \in \mathbf{U} \,\middle|\, \text{ある } r \text{ に対して } (h - \lambda)^r \cdot a = a \cdot (h - \mu)^r = 0 \right\}. \tag{2.6}$$

このとき $\lambda$ を左固有値，$\mu$ を右固有値と呼ぶことにする。

**命題 2.3** 広義固有空間 $\mathbf{U}[\lambda, \mu]$ について以下が成立する。

(1) $\mathbf{U}[\lambda, \mu] \subseteq \mathbf{U}(\lambda - \mu)$ である。

(2) $\mathbf{U}[\lambda, \mu] \neq 0$ ならば $\lambda - \mu \in \mathbb{Z}$ である。

(3) $\mathbf{U}[\lambda, \mu] \neq 0$ ならば $\lambda, \mu \in \Gamma_\infty$ である。

ここで，標準的な左 $\mathbf{U}$-加群 $\mathbf{Q}_n$ の斉次成分 $\mathbf{Q}_n = \mathbf{U}(d)/\mathbf{I}_n(\mathbf{U}(d))$ を考える。擬有限の仮定から，これは有限次元であるので，$h$ の作用について広義固有空間分解を持つ。

$$\mathbf{Q}_n(d) = \bigoplus_{\lambda - \mu = d} \mathbf{Q}_n[\lambda, \mu]. \tag{2.7}$$

このとき，完備性の条件 (U5) により，次の結果が成り立つ。

**命題 2.4（近似定理）** 各 $\lambda, \mu \in \Gamma_\infty$ に対して，十分大きな自然数 $N$ をとれば，$n \geq N$ のとき $\mathbf{U}[\lambda, \mu] = \mathbf{Q}_n[\lambda, \mu]$ が成立する。

このことから，各斉次部分空間 $\mathbf{U}(d)$ の中で，部分空間 $\sum_{\lambda - \mu = d} \mathbf{U}[\lambda, \mu]$ が稠密であることが従う。 (RE15)

### 有限次元環の構成

環 $\mathbf{U}$ の左右固有値は $\Gamma_0$ の元に自然数を加えた形をしているが，それを途中の第 $n$ 段で打ち切って得られる部分空間を考える。

$$\mathbf{A}_n = \mathbf{U}[\Gamma_n, \Gamma_n] = \sum_{k=0}^{n} \sum_{\ell=0}^{n} \sum_{\gamma, \delta \in \Gamma_0} \mathbf{U}[\gamma + k, \delta + \ell]. \tag{2.8}$$

定義から直ちに，$\mathbf{A}_n$ は $\mathbf{U}$ の部分環となることが分かる。さらに，前節の命題 2.4 から直ちに次が分かる。 (註16)

**命題 2.5** $\mathbf{A}_n$ は有限次元である。

環 $\mathbf{U}$ の右固有値のみを第 $n$ 段で打ち切って得られる部分空間も考えておく。

$$\mathbf{P}_n = \mathbf{U}[\Gamma_\infty, \Gamma_n] = \sum_{k=0}^{\infty} \sum_{\ell=0}^{n} \sum_{\gamma,\delta\in\Gamma_0} \mathbf{U}[\gamma + k, \delta + \ell]. \tag{2.9}$$

定義から $\mathbf{P}_n$ は自然に右 $\mathbf{A}_n$-加群となるが，Hamiltonian の性質によって，左 $\mathbf{U}$-加群ともなることが分かる。すなわち $\mathbf{P}_n$ は $(\mathbf{U}, \mathbf{A}_n)$-双加群となる。

### 究尽的な加群と圏同値関手の構成

左 $\mathbf{U}$-加群 $M$ に対して，$\mathbf{U}$ の $M$ への作用を，$a \in \mathbf{U}$ および $v \in M$ に対して $a \cdot v$ と表すことにする。

Hamiltonian を持つ擬有限環 $\mathbf{U}$ に対して，左イデアル $\mathbf{I}_n = \bigoplus_d \mathbf{I}_n(d)$ を考える。これを用いて，左 $\mathbf{U}$-加群 $M$ の部分線型空間 $\mathbf{K}_n(M)$ を次のように定義する。

$$\mathbf{K}_n(M) = \{v \in M \mid \mathbf{I}_n \cdot v = 0\}. \tag{2.10}$$

以上の状況の下で，次のように定義する。

**定義 2.6（究尽的加群）** 左 $\mathbf{U}$-加群 $M$ が究尽的 (exhaustive) であるとは，$M = \bigcup_n \mathbf{K}_n(M)$ が成立することである。 (註17)

例えば，標準的な左加群 $\mathbf{Q}_n$ は究尽的である。また，前節で定義した $(\mathbf{U}, \mathbf{A}_n)$-双加群 $\mathbf{P}_n$ は左 $\mathbf{U}$-加群とみて究尽的である。

左 $\mathbf{U}$-加群 $M$ に対して，次のようにおく。

$$M[\lambda] = \left\{v \in M \,\middle|\, \text{ある } r \text{ に対して } (h - \lambda)^r \cdot v = 0\right\}. \tag{2.11}$$

このとき，次が成立する。

**命題 2.7** 究尽的左 $\mathbf{U}$-加群 $M$ に対して，$M[\lambda] \neq 0$ ならば $\lambda \in \Gamma_\infty$ である。

左 $\mathbf{U}$-加群 $M$ に対して，固有値を第 $n$ 段で打ち切って得られる部分空間を考え，次のようにおく。

$$\mathbf{E}_n(M) = M[\Gamma_n] = \sum_{k=0}^{n} \sum_{\gamma\in\Gamma_0} M[\gamma + k]. \tag{2.12}$$

これは自然に左 $\mathbf{A}_n$-加群の構造を持つ。これによって，特に 究尽的な左 $\mathbf{U}$-加群の圏から左 $\mathbf{A}_n$-加群の圏への関手 $\mathbf{E}_n$ が得られる。

前節において $(\mathbf{U}, \mathbf{A}_n)$-双加群 $\mathbf{P}_n$ を定義した。これを用いることによって，左 $\mathbf{A}_n$-加群 $W$ に対して，左 $\mathbf{U}$-加群 $\mathbf{P}_n \otimes_{\mathbf{A}_n} W$ を対応させる関手が考えられる。このとき $\mathbf{P}_n \otimes_{\mathbf{A}_n} W$ は究尽的である。この関手を，記号の濫用により，同じ記号 $\mathbf{P}_n$ で表すことにする。

---

15. すべての固有値についての和 $\mathbf{B} = \sum_{\lambda,\mu} \mathbf{U}[\lambda, \mu]$ は環 $\mathbf{U}$ の正則双加群であるとみられる。
16. ただし，$\mathbf{U}$ の単位元は $\mathbf{A}_n$ の単位元と一致しない。
17. 英単語 exhaustive の訳語として，究尽的という言葉を造ってみた。より優れた訳語をご存じであればご教示願いたい。なお，究尽という言葉は仏教で用いられることがあるようで，すべてを究め尽くした悟りの境地を表すものと思われる。

### 圏同値定理

第 7 節において Hamiltonian $h$ の $\mathbf{Q}_0(0)$ における最小多項式の根の集合 $\Omega_0$ を思い出そう。集合 $\Omega_0$ の元の間の整数差の最大値を $g$ とおいたのであった。

以上の準備のもとで，我々の主要結果は次の定理である。

**定理 2.8（圏同値定理）** Hamiltonian を持つ擬有限環 $\mathbf{U}$ に対し，$n \geq g$ なる自然数 $n$ をとる。このとき，関手 $\mathbf{E}_n$ および $\mathbf{P}_n$ は究尽的な左 $\mathbf{U}$-加群の圏と左 $\mathbf{A}_n$-加群の圏の間の互いに逆な圏同値関手である。

この定理は，Hamiltonian の固有値に関する最高ウェイトの理論の一種であり，同時に森田同値定理の一種であると考えられる。(註18)

## 第3章 頂点作用素代数への応用

前章の結果を頂点作用素代数の普遍展開環に応用する。内容はかなり技術的であるので，詳細は論文 [MNT] に譲る。

### $V$-加群の特徴付け

まず，左 $\mathrm{U}(V)$-加群の中で $V$-加群の持ち上げになるようなものの特徴付けに関しては，次の結果が成り立つ。

**定理 3.1** 頂点作用素代数 $V$ に対して $V$-加群の圏は究尽的な左 $\mathrm{U}(V)$-加群の圏と等しい。

ただし，$V$-加群の定義としては，附録に述べるものを採用する。(註19)

さて，普遍展開環 $\mathbf{U}(V)$ の Hamiltonian として，元 $L_0 = J_0(\omega)$ の像をとることができる。そこで，$\mathbf{U}(V)$ が擬有限となるための $V$ の満たす良い十分条件が見いだせれば，問題 1.2 に対する一つの解答が得られることになる。

### Zhu の有限性条件

頂点作用素代数 $V$ に対するそのような有限性条件としては，Zhu によって論文 [Zhu] で最初に与えられ，現在では $\mathrm{C}_2$-有限性条件と名付けられて良く知られている条件をとることができる。すなわち，頂点作用素代数 $V$ が $\mathrm{C}_2$-有限であるとは，

$$\dim V/V_{(-2)}V < \infty \tag{3.1}$$

となることであり，この条件の下で，次の定理が成り立つ。

**定理 3.2** 頂点作用素代数 $V$ が $\mathrm{C}_2$-有限ならば，普遍展開環 $\mathrm{U}(V)$ は Hamiltonian を持つ擬有限環である。

---

18. 森田同値定理については [Gab] を参照のこと。
19. 頂点作用素代数 $V$ 上の加群の概念にはさまざまなものがある。よく使われるものとして，弱 $V$-加群 (weak module)，認容 $V$-加群 (admissible module)，通常 $V$-加群 (ordinary module) の概念があり，目的によって使い分けられる。本稿の定義は，一般の $V$ に対してはこれらのいずれとも異なる。ただし，$V$ が $\mathrm{C}_2$-有限である場合には，本稿の $V$-加群，弱 $V$-加群，認容 $V$-加群の概念は互いに同値となるので，どれをとっても良い。しかし，定理 3.1 を一般に成り立たせるような $V$-加群の定義としては，$\mathrm{U}(V)$ の定義の連動して，本稿の定義がちょうど良いのである。

この定理の証明には，Gaberdiel-Neitzke によって [GaN] において創始された論法を使用する。(註20)

### 有限性についての結論

かくして，定理3.1と定理3.2に前章の定理2.8を組合わせることによって，我々は次の結論を得る。

**系 3.3** 頂点作用素代数 $V$ が $C_2$-有限ならば $V$-加群の圏はある有限次元環上の加群の圏と自然に圏同値である。

## A 附録

頂点作用素代数とその上の加群および普遍展開環についてまとめておく。(註21)

### 頂点作用素代数

複素数体 $\mathbb{C}$ 上のベクトル空間 $V$ および以下のデータが与えられているとする。

(a) 整数 $n$ でパラメトライズされた可算個の双線型写像

$$V \times V \to V, \quad (a,b) \mapsto a_{(n)}b. \tag{A.1}$$

(b) 真空ベクトルと呼ばれるベクトル $1 \in V^0$.

(c) 共形ベクトルと呼ばれるベクトル $\omega \in V^2$.

このとき，$\omega_{(n+1)} : V \to V$ なる作用素が考えられるので，これを $L_n$ とおく。特に作用素 $L_0$ を考え，その固有値 $k$ の固有空間を $V^k$ とおく。

$$V^k = \{a \in V \mid L_0 a = ka\}. \tag{A.2}$$

頂点作用素代数とは，このようなデータの与えられたベクトル空間 $V$ であって，以下の条件を満たすようなものである。(註22)

(V1) ある自然数 $m$ が存在して $V = \bigoplus_{k=-m}^{\infty} V^k$ である。

(V2) 任意の $k,\ell \in \mathbb{N}$ および $n \in \mathbb{Z}$ に対して $V^k{}_{(n)}V^\ell \subseteq V^{k+\ell-n-1}$ である。

(V3) 任意の $p,q,r \in \mathbb{Z}$ および $a,b,c \in V$ に対して

$$\begin{aligned}&\sum_{i=0}^{\infty}\binom{p}{i}(a_{(r+i)}b)_{(p+q-i)}c \\ &\quad = \sum_{i=0}^{\infty}(-1)^i\binom{r}{i}a_{(p+r-i)}(b_{(q+i)}c) - \sum_{i=0}^{\infty}(-1)^{r+i}\binom{r}{i}b_{(q+r-i)}(a_{(p+i)}c).\end{aligned} \tag{A.3}$$

20. 論文 [MNT] では，Poisson 代数のループ化の議論を経由することにより，Gaberdiel-Neitzke の論法が自然に現れるような枠組みを構築した。
21. 詳しくは，拙著 [MaN] および論文 [MNT] を参照していただきたい。
22. 頂点作用素代数の定義は，母函数 $Y(a,z) = \sum_{n=-\infty}^{\infty} a_{(n)}z^{-n-1}$ を用いて述べられることが多いので，他の文献を参照する場合には注意されたい。。

(V4) 真空ベクトル 1 について，任意の $a \in V$ に対して

$$a_{(n)}1 = \begin{cases} a, & (n=-1), \\ 0, & (n \geq 0), \end{cases} \quad 1_{(n)}a = \begin{cases} a, & (n=-1), \\ 0, & (n \neq -1). \end{cases} \tag{A.4}$$

(V5) 共形ベクトル $\omega$ について

$$\omega_{(n)}\omega = \begin{cases} 2\omega, & (n=1), \\ (c_V/2)1, & (n=3), \\ 0, & (n=2, n \geq 4). \end{cases} \tag{A.5}$$

(V6) 任意の $a \in V$ に対して $L_{-1}a = a_{(-2)}1$ となる。

(V7) 各 $k$ について $V^k$ は有限次元である。

**頂点作用素代数の上の加群**

頂点作用素代数 $V$ の斉次元 $a \in V^k$ に対して，$L_0$ の固有値 $k$ を $a$ の共形ウェイトといい，$\Delta(a)$ で表す。

ベクトル空間 $M$ および整数 $n$ でパラメトライズされた可算個の線型写像

$$V \to \mathrm{End}_{\mathbf{C}}(M), \quad a \mapsto J_n^M(a) \tag{A.6}$$

が与えられたとする。

頂点作用素代数 $V$ に対して，このようなデータの与えられたベクトル空間 $M$ であって，以下の条件を満たすようなものを $V$-加群という。

(M1) 任意のベクトル $v \in M$ に対して，ある自然数 $N$ が存在して，$n \geq N$ ならば $J_n(a)v = 0$ がすべての $a \in V$ に対して成立する。 (註23)

(M2) 任意の $\ell, m, n \in \mathbb{Z}$ および $a, b \in V$ に対して

$$\begin{aligned} &\sum_{i=0}^{\infty} \binom{\ell + \Delta(a) - 1}{i} J^M_{\ell+m+n}(a_{(n+i)}b) \\ &\quad = \sum_{i=0}^{\infty} (-1)^i \binom{n}{i} \left( J^M_{\ell+n-i}(a) J^M_{m+i}(b) - (-1)^n J^M_{m+n-i}(b) J^M_{\ell+i}(a) \right) \end{aligned} \tag{A.7}$$

(M3) 真空ベクトル 1 について，

$$J_n(1) = \begin{cases} 1, & (n=0), \\ 0, & (n \neq 0). \end{cases} \tag{A.8}$$

特に共形ベクトル $\omega$ を考え，$L_n^M = J_n^M(\omega)$ とおく。すると，条件 (V5) および条件 (M2) により，$M$ 上の作用素 $L_n^M$ は Virasoro 代数の交換関係を満足する。

$$[L_m^M, L_n^M] = (m-n)L^M_{m+n} + \frac{m^3 - m}{12}\delta_{m+n,0} c_V 1_M. \tag{A.9}$$

23. 自然数 $N$ がすべての $a \in V$ に対して一様にとれるところに注目していただきたい。

なお，斉次元 $a$ に対して $O_n^M(a) = J^M_{n-\Delta(a)+1}(a)$ とおき，$p = \ell + \Delta(a) - 1$, $q = m + \Delta(b) - 1$, $r = n$ とすれば，条件 (M2) は次のようになる。

$$\begin{aligned}&\sum_{i=0}^{\infty}\binom{p}{i}O^M_{p+q-i}(a_{(r+i)}b)\\&\quad=\sum_{i=0}^{\infty}(-1)^i\binom{r}{i}O^M_{p+r-i}(a)O^M_{q+i}(b)-\sum_{i=0}^{\infty}(-1)^{r+i}\binom{r}{i}O^M_{q+r-i}(b)O^M_{p+i}(a).\end{aligned}\tag{A.10}$$

また，$O_n^M(L_{-1}a) = -nO^M_{n-1}(a)$ が成立する。

**普遍展開環**

頂点作用素代数 $V$ のループ化 $\hat{V} = V \otimes_{\mathbb{C}} \mathbb{C}[t, t^{-1}]$ を考え，この空間の自己準同型 $\hat{T} : \hat{V} \to \hat{V}$ を次のように定義する。

$$\hat{T}(a \otimes t^n) = L_{-1}a \otimes t^n + na \otimes t^{n-1} \tag{A.11}$$

写像 $\hat{T}$ の余核を考え，それを $\mathfrak{g} = \mathrm{Coker}\,\hat{T}$ とおく。すると，括弧積

$$[a \otimes t^m, b \otimes t^n] = \sum_{i=0}^{\infty}\binom{m}{i}a_{(i)}b \otimes t^{m+n-i} \tag{A.12}$$

は $\mathfrak{g}$ 上の Lie 代数の構造を誘導する。

ここで，斉次元 $a \in V$ に対して $J_n(a) = a \otimes t^{n+\Delta(a)-1}$ とおき，この元に次数 $-n$ を与えると，$\mathfrak{g} = \bigoplus_d \mathfrak{g}(d)$ は次数 Lie 代数となる。その普遍展開環 $\mathrm{U}(\mathfrak{g})$ を考えると，Lie 代数 $\mathfrak{g}$ の次数付けは環 $\mathrm{U}(\mathfrak{g})$ の次数付け $\mathrm{U}(\mathfrak{g}) = \bigoplus_{d=-\infty}^{\infty}\mathrm{U}(\mathfrak{g})(d)$ を誘導する。そこで，$\mathrm{F}_n\mathrm{U}(\mathfrak{g}) = \bigoplus_{d\le n}\mathrm{U}(\mathfrak{g})(d)$ とおき，

$$\mathrm{I}_n(\mathrm{U}(\mathfrak{g}))(d) = \mathrm{U}(\mathfrak{g})(d) \cap \big(\mathrm{U}(\mathfrak{g}) \cdot \mathrm{F}_n\mathrm{U}(\mathfrak{g})\big) \tag{A.13}$$

とする。そこで，Lie 代数 $\mathfrak{g}$ の普遍展開環 $\mathrm{U}(\mathfrak{g})$ の各斉次部分空間ごとの完備化を

$$\hat{\mathrm{U}}(\mathfrak{g}) = \bigoplus_d \hat{\mathrm{U}}(\mathfrak{g})(d), \quad \hat{\mathrm{U}}(\mathfrak{g})(d) = \varprojlim_n \mathrm{U}(\mathfrak{g})/\mathrm{I}_n(\mathrm{U}(\mathfrak{g}))(d) \tag{A.14}$$

と定める。これは次数環となる。

関係式 (A.7) において，$J_n^M(a)$ 等を $J_n(a)$ 等と置き換え，移項したものを考える。

$$\begin{aligned}&\sum_{i=0}^{\infty}(-1)^i\binom{n}{i}J_{\ell+n-i}(a)J_{m+i}(b)-\sum_{i=0}^{\infty}(-1)^{n+i}\binom{n}{i}J_{m+n-i}(b)J_{\ell+i}(a)\\&\quad-\sum_{i=0}^{\infty}\binom{\ell+\Delta(a)-1}{i}J_{\ell+m+n}(a_{(n+i)}b)=0\end{aligned}\tag{A.15}$$

この左辺は，$\hat{\mathrm{U}}(\mathfrak{g})(-\ell-m-n)$ に属する斉次元である。従って，この形の元で生成された $\hat{\mathrm{U}}(\mathfrak{g})$ の両側イデアル B は斉次イデアルである。このイデアル B の斉次部分空間ごとの閉包をとって得られる空間 $\hat{\mathrm{B}}$ を考えると，これも斉次イデアルとなる。そこで，斉次イデアル $\hat{\mathrm{B}}$ による $\hat{\mathrm{U}}(\mathfrak{g})$ の商を $\mathbf{U}(V)$ と定義し，頂点作用素代数 $V$ の普遍展開環と呼ぶ。

なお，関係式 (A.15) のうち，$n \ge 0$ のものは Lie 代数 $\mathfrak{g}$ の交換関係から得られるので，実質的に $n < 0$ のもののみ考えれば十分である。

## 文献


[DLM] C.-Y. Dong, H.-S. Li and G. Mason: Regularity of rational vertex operator algebras. Adv. Math. **132** (1997), no. 1, 148–166.

[FrZ] I.B. Frenkel and Y.-C. Zhu: Vertex operator algebras associated to representations of affine and Virasoro algebras. Duke Math. J. **66**, (1992), no. 1, 123–168.

[GaN] M.R. Gaberdiel and A. Neitzke: Rationality, quasirationality and finite $W$-algebras. Comm. Math. Phys. **238**, (2003), no. 1-2, 305–331.

[Gab] P. Gabriel: Des catégories abéliennes. Bull. Soc. Math. France **90**, (1962), 323–448.

[Kac] Victor G. Kac: Infinite-dimensional Lie algebras. Third edition. Cambridge University Press, Cambridge, 1990.

[KaR] V. Kac and A. Radul: Quasi-finite highest weight modules over the Lie algebra of differential operators on the circle. Commun. Math. Phys. **157**, (1993), 429–457.

[MaN] A. Matsuo and K. Nagatomo: Axioms for a vertex algebra and the locality of quantum fields. MSJ Memoirs, 4. Mathematical Society of Japan, Tokyo, 1999.

[MNT] A. Matsuo, K. Nagatomo and A. Tsuchiya: Quasi-finite algebras graded by Hamiltonian and vertex operator algebras. Preprint. (math.QA/0505071.)

[NaT] K. Nagatomo and A. Tsuchiya: Conformal field theories associated to regular chiral vertex operator algebras I: theories over the projective line. Duke Math. J. **128** (2005), no. 3, 393–471.

[TUY] A. Tsuchiya, K. Ueno and Y. Yamada: Conformal field theory on universal family of stable curves with gauge symmetries. Integrable systems in quantum field theory and statistical mechanics, 459–566, Adv. Stud. Pure Math., **19**, Academic Press, Boston, MA, 1989.

[Zhu] Y.-C. Zhu: Modular invariance of characters of vertex operator algebras. J. Amer. Math. Soc. **9**, (1996), no. 1, 237–302.

# Symplectic-fermionic 頂点作用素超代数の $\mathbb{Z}_2$-オービフォールド模型について

安部利之（愛媛大学理学部）

## 1 序

頂点作用素代数の表現論において重要な概念として,「有理性」と「$C_2$-有限性」がある．有理性は $\mathbb{Z}_{\geq 0}$-次数付けを持つ加群の完全可約性を表し，$C_2$-有限性は既約指標の存在と有限生成加群の組成列の有限性を導く頂点作用素代数自身の性質である．よく知られた頂点作用素代数の例として，ヴィラソロ頂点作用素代数，アファイン頂点作用素代数そして格子頂点作用素代数などがあげられるが，これらの模型においては有理性と $C_2$-有限性が同時に成立している．このことから１０年ほど前には有理性と $C_2$-有限性は同値な性質と考えられていた．

当時，有理性と $C_2$-有限性を満たす頂点作用素代数は Verlinde 公式と呼ばれる既約指標のモジュラー変換則とフュージョン則の間の不思議な関係が成立する事も予想されており（現在では証明された），実際，上に挙げた例で有理性と $C_2$-有限性を満たす物は Verlinde 公式によるフュージョン則がフュージョン則と一致している．しかしそのころから共形場理論の分類問題において現れた logarithmic な有理的共形場理論が研究され始めた．この共形場理論においては既約指標などは計算できるけれども，Verlinde 公式でフュージョン則を計算すると負の整数が現れ，intertwining 作用素の空間の次元とは解釈できない現象が起きる．この模型の出現は $C_2$-有限であるが，有理的でない頂点作用素代数の存在を予想させた．そこで本講演では，この模型のある構成法を一般化し，非有理かつ $C_2$-有限な頂点作用素代数を構成したのでそのことについて報告する．

## 2 $c=-2$ triplet 代数の実現

logarithmic な共形場理論のモデルとして triplet 代数が挙げられる．自然数 $p(\geq 2)$ に対し，中心電荷が $c=c_{p,1}=1-\frac{6(p-1)}{p}$ である Virasoro 元と 3 つの重み $2p-1$ の特異ベクトル生成される頂点作用素代数で適当な関係式を満たす物として構成される．対応する頂点作用素代数が非有理であることは知られていた ([FGST]) が，最近（本研究集会と報告集の原稿の締め切りの間に），$C_2$-有限であることが [CF] によって証明された．

さて $p=2$ つまり $c=-2$ の triplet 代数の実現としては次のような構成が知られている．$\mathfrak{h}=\mathbb{C}e\oplus\mathbb{C}f$ を二次元ベクトル空間とし，$\mathfrak{h}$ 上の非退化双線形型式 $\langle\cdot,\cdot\rangle$ を

$$\langle f,e\rangle=-\langle e,f\rangle=1,\quad \langle e,e\rangle=\langle f,f\rangle=0$$

で定める．そのとき，$\widehat{\mathfrak{h}}=\mathfrak{h}\otimes\mathbb{C}[t^{\pm 1}]\oplus\mathbb{C}K$ には偶部分を $\mathbb{C}K$，奇部分を $\mathfrak{h}\otimes\mathbb{C}[t^{\pm 1}]$ とし，交換関係を

$$\{\psi\otimes t^m,\phi\otimes t^n\}=m\langle\psi,\phi\rangle\delta_{m+n,0}K, \tag{1}$$

$$[K,\widehat{\mathfrak{h}}]=0 \tag{2}$$

と定義することによって Lie 超代数の構造が入る．このとき結合代数

$$\mathcal{A}=U(\widehat{\mathfrak{h}})/\langle K-1\rangle \tag{3}$$

を考える，ここで，$U(\widehat{\mathfrak{h}})$ は Lie 超代数 $\widehat{\mathfrak{h}}$ の普遍包絡代数，1 は $U(\widehat{\mathfrak{h}})$ の単位元で，$\langle K-1\rangle$ は $K-1$ で生成されるイデアルを表す．$\mathcal{A}$ には，$\widehat{\mathfrak{h}}$ の $\mathbb{Z}_2$-grading から 自然に $\mathbb{Z}_2$-grading が誘導されることがわかる．

頂点作用素超代数を構成するために左 $A$-加群 $T$ を次のように構成する．$I_{\geq 0}$ を $\psi \otimes t^n\,(\psi \in \mathfrak{h}, n \in \mathbb{Z}_{\geq 0})$ で生成される $A$ の左イデアルとする．この時，左 $A$-加群 $T$ を

$$T = A/I_{\geq 0} \tag{4}$$

で定める．その構成法からベクトル空間として $T$ は外積代数 $\Lambda(\mathfrak{h} \otimes t^{-1}\mathbb{C}[t^{-1}])$ に同型であることがわかる．従って，$\psi_{(n)}$ を $\psi \otimes t^n\,(\psi \in \mathfrak{h}, n \in \mathbb{Z})$ の $T$ 上の左作用とすると，$T$ は $v = \psi^1_{(-n_1)} \cdots \psi^r_{(-n_r)} 1\,(\psi^i \in \mathfrak{h}, n_i \in \mathbb{Z}_{>0})$ の形の元達で張られることがわかる，ただし

$$1 = 1 + I_{\geq 0}$$

とおいた．このベクトル $v$ に対し，対応する頂点作用素は，

$$Y(1, z) = \mathrm{id}, \tag{5}$$

$$\psi(z) = \sum_{n \in \mathbb{Z}} \psi_{(n)} z^{-n-1},\ (\psi \in \mathfrak{h}), \tag{6}$$

$$Y(v, z) = {:}\partial^{(n_1-1)}\psi^1(z) \cdots \partial^{(n_r-1)}\psi^r(z){:} \tag{7}$$

で与えられる．ここで $\partial^{(n)} = \frac{1}{n!}\left(\frac{d}{dz}\right)^n$ で，正規積は ${:}\psi_{(n)}{:} = \psi_{(n)}$ と

$${:}\psi_{(n)}\psi^1_{(n_1)} \cdots \psi^r_{(n_r)}{:} = \begin{cases} \psi_{(n)}{:}\psi^1_{(n_1)} \cdots \psi^r_{(n_r)}{:} & \text{if } n < 0, \\ (-1)^r {:}\psi^1_{(n_1)} \cdots \psi^r_{(n_r)}{:}\psi_{(n)} & \text{if } n \geq 0 \end{cases}$$

によって帰納的に定める．このようにして，組 $(T, Y(\cdot, z), 1)$ が頂点超代数の構造を持つようにできる．更に，$\omega = e_{(-1)}f_{(-1)}1$ と Virasoro 元をとることによって，$(T, Y(\cdot, z), 1, \omega)$ は中心電荷 $-2$ の頂点作用素超代数となる．この頂点作用素超代数の偶部分 $T^+$ が $c = -2$ triplet 超代数の実現を与える．

## 3 Symplectic-fermionic 頂点作用素超代数

$c = -2$ triplet 代数の構成法を見ると，その構成法は次のように一般化できることが容易にわかる．まず二次元ベクトル空間 $\mathfrak{h}$ とその上の双線形型式 $\langle \cdot, \cdot \rangle$ を，一般次元ベクトル空間 $\mathfrak{h}$ とその上の非退化歪対称双線形型式 $\langle \cdot, \cdot \rangle$ に取り直して同様の構成法を行う．このとき $\mathfrak{h}$ は偶数次元となり，以下

$$d = \frac{\dim \mathfrak{h}}{2} (\in \mathbb{Z}_{\geq 0})$$

とおくことにする．この設定から得られる $T$ に対応する頂点作用素超代数を **symplectic-fermionic 頂点作用素超代数**と呼び，$SF$ と書くことにする．Virasoro 元は，$\mathfrak{h}$ の基底 $\{e^i, f^i\}_{i=1,2,\ldots,d}$ で

$$\langle f^i, e^j \rangle = -\langle e^j, f^i \rangle = \delta_{i,j}, \quad \langle f^i, f^j \rangle = \langle e^i, e^j \rangle = 0 \tag{8}$$

を満たすものをとることにより，

$$\omega = \sum_{i=1}^{d} e^i_{(-1)} f^i_{(-1)} 1$$

で与えられる．この頂点作用超代数 $(SF, Y(\cdot, z), 1, \omega)$ は単純で，中心電荷は $-2d$ となることがわかる．更に，$L_0 = \omega_{(1)}$ としたとき，$SF$ は $L_0$ の固有空間に分解されるがその固有値（重みと呼ぶ）は非負整数となる；

$$SF = \bigoplus_{n=0}^{\infty} SF_n, \quad SF_n = \{u \in SF \mid L_0 u = nu\}.$$

$SF$ の主な性質について挙げてみる．そのために $C_2$-有限性と有理性の定義を思い出そう．

**定義 1.** $V$ をすべての重みが整数であるような頂点作用素超代数とし，$C_2(V)$ を $a_{(-2)}b\,(a,b\in V)$ の形の元で張られる $V$ の部分空間とする．$V/C_2(V)$ が有限次元となるとき，$V$ は $C_2$-有限であると呼ぶ．

**定義 2.** $V$ をすべての重みが整数であるような頂点作用素超代数とする．$\mathbb{Z}_{\geq 0}$-grading を持つ $V$-加群 $M=\bigoplus_{n=0}^{\infty}M_n$ で

$$a_{(n)}M_m\subset M_{k+m-n-1}\,(a\in V_k, m,n\in\mathbb{Z})$$

を満たす物が常に完全可約であるとき $V$ は**有理的**であるという．

まず容易にわかる事実として次の命題を得る．

**命題 1.** 頂点作用素超代数 $SF$ は $C_2$-有限．

*Proof.* ベクトル $\psi^1_{(-n_1)}\cdots\psi^r_{(-n_r)}1\,(\psi^i\in\mathfrak{h}, n_i\in\mathbb{Z}_{>0})$ はある $n_i$ が 2 以上ならば $C_2(SF)$ に属するので全射線形写像 $\Lambda(\mathfrak{h})\to SF/C_2(SF)$, $\psi^1\wedge\cdots\wedge\psi^r\mapsto\psi^1_{(-1)}\cdots\psi^r_{(-1)}1$ を得る．従って，$SF/C_2(SF)$ は有限次元となる． □

また $SF$ の直既約，可約加群が次のように構成できる．$I_{>0}$ を $\mathcal{A}$ の $\psi\otimes t^n\,(\psi\in\mathfrak{h}, n\in\mathbb{Z}_{>0})$ で生成される左イデアルとしたとき得られる左 $\mathcal{A}$-加群

$$\widehat{SF}:=\mathcal{A}/I_{>0}$$

とし，$v=\psi^1_{(-n_1)}\cdots\psi^r_{(-n_r)}1\in SF$ に対応する頂点作用素を (5)–(7) で定義する．このようにして得られる $SF$-加群が直既約な可約加群を与える．また $\widehat{SF}$ には $L_0$ の広義固有空間の直和として自然に $\mathbb{Z}_{\geq 0}$-grading が入る．このことより次のことがわかる．

**命題 2.** 頂点作用素超代数 $SF$ は非有理的である．

上の二つの命題から $SF$ は $C_2$-有限，非有理頂点作用素超代数の例を与えていることがわかる．

## 4 頂点作用素代数 $SF^+$

頂点作用素超代数の偶部分と奇部分をそれぞれ $SF^+, SF^-$ と書くことにする;

$$SF=SF^+\oplus SF^-.$$

この偶部分と奇部分は $SF$ の自己同型写像 $\theta: SF\to SF, u+v\mapsto u-v\,(u\in SF^+, v\in SF^-)$ の固定点のなす空間と $-1$-固有空間ととらえることができる．有限位数の自己同型写像によるオービフォールド模型が $C_2$-有限と有理性を保つという予想から，$C_2$-有限，非有理頂点作用素代数の例として $SF$ の偶部分 $SF^+$ が得られることが予測できるが，実際に成立することが証明できる．

**定理 1.** 頂点作用素代数 $SF^+$ は $C_2$-有限かつ非有理的である．

*Proof.* ( $C_2$-有限性) $T^+$ が $C_2$-有限であることは直接証明．一般の $\mathfrak{h}$ に関しては，$C_2$-有限頂点作用素代数 $\otimes_{i=1}^d T$ が $SF$ に共形的に（同じ Virasoro 元をもつ部分頂点作用素代数として）埋め込まれていることより導かれる．

( 非有理性 ) $\widehat{SF}$ は自然に偶部分 $\widehat{SF}^+$ と奇部分 $\widehat{SF}^-$ の直和に分解する．それぞれが直既約，可約 $SF^+$-加群を与える． □

自己同型写像 $\theta$ に対し，$\theta$-twisted $SF$-加群が同型をのぞきただ一つ存在する。その構成には [FLM] の twisted 加群の構成法を適用する．ベクトル空間 $\widehat{\mathfrak{h}}(\theta)=\mathfrak{h}\otimes t^{\frac{1}{2}}\mathbb{C}[t^{\pm 1}]\oplus\mathbb{C}K$ に Lie 超代数の構造を偶部分を $\mathbb{C}K$, 奇部分を $\mathfrak{h}\otimes t^{\frac{1}{2}}\mathbb{C}[t^{\pm 1}]$ とし、交換関係を (1)-(2) によって定める。こうしてできた Lie 超代数の普遍包絡代数を $K-1$ で生成されるイデアルで割って得られる超代数を $\mathcal{A}(\theta)$ と書くことにする;

$$\mathcal{A}(\theta)=U(\widehat{\mathfrak{h}}(\theta))/\langle K-1\rangle.$$

$I(\theta)$ を $\psi\otimes t^n\,(\psi\in\mathfrak{h}, n\in\frac{1}{2}+\mathbb{Z}_{\geq 0})$ で生成される左イデアルとし，その商左加群 $\mathcal{A}(\theta)/I(\theta)$ を $SF(\theta)$ 書くことにする。以前と同様に，$\psi\otimes t^n\,(\psi\in\mathfrak{h}, n\in\frac{1}{2}+\mathbb{Z}$ の $SF(\theta)$ 上の左作用を $\psi_{(n)}$ と書くことにする．このとき、次のようにして $SF(\theta)$ に $\theta$-twisted $SF$-加群の構造が入る。まず,

$$Y(1,z)=\mathrm{id},$$

と定義し，$v=\psi^1_{(-n_1)}\cdots\psi^r_{(-n_r)}1\,(\psi^i\in\mathfrak{h}, n_i\in\mathbb{Z}_{>0})$ の形の元に対し,

$$\psi^i(z)=\sum_{n\in\frac{1}{2}+\mathbb{Z}}\psi^i_{(n)}z^{-n-1},$$

$$W(v,z)=\,{}^{\circ}_{\circ}\partial^{(n_1-1)}\psi^1(z)\cdots\partial^{(n_r-1)}\psi^r(z){}^{\circ}_{\circ}$$

と定義する．更に係数 $c_{m,n}\in\mathbb{C}\,(m,n\in\mathbb{Z}_{\geq 0})$ を次の形式的巾級数展開

$$\sum_{m,n\geq 0}c_{mn}x^my^n=-\log\left(\frac{(1+x)^{\frac{1}{2}}+(1+y)^{\frac{1}{2}}}{2}\right),$$

によって定め，$SF$ 上の作用素 $\Delta(z)$ を

$$\Delta(z)=2\sum_{m,n\geq 0}\sum_{i=1}^{d}c_{mn}e^i_{(n)}f^i_{(m)}z^{-m-n}$$

で定義する．ここで $\{(e^i,f^i)\}_{1\leq i\leq d}$ は (8) を満たす $\mathfrak{h}$ の基底である．最後に $v=\psi^1_{(-n_1)}\cdots\psi^r_{(-n_r)}1$ に対する頂点作用素を

$$Y(v,z)=W(e^{\Delta(z)}v,z),$$

により定義すると，$(SF(\theta),Y(\cdot,z))$ は $\theta$-twisted $SF$-加群となる．この $\theta$-twisted $SF$-加群 $SF(\theta)$ も偶部分と奇部分に分解し，それぞれ $SF(\theta)^+$, $SF(\theta)^-$ と書くことにすると，どちらも自然に既約な $SF^+$-加群となることがわかる．次の結果は，一般の単純頂点作用素代数に対して予想されていることが，頂点作用素代数 $SF^+$ に対しても成立していることを示している．

**定理 2.** 任意の既約な $SF^+$-加群は，既約な $SF$-加群または *$\theta$-twisted* $SF$-加群を $SF^+$-加群とみたときの既約成分に同型である．すなわち，既約な $SF^+$-加群は，$SF^{\pm}$ もしくは $SF(\theta)^{\pm}$ のいずれかに同型である．

頂点作用素代数の既約加群の分類については，頂点作用素代数とその Zhu 代数と呼ばれる結合代数の表現論の関連によって実行されることが多い．実際 $SF^+$ の既約加群の分類は $SF^+$ の Zhu 代数の構造を調べ，Zhu 代数の既約加群を分類することにより与えられる．ここでは複雑になるので詳細は述べない．

## 5 跡関数のモジュラー不変性

頂点作用素代数 $V$ に対し，$V$-加群 $M$ が

$$M=\bigoplus_{n=0}^{\infty}M_{n+h},\quad M_{n+h}=\{u\in M\,|\,L_0u=(n+h)u\}$$

と $L_0$ の固有空間の直和に分解すると仮定する．このとき $q$ の形式的巾級数

$$ch_M(q)=\sum_{n=0}^{\infty}(\dim M_{n+h})q^{n+h-\frac{c}{24}}=\mathrm{tr}_M\,q^{L_0-\frac{c}{24}}$$

を $M$ の指標と呼ぶ，但し $c$ は $V$ の中心電荷である．$V$ が $C_2$-有限ならば，$\tau$ を上半平面の点とし，$q=e^{2\pi i\tau}$ とすると既約指標は上半平面上の正則関数となることが証明できる ([Z])．こうして得られる上半平面上の正則関数を跡関数といい $ch_M(\tau)$ と書くことにする．

頂点作用素代数 $SF^+$ に対し，既約指標は次のように計算できる．まず，

$$ch_{SF}(\tau)=\left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{2d},\quad ch_{SF(\theta)}(\tau)=\left(\frac{\eta(\tau)^2}{\eta(2\tau)\eta(\frac{\tau}{2})}\right)^{2d}$$

となることが容易にわかる，ここで $\eta(\tau)$ は Dedekind eta 関数である．また頂点作用素超代数の超跡関数 $sch_M=\mathrm{tr}_M\,\theta q^{L_0-\frac{c}{24}}$ も容易に計算できて，

$$sch_{SF}(\tau)=\eta(\tau)^{2d},\quad sch_{SF(\theta)}(\tau)=\left(\frac{\eta(\frac{\tau}{2})}{\eta(\tau)}\right)^{2d}.$$

よって既約 $SF^+$-加群の指標は

$$ch_{SF^\pm}(\tau)=\frac{1}{2}\left(ch_{SF}(\tau)\pm sch_{SF}(\tau)\right)=\frac{1}{2}\left(\left(\frac{\eta(2\tau)}{\eta(\tau)}\right)^{2d}\pm\eta(\tau)^{2d}\right),$$

$$ch_{SF(\theta)^\pm}(\tau)=\frac{1}{2}\left(ch_{SF(\theta)}(\tau)\pm sch_{SF(\theta)}(\tau)\right)=\frac{1}{2}\left(\left(\frac{\eta(\tau)^2}{\eta(2\tau)\eta(\frac{\tau}{2})}\right)^{2d}\pm\left(\frac{\eta(\frac{\tau}{2})}{\eta(\tau)}\right)^{2d}\right)$$

で与えられることがわかる．

一方，$ch_{SF}(\tau)$ 及び $sch_{SF}(\tau)$, $ch_{SF(\theta)}(\tau)$, $sch_{SF(\theta)}(\tau)$ のモジュラー変換則はよく知られている．そのモジュラー変換則により，次の命題を得る．

**命題 3.** 上半平面上の正則関数の集合

$$\{\tau^i sch_{SF}(\tau),\,ch_{SF}(\tau),\,ch_{SF(\theta)}(\tau),\,sch_{SF(\theta)}(\tau)\,|\,0\le i\le d\}$$

で張られる空間はモジュラー不変である．

ここで注目するのは既約指標だけではモジュラー不変にはならず，$2\pi i\tau=\log q$ の多項式を係数にこめるとモジュラー不変になることである．このことはもっと一般に，[M] において，$C_2$-有限で非有理な頂点作用素代数では既約指標だけではなく，interlocked 加群と呼ばれる加群の擬指標の概念を導入することにより説明されている．この interlocked 加群の定義には Zhu 代数の高次化を用いているため具体的には計算し辛いように見えるが，今の場合，加群のカテゴリーのおおよその構造（テンソル積はまだわかっていない）の雰囲気がわかっているのでどの加群が interlocked 加群に対応するのかはその加群の構造からわかる．そしてその加群の擬指標も計算できて，実際に上の命題のモジュラー不変な空間が擬指標たちで張られていることが確認できる．

フュージョン則の計算がこれからの課題だが，おそらくそれは 1 以下で 1 となる組は，

$$(SF^{\pm}, SF^{\pm}, SF^{+}), \quad (SF^{\pm}, SF^{\mp}, SF^{-}),$$
$$(SF(\theta)^{\pm}, SF(\theta)^{\pm}, SF^{+}), \quad (SF(\theta)^{\pm}, SF(\theta)^{\mp}, SF^{-})$$

及びこれらの組の $S_3$ による置換で得られる組のいずれかで与えられると期待している．

## 参考文献


[A] T. Abe, A $\mathbb{Z}_2$-orbifold model of the symplectic fermionic vertex operator superalgebra, math.QA/0503472.

[CF] N. Carqueville and M. Flohr, Nonmeromorphic operator product expansion and $C_2$-cofiniteness for a family of $W$-algebras, math-ph/0508015.

[FGST] B. Feigin, A. Gainutdinov, A. Semikhatov, I. Tipunin, Modular group representations and fusion in logarithmic conformal field theories and in the quantum group center, hep-th/0504093.

[FLM] I. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Appl. Math., Vol.134, Academic Press, Boston, 1988.

[M] M. Miyamoto, Modular invariance of vertex operator algebras satisfying $C_2$-cofiniteness. *Duke Math. J.* **122**, (2004), no. 1, 51–91.

[Z] Y.-C. Zhu, Modular invariance of characters of vertex operator algebras, *J. Amer. Math. Soc.* **9** (1996), 237–302.

# The fixed point subalgebra of a lattice vertex operator algebra by an automorphism of order three

田辺顕一朗　筑波大学大学院数理物質科学研究科
山田裕理　　一橋大学大学院経済学研究科

**概 要**

ある格子頂点作用素代数のある位数3の自己同型による固定点全体からなる部分代数の表現が決定できたことを報告する。詳細は我々のプレプリント [7] を参照して下さい。

## 1 動機

まず Frenkel-Lepowsky-Meurman による Moonshine 頂点作用素代数 $V^\natural$ の構成法 [4] を手短に紹介する。$\Lambda$ をリーチ格子とし、$\Lambda$ に付随する格子頂点作用素代数 $V_\Lambda$ を考える。$\Lambda$ の位数2の自己同型 $\Lambda \ni \alpha \mapsto -\alpha \in \Lambda$ を持ち上げて $V_\Lambda$ の位数2の自己同型 $\theta$ を構成し、それによる $V_\Lambda$ の固定点全体からなる部分頂点作用素代数 $V_\Lambda^\theta = \{u \in V \mid \theta(u) = u\}$ を考える。Frenkel-Lepowsky-Meurman は $V_\Lambda^\theta$ とある一つの既約 $V_\Lambda^\theta$ 加群 $(V_\Lambda^T)^\theta$ との直和 $V_\Lambda^\theta \oplus (V_\Lambda^T)^\theta$ に頂点作用素代数の構造が入ることを示した [4]。これが Moonshine 頂点作用素代数 $V^\natural$ である。彼らは同時に $V^\natural$ の自己同型群がモンスター単純群になることを Griess の結果に帰着させることによって示している。ここで $V_\Lambda^\theta$ 上で1, $(V_\Lambda^T)^\theta$ 上で $-1$ として定義される $V^\natural$ の位数2の自己同型はモンスター単純群の $2B$ 元となっている。

上記の構成法をリーチ格子の他の自己同型に対して考えてみることは自然である。現在我々はリーチ格子のある位数3の自己同型 $g$ に関して、以下に述べる設定でこの問題を考えている。$g$ による $V_\Lambda$ の固定点全体からなる部分頂点作用素代数 $V_\Lambda^g$ を考え、その特定の二つの既約 $V_\Lambda^g$ 加群 $W_1, W_2$ をとる ($W_1, W_2$ の取り方は既に分かっている)。直和 $W = V_\Lambda^g \oplus W_1 \oplus W_2$ を考える。次が予想されている。

(1) $W$ には頂点作用素代数の構造が入る。

(2) ((1) が出来たとして) $W$ は $V^\natural$ に同型である。また $V_\Lambda^g$ 上で1, $W_1$ 上で $e^{2\pi\sqrt{-1}/3}$, $W_2$ 上で $e^{4\pi\sqrt{-1}/3}$ で定義される $W$ の自己同型はモンスター単純群の $3B$ 元となる。

(1) の問題を解決する為には $W_i$ $(i=1,2)$ 上に頂点作用素代数の積をどう定義するか、また定義された積は頂点作用素代数の定義の条件を満たすかが問題となる。それらの問題の解決に大きな情報を与えてくれるものが $V_\Lambda^g$ の表現であり、最初にそこをきちんと決定する必要がある。つまり $V_\Lambda^g$ の既約加群を分類し、任意の加群の完全可約性を示し、さらに fusion rule を計算する必要がある。しかし、一般に頂点作用素代数の有限位数の自己同型群の固定点全体からなる部分代数の表現を決定することは、きれいな予想はあるものの簡単なことではない。

我々は $V_\Lambda^g$ の表現を決定する為に次の方法を採った。$L$ を $A_2$ 型ルート格子を $\sqrt{2}$ 倍した格子とし、$L$ に付随する頂点作用素代数 $V_L$ を考える。$L$ の自然な位数 3 の自己同型を $V_L$ の自己同型 $\tau$ に持ち上げ、$V_L^\tau=\{u\in V_L \mid \tau(u)=u\}$ とおく。実は $V_L^\tau$ の 12 個のテンソル積 $(V_L^\tau)^{\otimes 12}$ は $V_\Lambda^g$ の部分代数となっており、$V_\Lambda^g$ が $(V_L^\tau)^{\otimes 12}$ 加群としてどのように既約加群の直和に分解されるかは既に [5] において符号を用いて記述されている。したがって $V_L^\tau$ の表現 ($(V_L^\tau)^{\otimes 12}$ の表現はこれから直ちに分かる) が決定出来れば $V_\Lambda^g$ の表現の情報を得ることが出来る。

ここでは $V_L^\tau$ の既約加群の分類が出来た事、及び任意の $V_L^\tau$ 加群は完全可約であることを示す事が出来た事を報告する。

これから $V_\Lambda^g$ の表現を決定する為にはまだ解決しなければならない部分がいくつか残っており、現在進展中である。しかし、$V_\Lambda^g$ を直接扱うよりははるかに苦労は軽減されている。

## 2 $V_L^\tau$ の表現

ここでは先程出てきた $V_L^\tau$ の表現について述べていく。$L$ は $A_2$ 型ルート格子を $\sqrt{2}$ 倍した格子であった。$\beta_1$ と $\beta_2$ を $\langle\beta_i,\beta_i\rangle=4, \langle\beta_i,\beta_j\rangle=-2$ $(i\neq j)$ を満たす $L$ の $\mathbb{Z}$ 基底とする。$\beta_0=-\beta_1-\beta_2$ とおく。$\beta_1\mapsto\beta_2\mapsto\beta_0$ で定義される $L$ の位数 3 の自己同型を $\tau$ とおく。$\mathbb{C}[L]=\oplus_{\alpha\in L}\mathbb{C}e^\alpha$ を $L$ の群環とする。$\beta_i(-n)$, $(i\in\{1,2\}, n\in\mathbb{Z}_{>0})$ を変数として多項式環 $\mathbb{C}[\beta_i(-n)\mid i\in\{1,2\}, n\in\mathbb{Z}_{>0}]$ を考える。$\mathbb{C}[\beta_i(-n)\mid i\in\{1,2\}, n\in\mathbb{Z}_{>0}]$ と $\mathbb{C}[L]$ とのテンソル積

$$V_L=\mathbb{C}[\beta_i(-n)\mid i\in\{1,2\}, n\in\mathbb{Z}_{>0}]\otimes_{\mathbb{C}}\mathbb{C}[L]$$

には頂点作用素代数の構造が入るのであるが、それを $L$ に付随する格子頂点作用素代数という。$V_L$ 上には

$$\beta_{i_1}(-n_1)\cdots\beta_{i_k}(-n_k)\otimes e^\gamma\mapsto\tau(\beta_{i_1})(-n_1)\cdots\tau(\beta_{i_k})(-n_k)\otimes e^{\tau(\gamma)}$$

で位数 3 の自己同型が定義されるのであるが、それも $\tau$ で表すことにする。$V_L^\tau=\{u\in V_L\mid\tau(u)=u\}$ とおき、$\mathbf{1}=1\otimes e^0$ とおく。$V_L^\tau$ は次の 5 つの元で生成される

ことが分かっている [7].

$$
\begin{aligned}
\tilde{\omega}^1 &= \frac{1}{20}\sum_{i=0}^{2}\beta_i(-1)^2 1 - \frac{1}{5}\sum_{i=0}^{2}(e^{\beta_i}+e^{-\beta_i}),\\
J &= \frac{1}{6}\sum_{i=0}^{2}\beta_{i+1}(-2)(\beta_i(-1)-\beta_{i+2}(-1))1\\
&\quad +\sum_{i=0}^{2}(\beta_i(-1)-\beta_{i+2}(-1))(e^{\beta_{i+1}}-e^{-\beta_{i+1}}),\\
\tilde{\omega}^2 &= \frac{1}{30}\sum_{i=0}^{2}\beta_i(-1)^2 1 + \frac{1}{5}\sum_{i=0}^{2}(e^{\beta_i}+e^{-\beta_i}),\\
K &= -\frac{1}{9}\prod_{i=0}^{2}(\beta_i(-1)-\beta_{i+1}(-1))1\\
&\quad +\sum_{i=0}^{2}(\beta_i(-1)-\beta_{i+1}(-1))(e^{\beta_{i+2}}+e^{-\beta_{i+2}}),\\
P &= \sum_{i=0}^{2} e^{\beta_i}-e^{-\beta_i}.
\end{aligned}
$$

$M^{01}$ を $\tilde{\omega}^1$ と $J$ から生成される部分代数、$M^{02}$ を $\tilde{\omega}^2$ と $K$ から生成される部分代数とする。$M^{01}$ と $M^{02}$ は Fateev-Zamolodchikov[3] によって与えられた $W_3$ 代数と呼ばれる頂点作用素代数の、パラメータが特別な二つの場合の実現になっている。[3] ではそれらの既約加群達も与えられているが数学的な意味での分類はなされていない。$M^{01}$ の $M^{02}$ の既約加群の分類 ($M^{01}$ は 20 個で $M^{02}$ は 6 個) と、任意の加群が完全可約であることの証明は [2] と [6] とでなされている。

$M^0$ を $\tilde{\omega}^1$, $\tilde{\omega}^2$, $J$ と $K$ から生成される部分代数とすると、実は $M^0 \simeq M^{01}\otimes_{\mathbb{C}} M^{02}$ となるので $M^0$ の既約加群の数は $20\times 6 = 120$ であり、任意の $M^0$ 加群は完全可約であることが分かる。$W^0$ を $P$ から生成される $V_L^T$ の部分 $M^0$ 加群とする。$M^0$ と $W^0$ は非同型な既約 $M^0$ 加群になっている。この時、

**命題 1.** $V_L^T = M^0 \oplus W^0$.

が成り立つ。$M^0$ の表現は分かっているのでこの分解を用いて既約 $V_L^T$ 加群の分類することが出来る。少し専門用語 (twisted 加群、fusion rule、Zhu 代数等) を用いて概略を述べる。まず Dijkgraaf-Vafa-Verlinde-Verlinde[1] の予想に従えば、既約 $V_L^T$ 加群は $\tau^i$-twisted 既約 $V_L$ 加群 ($i=0,1,2$) を $V_L^T$ 加群として既約分解する事によって全て得られるはずである。そのようにして得られた 30 個 (同型なものは除いておく) の既約 $V_L^T$ 加群の集合を $\mathcal{N} = \{N_i\}_{i=0}^{29}$ ($N_0 = V_L^T$) で表す。$\tau^i$-twisted 既約 $V_L$ 加群 ($i=0,1,2$) の定義と、それらが $V_L^T$ 加群としてどのように既約分解するのかの記述は省略する。

$\mathcal{N}$ の元に対して個別に確認することで次の事が分かる。各 $0 \leq i \leq 29$ に対して $N_i$ は $M^0$ 加群として二つの既約 $M^0$ 加群の直和 $M^i \oplus W^i$ に既約分解される。またこれら 60 個の既約 $M^0$ 加群 $M^i$, $W^j$ $(0 \leq i, j \leq 29)$ 達は互いに非同型な既約 $M^0$ 加群となっている。既約 $M^0$ 加群の数は 120 であったから丁度半分の既約加群がここに表れているわけである。さらに fusion rule

$$(*)\ W^0 \times M^i = W^i, \quad W^0 \times W^i = M^i + W^i \quad (0 \leq i \leq 29)$$

が成立している。$N_i$ 中の二つの既約 $M^0$ 加群のどちらを $M^i$ とおくかはこの fusion rule から決める。$\mathcal{M} = \{M^i\}_{i=0}^{29}$, $\mathcal{W} = \{W^i\}_{i=0}^{29}$ とおき、$\mathcal{S} = \mathcal{M} \cup \mathcal{W}$ とおく。

次に任意の既約 $V_L$ 加群 $N$ は $M^0$ 加群として $M^i \oplus W^i$ $(0 \leq {}^{\exists} i \leq 29)$ と表せることを示していく。$M^0$ 加群として $N$ を既約分解した時、その各既約成分は $\mathcal{S}$ の元でなければいけない事は $M^{01}$ と $M^{02}$ の fusion rule を用いて簡単に分かる。その中の少なくとも一つの既約成分は $\mathcal{M}$ の元となっていることを示すことが証明で一番困難な部分である。$N$ が $M^0$ 加群として $\mathcal{W}$ の元である既約 $M^0$ 加群達の直和になったと仮定して、頂点作用素代数の表現を考察する際に標準的な道具である Zhu 代数 [8] の表現を用いて矛盾を導くのであるが、$V_L^+$ の Zhu 代数の関係式をたくさん得るためにここで計算機を用いている。

$M^i \in \mathcal{M}$ が既約成分に表れれば、$N = M^i \oplus W^i$ となることは fusion rule $(*)$ を用いて直ちに分かる。最後に $M^0$ 加群としての構造が $M^i \oplus W^i$ となる既約 $V_L^+$ 加群は一意的に決まる事は簡単な議論で示すことが出来る。以上から任意の既約 $V_L^+$ 加群は $\mathcal{N}$ のどれかの元に同型であることが分かり、既約加群の分類は完了する。

任意の $V_L^+$ 加群は完全可約である事も同様の議論で示す事が出来る。得られた結果をまとめておく。

**定理 2.** (1) 既約 $V_L^+$ 加群の同型類の個数は 30 である.

(2) 全ての $V_L^+$ 加群は完全可約である.

(3) $V_L^+$ は $C_2$ 有限である.

## 参考文献


[1] R. Dijkgraaf, C. Vafa, E. Verlinde, and H. Verlinde, The operator algebra of orbifold models, *Comm. Math. Phys.* **123** (1989), 485–526.

[2] C. Dong, C.H. Lam, K. Tanabe, H. Yamada and K. Yokoyama, $\mathbb{Z}_3$ symmetry and $W_3$ algebra in lattice vertex operator algebras, *Pacific J. Math.* **215** (2004), 245–296.

[3] V. A. Fateev and A. B. Zamolodchikov, Conformal quantum field theory models in two dimensions having $Z_3$ symmetry, *Nuclear Phys.* **280**(1987), 644–660.

[4] I. B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. **134**, Academic Press, 1988.

[5] K. Kitazume, C.H. Lam and H. Yamada, 3-state Potts model, moonshine vertex operator algebra and $3A$ elements of the monster group, *Internat. Math. Res. Notices*, No. **23** (2003), 1269–1303.

[6] M. Kitazume, M. Miyamoto and H. Yamada, Ternary codes and vertex operator algebras, *J. Algebra* **223** (2000), 379–395.

[7] K. Tanabe and H. Yamada, The fixed point subalgebra of a lattice vertex operator algebra by an automorphism of order three, preprint(math.QA/0508175).

[8] Y. Zhu, Modular invariance of characters of vertex operator algebras, *J. Amer. Math. Soc.* **9** (1996), 237–302.

# McKay's observation and vertex operator algebras generated by two conformal vectors of central charge 1/2

Ching Hung Lam
台湾国立成功大学

山田裕理
一橋大学経済学研究科

山内 博*
東京大学大学院数理科学研究科
日本学術振興会特別研究員 PD

2005年6月27日

## 1 McKay's observation

今回の愛媛での講演ではモンスター散在型有限単純群 $\mathbb{M}$ と拡大 $E_8$ 型 Dynkin 図形に関する McKay observation について、頂点作用素代数を用いてその解明を目指す Ching Hung Lam, 山田裕理両氏との共同研究で分かったことを報告致しました。モンスターの対合 (involution) には [ATLAS] において 2A-共役類と 2B-共役類と呼ばれる二つの共役類があります。今回の話では 2 個の 2A 元に注目します。2A-共役類には 6-互換性 (6-transposition property) と呼ばれる性質が成り立ちます。これは $\alpha, \beta \in \mathbb{M}$ をモンスターの 2A-共役類の元とすると、その積 $\alpha\beta$ の位数は常に 6 以下になっていることを意味します。より詳しく、$\alpha\beta$ の属する共役類 $(\alpha\beta)^{\mathbb{M}}$ は以下の 9 種類になることが知られています:

1A, 2A, 3A, 4A, 5A, 6A, 4B, 2B, または 3C.

*講演者

J. McKay は文献 [Mc] において、ここに現れる数字は丁度拡大 $E_8$ 型 Dynkin 図形のラベルと一致することに気がつきました。


(1)

この類似は偶然かも知れませんが、もしかしたらモンスターと $E_8$ には何か関係があるのではないか？というのが McKay's observation です。この不思議な関係を頂点作用素代数を用いて説明しようというのが私たちの研究テーマです。

## 2 頂点作用素代数からのアプローチ

頂点作用素代数の立場からは、モンスターは Frenkel, Lepowsky そして Meurman が構成したムーンシャイン頂点作用素代数 $V^\natural$ [FLM] の自己同型群として定義することができます。そこで $V^\natural$ の頂点作用素代数構造を調べることで $E_8$ との関係を探そうという訳です。モンスターと $V^\natural$ の間には単に作用があるというのではなく、互いの構造に密接な関係があることが分かっています。特に注目したい結果として、Conway-宮本によるモンスターの 2A 元と $V^\natural$ の中心電荷 1/2 のヴィラソロ元の間の一対一対応があります。

一般に、頂点作用素代数 $V = \oplus_{n\geq 0} V_n$ において、ベクトル $e \in V_2$ がヴィラソロ元[1]であるとは、その頂点作用素 $Y(e,z) = \sum_{n\in\mathbb{Z}} e_{(n)} z^{-n-1}$ の展開係数を $L^e(m) := e_{(m+1)}$ とおいたときに、これらが $V$ 上にヴィラソロ代数の表現をを生成することとします:

$$[L^e(m), L^e(n)] = (m-n)L^e(m+n) + \delta_{m+n,0}\frac{m^3-m}{12}c.$$

ここで $c$ はスカラーであり、$e$ の 中心電荷 (central charge) と呼ばれます。$e$ がヴィラソロ元であるならば、$e$ はヴィラソロ頂点作用素代数を $V$ の部分代数として生成します。これを $\mathrm{Vir}(e)$ と書くことにします。今、$e$ が中心電荷 1/2 であり、$\mathrm{Vir}(e)$ が単純である場合、即ち $\mathrm{Vir}(e) \simeq L(1/2, 0)$ である場合を考えます。$L(1/2,0)$-加群は全て完全可約であり、3 つの既約表現 $L(1/2,0)$, $L(1/2,1/2)$, $L(1/2,1/16)$ を持つことが知られています (cf. [DMZ])。そこで $V$ を $\mathrm{Vir}(e)$-加群と見た場合、次のような分解を得ることができます:

$$V = V_e(0) \oplus V_e(1/2) \oplus V_e(1/16). \tag{2}$$

ここで $V_e(h)$ は $L(1/2,h)$ と同型な $\mathrm{Vir}(e)$-部分加群全ての和を表します。この分解 (2) を用いることで $V$ の自己同型を構成することができます。$V$ 上の線型変換 $\tau_e$ を $V_e(0) \oplus V_e(1/2)$

[1]論文 [M1, LYY1, LYY2] ではこれを conformal vector と呼んでいます。そのため本講演のタイトルも conformal vector となっています。conformal vector と Virasoro vector の定義には二つの流派があるのですが、最近の主流となっている用法に従い、本稿ではこの定義を採用しています。

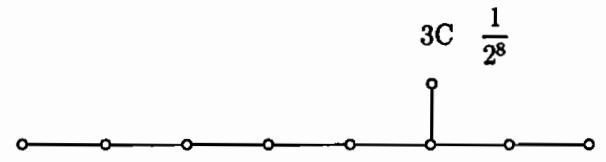
上 1 倍で、$V_e(1/16)$ 上 $-1$ 倍で定めます。このとき $\tau_e$ は $V$ の頂点作用素代数構造に関する自己同型を定めます (cf. [M1])。そのため、頂点作用素代数 $V$ に中心電荷 1/2 のヴィラソロ元があれば、$V$ 上の対合を定めることができます。この事実から、中心電荷 1/2 のヴィラソロ元であって、$\mathrm{Vir}(e) \simeq L(1/2, 0)$ となるものを本稿ではイジング元と呼ぶことにします。イジング元から定まる頂点作用素代数上の対合は特にムーンシャイン頂点作用素代数の研究において重要な役割を果たします。Conway と宮本氏の結果 [C, M1] から、$V = V^\natural$ とした場合、モンスター $\mathbb{M} = \mathrm{Aut}(V^\natural)$ の 2A-対合と $V^\natural$ のイジング元の間には一対一対応があるからです:

$$e \in V^\natural : \text{イジング元} \quad \overset{1:1}{\longleftrightarrow} \quad \tau_e \in \mathbb{M} : \text{2A-対合}$$

そのため、McKay observation を頂点作用素代数の問題と考えた場合、$V^\natural$ のイジング元と $E_8$ との関係を明確にできればいいことになります。

## 3 $V^\natural$ におけるイジング元

ムーンシャイン頂点作用素代数 $V^\natural$ は $V^\natural = \oplus_{n \geq 0} V^\natural_n$, $V^\natural_0 = \mathbb{C}\mathbf{1}$, $V^\natural_1 = 0$ なる次数分解を持っており、さらにウェイト 2 の空間 $V^\natural_2$ は Griess-Conway により構成されたモンスター不変な $1 + 196883 = 196884$ 次元可換非結合代数構造を持っています (cf. [C, G, FLM])。この可換代数構造を $\mathcal{B}$ と書くことにすると、$\mathrm{Aut}(\mathcal{B}) = \mathbb{M}$ であることが知られています (cf. [C, G, T])。$V^\natural_2 = \mathcal{B}$ において、二つのイジング元の関係は Conway によって調べられており、次のような面白い関係があることが分かっています。$e, f \in V^\natural$ をイジング元とすると、$V^\natural_2$ における内積 $\langle e, f \rangle$ は共役類 $(\tau_e \tau_f)^{\mathbb{M}}$ によって一意に定まっており、以下の様になっています (cf. [C])。




(3)

| 1A | 2A | 3A | 4A | 5A | 6A | 4B | 2B |
|---|---|---|---|---|---|---|---|
| $\frac{1}{4}$ | $\frac{1}{32}$ | $\frac{13}{2^{10}}$ | $\frac{1}{2^7}$ | $\frac{3}{2^9}$ | $\frac{5}{2^{10}}$ | $\frac{1}{2^8}$ | 0 |

さらに $V^\natural_2 = \mathcal{B}$ において $e, f$ が生成する部分代数の構造も類 $(\tau_e \tau_f)^{\mathbb{M}}$ によって一意に決定されることも [C] において示されています。これらの関係を $E_8$ の構造とどうやって結びつけるかが私たちの考えている問題であり、$E_8$ 型ルート格子の内積を 2 倍した格子 $\sqrt{2}E_8$ を使うとうまい対応が見つかることを [LYY1] で示しました。まず何故 $\sqrt{2}E_8$ に注目したのか説明したいと思います。

## 4 ルート系に付随したヴィラソロ元

Griess 代数 $\mathcal{B}$ の極大結合的部分代数の研究において、Dong et al. は [DLMN] においてルート格子 $R$ の内積を 2 倍した格子 $\sqrt{2}R$ に付随する格子頂点作用素代数 $V_{\sqrt{2}R}$ を調べ、ルート系に付随したヴィラソロ元を構成しました。$R$ を階数 $\ell$ の既約ルート格子、$\Phi(R)$ を $R$ のルート系、$h$ を $R$ の Coxeter 数として、$V_{\sqrt{2}R}$ において以下の元を考えます:

$$\begin{aligned} s_R &:= \frac{1}{4(h+2)} \sum_{\alpha\in\Phi(R)} \alpha_{(-1)}^2 \mathbf{1} - \frac{1}{h+2} \sum_{\alpha\in\Phi(R)} e^{\sqrt{2}\alpha}, \\ \tilde{\omega}_R &:= \frac{1}{2h(h+2)} \sum_{\alpha\in\Phi(R)} \alpha_{(-1)}^2 \mathbf{1} + \frac{1}{h+2} \sum_{\alpha\in\Phi(R)} e^{\sqrt{2}\alpha}. \end{aligned} \tag{4}$$

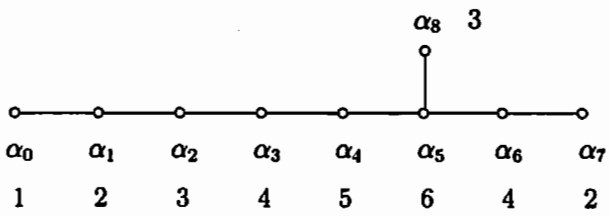
すると $s_R, \tilde{\omega}_R$ はそれぞれ中心電荷 $\ell h/(h+2), 2\ell/(h+2)$ のヴィラソロ元であることが [DLMN] において示されました。注目して頂きたいのは (4) における $s_R$ 及び $\tilde{\omega}_R$ の定義においてルート系 $\Phi(R)$ における平均を取っていることです。このことから $s_R$ 及び $\tilde{\omega}_R$ はルート系 $\Phi(R)$ に付随したヴィラソロ元と考えることができます。私たちが注目したのは $\tilde{\omega}_R$ の中心電荷です。この中心電荷を表にすると以下のようになります。

| $R$ | $A_n$ | $D_n$ | $E_6$ | $E_7$ | $E_8$ |
|---|---|---|---|---|---|
| c.c. of $\tilde{\omega}_R$ | $2n/(n+3)$ | 1 | 6/7 | 7/10 | 1/2 |

$R$ として $E_8$ を取ると、$\tilde{\omega}_{E_8}$ は中心電荷 1/2 になり、イジング元になることが分かります。先ほども述べたように、$\tilde{\omega}_{E_8}$ は $E_8$ のルート系から定まるヴィラソロ元ですから、$V_{\sqrt{2}E_8}$ のイジング元 $\tilde{\omega}_{E_8}$ と $V^\natural$ の関係が McKay observation を考える上で重要であると気づきました[2]。

## 5 $E_8$ からくる対称性

$\alpha_i$ $(0 \le i \le 8)$ をルート、即ち $\langle \alpha_i, \alpha_i \rangle = 2$ なる元として、以下の Coxeter 図形から定まる格子 $\bigoplus_{0\le i\le 8} \mathbb{Z}\alpha_i$ を考えます:




(5)

[2] $\tilde{\omega}_{E_8}$ と $V^\natural$ の関係はすでに [M2] において考えられています。定義から $\tilde{\omega}_{E_8} \in V^+_{\sqrt{2}E_8}$ であり、[M2] における $V^\natural$ の再構成において $V^+_{\sqrt{2}E_8}$ 及び $\tilde{\omega}_{E_8}$ は重要な役割を果たしています。

$n_i$ を (5) において $\alpha_i$ につけられたラベルとします。このとき $E_8$ 型ルート格子は以下のように実現することができます:

$$E_8 = \bigoplus_{i=0}^{8} \mathbb{Z}\alpha_i \Big/ \left( \sum_{i=0}^{8} n_i \alpha_i = 0 \right). \tag{6}$$

今、$\alpha_i$ をひとつとり、固定します。(6) で定めた $E_8$ の部分格子 $L^i := \bigoplus_{j \neq i} \mathbb{Z}\alpha_j$ を考えます。このとき次のような剰余分解ができます。

$$E_8 = \bigsqcup_{k=0}^{n_i-1} (k\alpha_i + L^i).$$

よって剰余群 $E_8/L^i$ の位数は $n_i$ になることが分かります。この対称性は格子頂点作用素代数 $V_{\sqrt{2}E_8}$ に持ち上げることができます。$L^i \hookrightarrow E_8$ から $V_{\sqrt{2}L^i} \hookrightarrow V_{\sqrt{2}E_8}$ であり、$E_8/L^i = \{k\alpha_i + L^i \mid 0 \leq k \leq n_i - 1\}$ ですから $V_{\sqrt{2}E_8}$ は次のように分解します:

$$V_{\sqrt{2}E_8} = \bigoplus_{k=0}^{n_i-1} V_{\sqrt{2}(k\alpha_i + L^i)}. \tag{7}$$

このとき $V_{\sqrt{2}E_8}$ 上の線型同型 $\rho_i$ を $V_{\sqrt{2}(k\alpha_i+L^i)}$ 上 $\exp(2\pi ik/n_i)$ 倍と定めると、$\rho_i$ は頂点作用素代数 $V_{\sqrt{2}E_8}$ の位数 $n_i$ の自己同型になります。こうして、(6) の各ラベルを位数に持つ $V_{\sqrt{2}E_8}$ の自己同型が定義されました。

## 6 Lam-山田-Y の observation

前節までに、$E_8$ のルート系から定まる $V_{\sqrt{2}E_8}$ のイジング元 $\tilde{\omega}_{E_8}$ と、拡大 $E_8$ 型図形のラベルから定まる $V_{\sqrt{2}E_8}$ の自己同型 $\rho_i$ が得られました。論文 [LYY1] において私たちは、$\tilde{\omega}_{E_8}$ と $\rho_i$ を用いることで $V^\natural$ における二つのイジング元が持つ関係を $V_{\sqrt{2}E_8}$ の中で実現できることを示しました。

**定理 1.** ([LYY1, LYY2]) 二つのイジング元 $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8} \in V_{\sqrt{2}E_8}$ について以下が成り立つ:

(1) 内積 $\langle \tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8} \rangle$ の値は式 (3) のものと一致する。

(2) $\tilde{\omega}_{E_8}$, $\rho_i\tilde{\omega}_{E_8}$ の生成する部分頂点作用素代数は Griess 代数を持ち、それは Conway が与えた $V_2^\natural = \mathcal{B}$ における二つのイジング元が生成するものと同型である。

(3) $\tau_{\tilde{\omega}_{E_8}}\tau_{\rho_i\tilde{\omega}_{E_8}} = \rho_i^{-2}$ on $V_{\sqrt{2}E_8}$ であり、それゆえ $n_i$ が奇数ならば $|\tau_{\tilde{\omega}_{E_8}}\tau_{\rho_i\tilde{\omega}_{E_8}}| = n_i$, 偶数ならば $|\tau_{\tilde{\omega}_{E_8}}\tau_{\rho_i\tilde{\omega}_{E_8}}| = n_i/2$ となる。

この結果から、$V^\natural$ における二つのイジング元の持つ関係は $V_{\sqrt{2}E_8}$ を通じて $E_8$ と関係していることが漠然とではありますが分かってきました。

ムーンシャイン頂点作用素代数 $V^\natural$ は [FLM] において Leech 格子に付随する格子頂点作用素代数 $V_\Lambda$ に $\mathbb{Z}_2$-軌道体構成法を用いることで構成されています。$\theta$ を $\Lambda$ 上 $-1$ 倍する計量同型とすると、$\theta$ は $\Lambda$ 上 fixed-point free に作用します。$\theta$ は $V_\Lambda$ 上の対合に持ち上げることができ、$\theta$ による $V_\Lambda$ の固有空間分解を $V_\Lambda = V_\Lambda^+ \oplus V_\Lambda^-$ とします。ここで $\theta$ は $V_\Lambda^\pm$ 上 $\pm 1$ 倍で作用するものとします。このとき $V^\natural$ は固定点のなす部分代数 $V_\Lambda^+$ の拡大 $V^\natural = V_\Lambda^+ \oplus V_\Lambda^{T+}$ として構成されています。これから、$\sqrt{2}E_8$ の $\Lambda$ への埋め込みを考えることによって $\tilde{\omega}_{E_8} \in V^+_{\sqrt{2}E_8} \hookrightarrow V_\Lambda^+ \hookrightarrow V^\natural$ が分かります。しかしながら、この構成法では $\rho_i\tilde{\omega}_{E_8}$ が $V_\Lambda^+$ に含まれているかどうかは直接見ることはできません。また、定理 1 (3) においては、対応する自己同型の位数が $V_{\sqrt{2}E_8}$ 上では $n_i$ にはなりません。しかし、Leech 格子 $\Lambda$ への埋め込み $\sqrt{2}E_8 \hookrightarrow \Lambda$ を考えると、位数 $n_i$ の自己同型が得られます。

**定理 2.** ([LYY1]) 埋め込み $\sqrt{2}E_8 \hookrightarrow \Lambda$ を用いた埋め込み $V_{\sqrt{2}E_8} \hookrightarrow V_\Lambda$ を考えると、$V_\Lambda$ 上では $|\tau_{\tilde{\omega}_{E_8}}\tau_{\rho_i\tilde{\omega}_{E_8}}| = n_i$ である。

私たちが見つけた $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ は今のところ $V^\natural$ ではうまく見えないのですが、もし $p > 2$ に対して $V^\natural$ を $V_\Lambda$ から $\mathbb{Z}_p$-軌道体構成法で構成することができれば、$V_{\sqrt{2}E_8}$ の二つのイジング元は自然に $V^\natural$ の中で見て取ることができ、さらに定理 2 からこれらは求める自己同型を生成するものと考えられます。$E_8$ の fixed-point free な計量同型 $\mu$ で、その $V_{\sqrt{2}E_8}$ への持ち上げが $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ の両方を固定しているものを考えます。埋め込み $\sqrt{2}E_8 \hookrightarrow \Lambda$ を通じてこの計量同型 $\mu$ が $\Lambda$ 上でも fixed-point free になっていれば、$|\mu| = p$ として $V_\Lambda$ の $\mu$ による $\mathbb{Z}_p$-軌道体構成を考えることができます。もしこの操作が実行可能ならば、ムーンシャイン VOA の一意性予想などから $V^\natural$ が得られることになり、$\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ の両方が $V^\natural$ の中で自然に見ることができます。$\mathbb{Z}_p$-軌道体構成法は頂点作用素代数の軌道体構成及びムーンシャイン頂点作用素代数の一意性予想に絡む有名な問題ですが、今のところ $\mu = \theta$ の場合、即ち $p = |\mu| = 2$ の場合しか解けていません。McKay observation を $\mathbb{Z}_p$-軌道体構成法を用いて説明できれば最良なのですが、その難しさからこの方法は現在のところ予想に留まっています。しかしながら、最近になって、Lam 氏と宮本氏によって $\tilde{\omega}_{E_8}, \rho\tilde{\omega}_{E_8}$ の $V_\Lambda^+$ への埋め込みなら可能だという結果がアナウンスされています。

## 7 $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ の生成する部分代数

前節までに、$V^\natural$ の Griess 代数において二つのイジング元が満たす関係式と同じ関係式を満たすイジング元の組 $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ を $E_8$ の構造を用いて $V_{\sqrt{2}E_8}$ の内部で実現しました。私たちの構成から、$V^\natural$ と $V_{\sqrt{2}E_8}$ の部分代数の間には Griess 代数のレベルでは同型が存在するという分かりました。では頂点作用素代数レベルではどうなのでしょうか。この問題を考えるには、私たちが考えた二つのイジング元 $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ が生成する $V_{\sqrt{2}E_8}$ の頂点作用素部分代数について知る必要があります。この部分代数は [LYY2] で考えられており、ワイル群の包含関係 $W(L^i) \leq W(E_8)$ を用いることで分かりやすく表示することができます。

式 (5) においてノード $\alpha_i$ をひとつ固定し、$E_8$ の部分格子 $L = L^i$ を既約成分の和に分解します。

$$L = R^1 \oplus \cdots \oplus R^r.$$

このとき $V_{\sqrt{2}E_8}$ の格子頂点作用素部分代数 $V_{\sqrt{2}L}$ は $V_{\sqrt{2}R^1} \otimes \cdots \otimes V_{\sqrt{2}R^k}$ を部分代数に持ちます。$L$ の各既約部分格子 $R^k$ について、式 (4) で定義される $V_{\sqrt{2}R^k}$ の二つのヴィラソロ元 $s_{R^k}, \tilde{\omega}_{R^k}$ を考えます。$s_{R^k}$ と $\tilde{\omega}_{R^k}$ は $V_{\sqrt{2}R^k}$ において互いに可換な元になっており、その和 $s_{R^k} + \tilde{\omega}_{R^k}$ は $V_{\sqrt{2}R^k}$ の共形ベクトルを定めます。このように共形ベクトルを互いに可換なヴィラソロ元の和に表すことを、共形ベクトルの直交分解といいます。$V_{\sqrt{2}E_8}$ 及び $V_{\sqrt{2}L}$ は同じ共形ベクトルを共有しており、$V_{\sqrt{2}L}$ の共形ベクトルは $V_{\sqrt{2}R^k}$ の共形ベクトルの直交和なので、$\omega$ を $V_{\sqrt{2}E_8}$ の共形ベクトルとすると、次のような直交分解が得られます:

$$\omega = s_{R^1} + \cdots + s_{R^k} + \tilde{\omega}_{R^1} + \cdots + \tilde{\omega}_{R^k}. \tag{8}$$

$L = R^1 \oplus \cdots \oplus R^r < E_8$ より $W(L) = W(R^1) \times \cdots \times W(R^k) < W(E_8) < \mathrm{Aut}(V_{\sqrt{2}E_8})$ ですから、$W(L)$ の $V_{\sqrt{2}E_8}$ への作用を考えることができます。式 (4) から $s_{R^k}, \tilde{\omega}_{R^k}$ はワイル群 $W(R^k)$ の作用で不変です。よって直交分解 (8) は $W(L)$ の作用で保たれることが分かります。ここで次で定義される $V_{\sqrt{2}E_8}$ の部分代数を考えます:

$M := s_{R^1} + \cdots + s_{R^k}$ を共形ベクトルに持つ $V_{\sqrt{2}E_8}$ 最大の頂点作用素部分代数

$X := \tilde{\omega}_{R^1} + \cdots + \tilde{\omega}_{R^k}$ を共形ベクトルに持つ $V_{\sqrt{2}E_8}$ 最大の頂点作用素部分代数

頂点作用素代数の交換団部分代数の一般論から、上の定義により $M$ 及び $X$ は well-defined になり、直交分解 (8) より $M$ と $X$ は $V_{\sqrt{2}E_8}$ において互いに可換な部分代数になっています。自己同型群の作用に関して、$M$ と $X$ は次のような特徴を持っています。

**命題 3.** $W(L) = W(R^1) \times \cdots \times W(R^k)$ の作用に関して、
(1) $M$ 上 $W(R^k), 1 \le k \le r$, はその中心を除いて非自明に作用している。
(2) $X$ 上 $W(L) = W(R^1) \times \cdots \times W(R^k)$ は自明に作用している。

ここで $V_{\sqrt{2}E_8}$ の二つのイジング元 $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ について考えます。$U$ を $\tilde{\omega}_{E_8}, \rho_i\tilde{\omega}_{E_8}$ の生成する $V_{\sqrt{2}E_8}$ の部分頂点作用素代数とすると、定義に基づく直接計算により次の事実が示せます。

**補題 4.** $U$ は $\tilde{\omega}_{R^1} + \cdots + \tilde{\omega}_{R^k}$ を共形ベクトルに持つ $V_{\sqrt{2}E_8}$ の頂点作用素部分代数である。

この補題から、$U$ は $X$ の部分代数になることが分かるのですが、実はこれらは一致することを [LYY2] で示しました。

**定理 5.** ([LYY2]) $U = X$.

この表示から、$U$ は $V_{\sqrt{2}E_8}$ において $W(L)$ が自明に作用する部分代数として理解でき、さらに $W(L)$ の作用を受け持つ $M$ と可換な最大の部分代数として特徴付けができることが分かりました。

## 8 $M$ と $U$ の双対性から分かること・期待されること

前節の結果から、$\tilde{\omega}_{E_8}$, $\rho_i\tilde{\omega}_{E_8}$ の生成する $V_{\sqrt{2}E_8}$ の部分代数 $U$ を考えた場合、$V_{\sqrt{2}E_8}$ において $U$ は $M\otimes U\subset V_{\sqrt{2}E_8}$ という形で入っており、$M$ 及び $U$ はワイル群 $W(L)$ の作用を見ることで分離できることが分かりました。Dual-pair の理論から、$M$ と $U$ にはある意味で互いに双対の関係があることが分かり、それゆえ $M$ と $U$ の両方を同時考えることで $U$ 自身の構造・表現がより詳細に調べることができます。この双対性を用いることで、[LYY2] において以下の結果を得ました。

**定理 6.** ([LYY2]) $U=\oplus_{n\geq 0}U_n$ を $\tilde{\omega}_{E_8}$, $\rho_i\tilde{\omega}_{E_8}$ で生成される $V_{\sqrt{2}E_8}$ の部分代数とすると、

(1) $X=U$ はその Griess 代数 $(=U_2)$ により生成されている。

(2) $U$ の既約表現の分類が完了。

$V_{\sqrt{2}E_8}$ における双対関係 $M\otimes U\subset V_{\sqrt{2}E_8}$ は、Glauberman–Norton's observation についてとても示唆的な関係を意味しているものと思われます。講演では詳しく話せませんでしたが、今後の研究課題としてこの話題について解説したいと思います。

論文 [GN] において、Glauberman–Norton は McKay observation について考察しており、McKay が提案した以上にミステリアスな関係があることを指摘しました。$\tau_1,\tau_2\in\mathbb{M}$ を 2A-元として、$\tau_1\tau_2$ の共役類を式 (1) のように並べた場合、式 (5) においてノード $\alpha_i$ が対応しているものとします。$L^i<E_8$ を今までと同じように考えると、ある 2B-元 $\theta\in\mathbb{M}$ が存在して、$\mathbb{M}$ における中心化群の構造について

$$C_{\mathbb{M}}(\tau_1,\tau_2,\theta)\fallingdotseq W(L^i)$$

であることが [GN] において示されています。この事実を頂点作用素代数で考えた場合、$\tau_1$, $\tau_2$ に対応する $V_{\sqrt{2}E_8}$ の二つのイジング元が生成する部分代数 $U$ 及びその $V_{\sqrt{2}E_8}$ における交換団 $M$ について、ある埋め込み

$$\varphi: M\otimes U\hookrightarrow V_\Lambda^+=(V^\natural)^{\langle\theta\rangle}$$

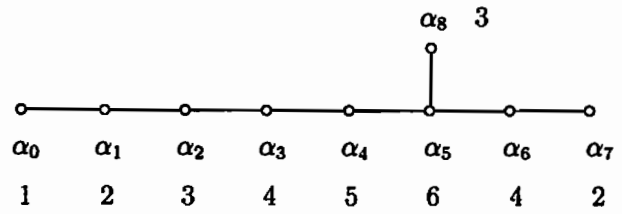
が存在することを意味していると思われます。何故ならば、$\tau_1,\tau_2$ の中心化群を考えることは $U$ の交換団部分代数を考えることに対応し、$\theta$ に関しても可換性を要求するということは $V^\natural$ の $\theta$ による軌道体において交換団を考えることに対応していると考えられるからです。ですので $M$ 及び $U$ の定める対称性を同時に考えて $V^\natural$ を調べることにより、$V^\natural$ の対称性としてのモンスターの理解がより深まるものと考えられます。この問題に動機付けられて、ワイル群の作用を受け持つ代数 $M$ に関して Lam-佐久間氏と共同研究を行いました。$M$ の構造・対称性に関する結果は最近公表した論文 [LSY] にまとめられております。

中心化群と交換団部分代数の関係について、関連する話題としてベビーモンスター頂点作用素 (超) 代数の話題 [Y] があります。$e\in V^\natural$ をイジング元、$\tau_e\in\mathbb{M}$ を対応する 2A-

元とします。このときベビーモンスター単純群 $\mathbb{B}$ は $\mathbb{B} = C_{\mathbb{M}}(\tau_e)/\langle\tau_e\rangle$ として表示することができます。$\tau_e$ はイジング元 $e$ から定まっていますから、$\tau_e$ の中心化群は $V^\natural$ の部分代数 $\mathrm{Vir}(e)$ の交換団部分代数に自然に作用しています。それゆえ、ある頂点作用素部分代数 $VB \subset V^\natural$ であって、$\mathrm{Vir}(e) \otimes VB \hookrightarrow V^\natural$ かつ $\mathrm{Aut}(VB) = \mathbb{B}$ となるものが存在することが予想できます。この問題はすでに [Y] において肯定的に解決されています。同様に、$C_{\mathbb{M}}(\tau_1, \tau_2, \theta)$ についても類似が成り立つことが期待しており、今後の研究課題として考えています。

最後に [GN] で考察されている群の類似の一覧を載せておきます (単純群の記法については [ATLAS] と同一のものを使用してます)。

$L^i = \bigoplus_{j \neq i} \mathbb{Z}\alpha_i,$




| $i$ | $L^i$ | $W(L^i)$ | $C_{\mathbb{M}}(\langle\tau_e, \tau_f, \theta\rangle)$ |
|---|---|---|---|
| 0 | $E_8$ | $2.O_8^+(2).2$ | $2^{2+8+16}.O_8^+(2)$ |
| 1 | $A_1 \oplus E_7$ | $2^2 \times S_6(2)$ | $2^{3+7+16}.S_6(2)$ |
| 2 | $A_2 \oplus E_6$ | $S_3 \times U_4(2).2$ | $(2^2 \times 2^{1+8}).(3 \times U_4(2)).2$ |
| 3 | $A_3 \oplus D_5$ | $2^6.(S_3 \times S_5)$ | $2^{1+14}.(3 \times 2.A_5).2$ |
| 4 | $A_4 \oplus A_4$ | $S_5 \times S_5$ | $2^{1+8}.(A_5 \times A_5).2$ |
| 5 | $A_5 \oplus A_2 \oplus A_1$ | $2 \times S_3 \times S_6$ | $2^2.U_6(2)$ 註 1 |
| 6 | $A_7 \oplus A_1$ | $2 \times S_8$ | $(2^{1+8} \times 2^6).S_6(2)$ 註 2 |
| 7 | $D_8$ | $2^7.S_8$ | $2^{2+14}.(2^4 \times 2^{1+6}).A_8$ |
| 8 | $A_8$ | $S_9$ | $2^{1+8}.A_9$ |

註 1: $U_6(2) > S_3 \times S_6$　　註 2: $S_6(2) > S_8$

# 参考文献


[ATLAS] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, 1985.

[C] J. H. Conway, A simple construction for the Fisher-Griess Monster group, *Invent. Math.* **79** (1985), 513–540.

[DLMN] C. Dong, H. Li, G. Mason and S. P. Norton, Associative subalgebras of Griess algebra and related topics, *Proc. of the Conference on the Monster and Lie algebra at the Ohio State University*, May 1996, ed. by J. Ferrar and K. Harada, Walter de Gruyter, Berlin-New York, 1998, pp. 27–42.

[DMZ] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, Proc. Symp. Pure. Math., American Math. Soc. **56** II (1994), 295–316.

[FLM] I.B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. **134**, Academic Press, New York, 1988.

[GN] G. Glauberman and S. P. Norton, On McKay's connection between the affine $E_8$ diagram and the Monster, *CRM Proceedings and Lecture Notes*, Vol. **30**, Amer. Math. Soc., Providence, RI, 2001, pp. 37–42.

[G] R. Griess, The Friendly Giant, *Invent. Math.* **69** (1982), 1–102.

[LSY] C.H. Lam, S. Sakuma and H. Yamauchi, Ising vectors and automorphism groups of commutant subalgebras related to root systems, preprint, `arXiv:math.QA/0507371`.

[LYY1] C.H. Lam, H. Yamada and H. Yamauchi, Vertex operator algebras, extended $E_8$ diagram, and McKay's observation on the Monster simple group, to appear in *Trans. Amer. Math. Soc.*

[LYY2] C.H. Lam, H.Yamada and H. Yamauchi, McKay's observation and vertex operator algebras generated by two conformal vectors of central charge 1/2, *Internat. Math. Res. Papers* **3** (2005), 117–181.

[Mc] J. McKay, Graphs, singularities, and finite groups, *Proc. Symp. Pure Math.*, Vol. **37**, Amer. Math. Soc., Providence, RI, 1980, pp. 183–186.

[M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* **179** (1996), 523–548.

[M2] M. Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, *Ann. Math.* **159** (2004), 535–596.

[T] J. Tits, On R. Griess' "Friendly giant", *Invent. Math.* **78** (1984), 491–499.

[Y] H. Yamauchi, 2A-orbifold construction and the baby-monster vertex operator superalgebra, *J. Algebra* **284** (2005), 645–668.

# 頂点作用素代数とジョルダン代数

芦原　崇裕

筑波大学大学院　数理物質科学研究科

## 1　序文

### 1.1　はじめに

今回、$\mathbb{C}$ 上の $d$ 次対称行列全体 ($d \in \mathbb{N}$) のなすジョルダン代数 $J_d$ をグライス代数として持ち、central charge(c.c.) が任意の複素数となる頂点作用素代数 (VOA) の構成を説明します。一般に VOA $V = \oplus_{n=0}^{\infty} V_n$ が

$$V_0 = \mathbb{C}1,\ V_1 = 0$$

を満たす時、$V_2$ は 1 積で可換代数 (一般には結合律は成り立たない) となり、これをグライス代数と言います。このグライス代数にどの様な代数が現れるのかと言う事は非常に興味深い事であります。これまで、任意の可換結合代数と $\mathbb{C}$ 上の単純ジョルダン代数がグライス代数となる VOA の存在がいずれも C.H.Lam によって示されており、その中でも単純ジョルダン代数に関しては c.c. は自然数となっています。VOA の研究において c.c. が有理数や半整数の時に、しばしばおもしろい対象が現れる事があります。この VOA をより興味深い対象にする為に c.c. が任意の複素数となように拡張しました。尚、今回の結果は筑波大学の宮本雅彦先生との共同研究の結果です。ここでジョルダン代数の説明を簡単にします。

**Definition 1.1.1** $\mathbb{C}$ 上のベクトル空間 $V$ が以下の条件を満たす時、$V$ をジョルダン代数と言う。

$$vu = uv$$
$$(v^2u)z = v^2(uz) \quad u, v, z \in V.$$

□

簡単な例として、任意の結合代数 $A$ に対して

$$a * b := ab + ba$$

とおけば $A$ は積 $*$ でジョルダン代数となります。$J_d$ に関しても通常の行列の積を用いて上記と同様の定義でジョルダン代数となります。

## 2 C.H.Lam の結果

まず、C.H.Lam によって構成されたグライス代数が $J_d$ となる VOA の構成を紹介します。今回は $J_d$ についての結果ですがその他の単純な $\mathbb{C}$ 上のジョルダン代数についての c.c. が自然数となる VOA の構成については [Lam] を参照して下さい。

### 2.1 フリーボゾン型 VOA

$K$ を非退化な対称形式 $<,>$ をもつ $\mathbb{C}$ 上の $d$ 次元ベクトル空間とします。$K$ を可換なリー代数とみなしてそのアフィンリー代数を

$$\hat{K} := K \otimes_{\mathbb{C}} \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}l$$

とおき、$\hat{K}$ のリー積を $a \otimes t^m := a(m), b \otimes t^n := b(n)$ $(a, b \in K,\ m, n \in \mathbb{Z})$ として、

$$[a(m), b(n)] := [a, b](m+n) + m < a.b > l$$
$$[a(m), l\,] := 0$$

と定義すれば、$\hat{K}$ はリー代数となります。次に、

$$\hat{K}^+ := K \otimes t\mathbb{C}[t],\ \hat{K}^0 := K \oplus \mathbb{C}l,\ \hat{K}^- := K \otimes t^{-1}\mathbb{C}[t^{-1}]$$

とおけば、$\hat{K}$ は

$$\hat{K} = \hat{K}^+ \oplus \hat{K}^0 \oplus \hat{K}^-$$

と分解できますので、その普遍包絡環は

$$U(\hat{K}) = U(\hat{K}^+) \otimes U(\hat{K}^0) \otimes U(\hat{K}^-)$$

と書けます。そして、$\mathbb{C}1$ に $K$ と $\hat{K}^+$ は自明に作用させ、$l$ を 1 倍で作用させれば $\mathbb{C}1$ は 1 次元 $\hat{K}^+ \oplus \hat{K}^0$-加群とみなす事ができ、これを用いて加群

$$M := \hat{K} \otimes_{U(\hat{K}^+) \otimes U(\hat{K}^0)} \mathbb{C}1$$

を構成します。$M$ に VOA の構造を入れるのですが、その前に次数を定義します。$K$ の $<,>$ に関する正規直交基底を $\{u^i\}_{1 \le i \le d}$ とすれば、$M$ の基底は

$$\{u^{i_1}(m_1) \cdots u^{i_k}(m_k)1 \mid 1 \le i_1, \ldots, i_k \le d,\ m_1, \ldots, m_k \lneq 0,\ k \in \mathbb{N}\}$$

となります。これを用いて次数を

$$\deg\, u^{i_1}(m_1) \cdots u^{i_k}(m_k)1 := -m_1 - m_2 - \cdots - m_k$$
$$\deg 1 := 0$$

と定義し、次数 $n$ の空間を $M_n$ と書きます。そして、頂点作用素を正規積を用いて帰納的に
($a(z) := \sum_{m\in\mathbb{Z}} a(m)z^{-m-1}$, $a \in K$ とする。)

$$Y(1,z); = 1_M$$
$$Y(a(-1)1,z) := a(z)$$
$$Y(a(n)v,z) := Res_w\{(z-w)^n a(w)Y(v,z) - (-w+z)^n Y(v,z)a(w)\}$$

と定義すれば、$M$ に VOA の構造が入り、ヴィラソロ元は

$$\omega := \frac{1}{2}\sum_{1\le i\le d} u^i(-1)u^i(-1)1$$

となり、c.c. が $d$ となる事が知られています。この VOA をフリーボソン型 VOA と言います。

## 2.2 オービフォルド

ここで、$M$ のある自己同型の固定点全体のなす $M$ の VOA としての部分代数のグライス代数が $J_d$ となる事を簡単に説明します。

まず、$K$ から $K$ への写像 $\tau$ を次の様に定義します。

$$\tau(a) := -a \quad \text{for } a \in K.$$

$\tau$ は $<,>$ を保存するリー代数としての自己準同型となり、よく知られている様に $\tau$ は $M$ の VOA としての自己同型写像に拡張できます。すると、

$$\tau(u^{i_1}(m_1)\cdots u^{i_k}(m_k)1) = (-1)^k u^{i_1}(m_1)\cdots u^{i_k}(m_k)1$$

となるので、$\tau$ の固定点全体のなす $M$ の VOA としての部分代数を $M^\tau := \bigoplus_{n\ge 0} M_n^\tau$ とおけば、

$$M_0^\tau = \mathbb{C}1,\ M_1^\tau = \{0\},\ M_2^\tau = \bigoplus_{1\le i\le j\le d} \mathbb{C}u^i(-1)u^j(-1)1$$

となる事が容易に分かり、$M_2^\tau$ の 1 積を計算すると、

$$\begin{aligned} u^i(-1)u^j(-1)1 \times_1 u^s(-1)u^t(-1)1 = {} & \delta_{i,s}u^j(-1)u^t(-1)1 + \delta_{i,t}u^j(-1)u^s(-1)1 \\ & + \delta_{j,s}u^i(-1)u^t(-1)1 + \delta_{j,t}u^i(-1)u^s(-1)1 \end{aligned}$$

となる事が計算により分かります。$E^{ij}$ を $(i,j),(j,i)$ 成分が 1 の行列とすれば $\{E^{ij}\}_{1\le i\le j\le d}$ は $J_d$ の基底となります。計算により

$$E^{ij} * E^{st} = \delta_{i,s}E^{jt} + \delta_{i,t}E^{js} + \delta_{j,s}E^{it} + \delta_{j,t}E^{is}$$

となるので、$u^i(-1)u^j(-1)1$ と $E^{ij}$ を対応させれば $J_d$ と $(M_2^\tau,\ \times_1)$ は代数として同型となる事が分かります。

# 3 主結果

この章で今回得られた VOA の構成について説明します。この構成法には前章までの方法を参考にしており、得られた関係式等は直接計算による所が殆どですのでその部分は割愛させて頂きます。

## 3.1 あるリー代数とその加群

記号は 2.1 で使ったものをそのまま使用します。まず、$\hat{K}$ の center $l$ は後々に加群に 1 倍で作用させたので、出発点としては

$$H := U(\hat{K})/(l-1)$$

を考えます。

$$\{u^i(m)u^j(n) \mid 1 \leq i \leq j \leq d,\ m,n \in \mathbb{Z}\} \cup \{u^i(m)u^i(n) \mid 1 \leq i \leq d,\ m \leq n\}$$

を基底とする部分空間を $L'$ とおけば、

$$L := L' \oplus \mathbb{C}$$

は $L$ は $H$ のリー代数としての部分代数となる事が計算により分かります。$c \in \mathbb{C}$ に対して $L$ に新しい積を定義します。まず、$a, b \in L$ に対して

$$[a,b] := [a,b]' + [a,b]'' \in L' \oplus \mathbb{C}$$

と分解します。

$$[a,b]_c := [a,b]' + c[a,b]'' \in L' \oplus \mathbb{C}$$

と定義すれば、次が得られます。

**Lemma 3.1.1** $L_c := (L,\ [,]_c)$ はリー代数となる。

□

$L_c$ と $L$ はベクトル空間としては、同じものですがリー代数としては別物なので、区別するという意味をこめて、あえてですが、$L_c$ の基底の表記を次の様にします。

$$:u^i(m)u^j(n):_c .$$

そして、$L_c$ の部分空間を

$$L_c^+ := \mathrm{Span}\{:u^i(m)u^j(n):_c \mid m \geq 0 \text{ or } n \geq 0\} \oplus \mathbb{C}$$
$$L_c^- := \mathrm{Span}\{:u^i(m)u^j(n):_c \mid m \leq 0\ , n \leq 0\}$$

とおけば、$L_c = L_c^+ \oplus L_c^-$ となりそれぞれが $L_c$ の部分代数となります。よって、

$$U(L_c) = U(L_c^+) \otimes U(L_c^-)$$

となるので、前章と同様に一次元 $U(L_c^+)$-加群 $\mathbb{C}1$ を $\mathbb{C}$ は定数倍で作用しその他は自明に作用するとして定義すれば、加群

$$M_c = U(L_c) \otimes_{U(L_c^+)} \mathbb{C}1$$

が構成でき、次数も同様に

$$\deg\ : u^i(m)u^j(n) :_c := -m - n$$
$$\deg\ 1 := 0$$

で定義します。すると $M_c = \bigoplus_{n=0}^{\infty} (M_c)_n$ について次が成り立つ事が容易に分かります。

**Lemma 3.1.2**

$$(M_c)_0 = \mathbb{C}1,\ (M_c)_1 = \{0\},\ (M_c)_2 = \bigoplus_{1 \le i \le j \le d} \mathbb{C} : u^i(-1)u^j(-1) :_c$$

が成立。

□

## 3.2 頂点作用素

この章で前章で定義した加群上に頂点作用素を構成します。VOA の構成は Local system の理論を用いるのですが、その説明は割愛させて頂きます。[Li] を参照してください。

$M_c$ への作用素を次の様に定義します。

$$L_c^{ii}(n) := \frac{1}{2} \sum_{n-h \le h} : u^i(n-h)u^i(n) :_c + \frac{1}{2} \sum_{h \le n-h} : u^i(h)u^i(n-h) :_c$$
$$L_c^{ij}(n) := \frac{1}{2} \sum_{h \in \mathbb{Z}} : u^i(n-h)u^i(n) :_c \quad \text{if } i \le j$$

この作用素は $L_c$ の元の無限和になっていますが、$M_c$ に作用させれば $M_c$ の元の有限和となっている事が計算によってわかりますので、この作用素は $\mathrm{End}M_c$ の元としては well-defined となります。この作用素同士の交換関係式を計算して次を得ました。

**Proposition 3.2.1**

$$[L_c^{ii}(m), L_c^{ii}(n)] = (m-n)L_c^{ii}(m+n) + \delta_{m+n,0}\frac{m^3-m}{12}c \tag{1}$$

$$[L_c^{ij}(m), L_c^{st}(n)] = 0 \text{ if } \{i,j\} \cap \{s,t\} = \emptyset \tag{2}$$

$$[L_c^{ii}(m), L_c^{ij}(n)] = [L_c^{ii}(-1), L_c^{ij}(n+m+1)] + (m+1)L_c^{ij}(n+m) \tag{3}$$

$$[L_c^{ij}(m), L_c^{ij}(n)] = \frac{m-n}{4}(L_c^{ii}(n+m) + L_c^{jj}(n+m)) + \delta_{n+m,0}\frac{m^3-m}{24}c \tag{4}$$

$$[L_c^{ij}(m), L_c^{jk}(n)] = \frac{1}{4}\sum_{i\in\mathbb{Z}} i : v^i(m-i)v^k(n+i) :_c \text{ for } i \neq j \neq k \neq i \tag{5}$$

$$[\sum_{i=1}^{d} L_c^{ii}(-1), L_c^{st}(m)] = (-1-m)L_c^{st}(-1+m). \tag{6}$$

が成立。

□

これらの交換関係式から量子作用素 $\omega_c^{ij}(x) := \sum_{n\in\mathbb{Z}} L^{ij}(n)x^{-n-2}$ は次の locality を満たします。

**Proposition 3.2.2** 量子作用素 $\omega_c^{ij}(x)$, $\omega_c^{st}(x)$ に対して、

$$(x-z)^4[\omega_c^{ij}(x),\ \omega_c^{st}(z)] = 0$$

が成立。

□

Proposition3.2.2 から local system の理論が適用できます。よって、

$$S := \{\omega_c^{ij}(x) \mid 1 \leq i \leq j \leq d\}$$

とおけば、$S$ で生成される頂点代数 $< S >$ が構成できます。(vacuum vector は $M_c$ から $M_c$ への identity map $1_{M_c}$ です。) さらに、

$$\omega_c(x) := \sum_{m\in\mathbb{Z}} L_c(m)x^{-m-2} := \sum_{i=1}^{d} \omega_c^{ii}(x)$$

は Proposition3.2.1 の (1),(6) からヴィラソロ元であるための条件である微分の式とヴィラソロ関係式を満たします。あとは、$< S >$ の次数を線形変換

$$[L_c(0),\ \cdot\ ] - x\frac{d}{dx}\cdot$$

の固有値で定義すれば

$$[L_c(0), L_c^{ij}(x)] - x\frac{d}{dx}L_c^{ij}(x) = 2L_c^{ij}(x)$$

を満たすので $\omega_c(x)$ が c.c. が $dc$ となるヴィラソロ元となり、$< S >$ は $\mathbb{Z}$ で次数付けされることが分かりました。しかし、この段階では各斉次空間が有限次元であるかどうかは分かりません。現段階では $< S >$ をしかるべきイデアルで割って構成する方法を用います。今回はその方法を簡単に紹介してこの報告を終えます。

$< S >$ から $M_c$ への写像 $f$ を次の様に定義します。

$$f(a(x)) := a_{-1}1 \quad \text{for } a(x) \in < S >$$

$L_c(-1)1 = 0$ であることから $f$ は $< S >$-module としての準同型写像となります ([Li] 参照)。よって、$\ker f$ は $< S >$ のイデアルとなり、$< S > / \ker f$ に頂点作用素代数の構造が入ります。そして次の主結果を得ました。

**Theorem 3.2.3** $< S > / \ker f$ は c.c. が $dc$ である頂点作用素代数となり、次を満たす。

$$(< S > / \ker f)_n = \{0\} \quad \text{for all } n \in \mathbb{Z}_{\leq 0},$$
$$(< S > / \ker f)_0 = \mathbb{C}1_{M_c} + \ker f,$$
$$(< S > / \ker f)_1 = \{0\},$$
$$((< S > / \ker f)_2, \times_1) \cong J_d.$$

□

## 参考文献


[B] R. E. Borcherds, Vetex algebras, Kac-Moody algebras, and the monster, Proc. Nalt. Acad. Sci. USA, 83,(1986), 3068-3071.

[FLM] I. Frenkel, J. Lepowsky and A. Meurman, "Vertex operator algebras and the Monster", Pure and Applied Mathematics, 134. Academic Press, (1988).

[FZ] I. Frenkel and Y. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras. Duke Math. J. 66 (1992), no. 1, 123-168.

[Lam] C.H.Lam, On VOA associated with special Jordan algebras. Comm. Algebra 27 (1999), no. 4, 1665-1681.

[Li] H. S. Li, Local systems of vertex operators, vertex superalgebras and modules. J. Pure Appl. Algebra 109 (1996), no. 2, 143-195.

# 偶数位数の群の位数に関して

原田耕一郎（オハイオ州立大学），宮本雅彦（筑波大学）

## 1 序文

単純群の発見の過程で，発見者の栄誉を勝ち得る為に重要なことは，位数を決定することであった．$G$ を偶数位数の群，$t$ を位数 2 の元 (involution) とし，$t$ の共役類を $C_1 = \{t^g = g^{-1}tg \mid g \in G\}$ で表す．もし，$G$ が involution $u$ の別の共役類を持っている場合，有名なトンプソンの位数公式によって，$G$ の位数 $|G|$ が $|C_G(t)|$, $|C_G(u)|$ から分かる．例えば，involutions の共役類が 2 つ $C_1$ と $C_2$ しかない場合には，

$$|G| < |C_G(t)||C_1 \cap C_G(u)||C_2 \cap C_G(u)| + |C_G(u)||C_1 \cap C_G(t)||C_2 \cap C_G(t)|$$

となる。この定理の証明を少し説明しよう．重要なことは involution $t$, $s$ の積 $ts$ は $t$, $s$ の共役作用によって逆元に移るということで，

$$t(ts)t^{-1} = st = (ts)^{-1}$$

である．特に，$ts$ の位数が奇数 $m$ の場合 $< t >, < s >$ は位数 $2m$ の 2 面体群 $< t, s >$ のシロー 2 群となるから，$t$, $s$ は同じ共役類に入る．逆に，$t$, $s$ が共役でなければ，$ts$ が偶数位数 $2m$ となり，$(ts)^m$ は $< t, s >$ の中心に入る involution である．それゆえ，$C_G(ts) \subseteq C_G((ts)^m)$ となり，$ts$ 達の中心化群はある involution の中心加群に含まれてしまう。証明にはこれを利用している．

それゆえ，involutions の共役類が一つしかない場合にはこの方法は使えないし、その場合の $|G|$ に対する一般的な不等式も知られていなかった．(Michler の本の 4 章を参照)．マシュー群，ヤンコ群，リオン群，トンプソン群などの単純群の計算の実際の場合には，個々に例外指標などの群論的手法を駆使して，$C_G(t)$ の構造から $G$ の位数を計算することに成功していたのである．

この講演では，一意的な involution の共役類を持つ偶数位数の群に対して，その位数 $|G|$ の上限を与える式を提示するのが目的である．

残念ながら，位数 2 の元の共役類が一つの場合には，$|C_G(t)|$ だけでは $|G|$ の上限を決定できない．例えば，2 面体群 $D_{2p}$ を考えた場合，$|C_G(t)| = 2$ であるが，群の位数はいくらでも大きくなりうる．トンプソンの定理と同じく他の元を必要なのである．

群 $G$ の素数グラフ $\Gamma(G)$ の定義はよく知られていると思うが，一応説明しておこう．

頂点集合を $G$ の位数 $|G|$ を割る素数全体の集合 $\pi(G)$ とし，2 頂点（2 つの素数）$p, q$ が連結であるとは，$G$ が位数 $pq$ の元を含むこととして定義する．すなわち，位数 $p$ の元と位数 $q$ の元で可換なものがあることを意味する．

2 と連結な素数全体を $\pi$ と書くことにする．これが重要な働きをする．

単純群分類の Lyons や Parrott の仕事でも分かるように，位数 2 の元から始めて，それらと可換な元の情報を捉えるという仕事は成功することが多い．簡単に言えば，2 と連結な $\pi_1$-元の情報はかなり正確に求まると言っているのである．

結果を述べる．

**定理 1.1** $G$ を一意的な位数 2 の元の共役類を持つ群とし，位数 2 の元 $t$ を固定し，中心化群を $H = C_G(t)$ と置く．しかも，$G$ のシロー 2 群は巡回群でも一般四元数群でもないとする．このとき，

$$|G| < |H|^3 + m_\pi |H|^2,$$

が成り立つ．ここで，$m_\pi$ は $\max\{|H|, |C_1 \cap C_G^-(g)| \mid 1 \neq g \text{ は } \pi\text{-元}\}$ であり，$\pi$ は 2 を含む $G$ の素数グラフの連結成分を表し，$C_1 = \{t^g = g^{-1}tg \mid g \in G\}$ は $t$ を含む共役類，$C_G^-(g) = \{h \in G \mid h^{-1}gh = g^{-1}\}$ は共役作用で $g$ を逆元 $g^{-1}$ に移す元全体の集合である．

## 2 応用

主定理の証明の前に応用を紹介しておこう．素数の集合 $\pi \subseteq \pi(G)$ に対して，$g_\pi$ で $|G|$ の $\pi$-部分を表すことにする．また，$\pi'$ で $\pi$ の補集合を表すことにする．

**定理 2.1** 上の定理の仮定のもとで，もし

$$|H|^3 + m_\pi |H|^2 \leq g_\pi^2$$

なら，$G$ の位数は $\pi$-元の中心化群の位数と $\pi$-元の共役類の個数によって一意的に定まる．

**証明** $|G| = g_\pi g_{\pi'}$ であることに注意．$\Omega_\pi$ で $G$ の $\pi$-元全体の集合，$\{C_0 = 1, C_1, \ldots, C_r\}$ で $\pi$-元の共役類を表す．$t_i$ を $C_i$ の代表元とする．このとき，フロベニウスの定理から，

$$|\Omega_\pi| = \sum_{i=0}^{r} |C_i| \equiv 0 \pmod{g_\pi}$$

であり、一方，$|C_G(t_i)|$ は $g_\pi$ を割るので，

$$|\Omega_\pi| = \sum_{i=0}^{r} |G|/|C_G(t_i)| = 1 + g_{\pi'} \left( \sum_{i=1}^{r} g_\pi/|C_G(t_i)| \right)$$

となる．それゆえ，$g_{\pi'}$ は法 $g_\pi$ で $\sum_{i=1}^{r} g_\pi/|C_G(t_i)|$ の逆元として決まる．ここで，仮定 $|H|^3 + m_\pi |H|^2 \leq g_\pi^2$ を加えると，主定理より，$|G| < g_\pi^2$ である．$|G|/g_\pi$ が法 $g_\pi$ に関して一意に定まるので，$|G|$ が一意的に決まることが分かる． ∎

例 1. $G = Ly$ (Lyons' 単純群).
$|G| = 2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67 \doteqdot 5.2 \times 10^{16}$ ということを示そう．

次の事が分かっているとする．
$|H| = |2A_{11}| = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \doteqdot 4.0 \times 10^7$.

$\pi = \{2,3,5,7,11\}$ かつ $g_\pi = 2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \fallingdotseq 6.7 \times 10^{11}$ (Lyons による).
これらから，$m_\pi = |H|$ が分かる．もし $\pi$-元 $g \neq 1$ に対して，$|C_G(g)| > |H|$ なら，$g$ は位数 3 の元で，$C_G(g)$ は McLaughlin's 単純群 $McL$ の $\mathbb{Z}/3\mathbb{Z}$ 上の拡大となっているが、この $g$ に対しては，$|C_1 \cap C_G^-(g)| = (3 \cdot 2|McL|)/(2|M_{11}|) = 340,200 < |H|$ である．
また，Lyon の結果から，$|G|/g_\pi \equiv 31 \cdot 37 \cdot 67 \pmod{g_\pi}$ となる．計算より，$|H|^3 + m_\pi |H|^2 = 2|H|^3 \fallingdotseq 1.3 \times 10^{23}$ で，$g_\pi^2 \fallingdotseq 4.5 \times 10^{23}$ である．それゆえ，定理より，$|H|^3 + m_\pi |H|^2 \leq g_\pi^2$ を得て，$|G|$ が一意的に決まるので、$|G| = 2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$ を得る．

例 2. $G = Th$ (Thompson's 単純群).
$|G| = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31 \fallingdotseq 9.1 \times 10^{16}$ を示そう．

$|H| = |2^{1+8}A_9| = 2^{15} \cdot 3^4 \cdot 5 \cdot 7 \fallingdotseq 9.3 \times 10^7$.
$\pi = \{2,3,5,7,13\}$ で，$g_\pi = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \fallingdotseq 1.5 \times 10^{14}$ または $2^{15} \cdot 3^{10} \cdot 5 \cdot 7^2 \cdot 13 \fallingdotseq 6.2 \times 10^{12}$ ([P] 参照) が与えられている．
すべての $\pi$-元 $g \neq 1$ に対して，$|C_G(g)| \leq |H|$ なので，$m_\pi = |H|$ である．$|G|/g_\pi \equiv 19 \cdot 31 \pmod{g_\pi}$ (この場合 $g_\pi = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13$) または，$|G|/g_\pi \geq 1.2 \times 10^{12}$ ([P] 参照) である．定理より，$|G| < |H|^3 + m_\pi |H|^2 = 2|H|^3 \fallingdotseq 1.6 \times 10^{24}$ である．もし，$|G|/g_\pi \geq 1.2 \times 10^{12}$ なら，$|G| \geq 6.2 \times 10^{12} \times 1.2 \times 10^{12} \fallingdotseq 7.44 \times 10^{24}$ となり，これは上の結果に矛盾する．故に，$|G|/g_\pi \equiv 19 \cdot 31 \pmod{g_\pi}$ で，$g_\pi = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13$ となる．それゆえ，$g_\pi^2 \geq 2.3 \times 10^{28}$ であり $|H|^3 + m_\pi |H|^2 \leq g_\pi^2$ を得る．定理 2.1 より，$|G|$ は一意的に決まるので，[P] で示されているように，$|G| = 2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$ となる．

## 3 定理 1.1 の証明

$$G = C_0 \cup C_1 \cup C_2 \cup \ldots \cup C_q$$

を共役類の分解とする．$C_0 = \{1\}$, $t \in C_1$ としてよい．$t_i \in C_i$ で代表元を表す．まず，$\{C_0, C_1, \ldots, C_r\}$ を involution で逆元に送られる $\pi$-元の共役類，$C_{r+1}, \ldots, C_s$ を $\pi'$-元の共役類とする．

$\pi_1$ で $C_{r+1} \cup \ldots \cup C_s$ の中に入っている元を割る素数の集合とする．

[BF] の論法を説明しよう．群環で考えた方が便利なので，$\overline{C_i} = \sum_{g \in C_i} g \in \mathbb{C}G$ とおく．すると，

$$\overline{C_1} \cdot \overline{C_1} = \sum_{i=0}^{s} a_i \overline{C_i}$$

である．もし $i \neq 1$ なら，明らかに

$$a_i = |\{(h,k) \in (C_1, C_1) \mid hk = t_i\}| = |C_1 \cap C_G^-(t_i)|$$

である．$a_0 = |C_1|$ で，$a_1 = |C_1 \cap H - \{t\}|$ なので，$a_0|C_0| + a_1|C_1| = |C_1| + |C_1 \cap H - \{t\}||C_1| = |C_1 \cap H||G/H|$ となるので，

$$\left(\frac{|G|}{|H|}\right)^2 = |C_1 \cap H|\frac{|G|}{|H|} + \sum_{i=2}^{s} |C_1 \cap C_G^-(t_i)|\frac{|G|}{|C_G(t_i)|}$$

を得る．

$t_\alpha$ を $|C_1 \cap C_G^-(t_\alpha)| = \max\{|C_1 \cap C_G^-(t_i)|, i = 1, 2, \ldots, s\}$ となる元とする．この時，

$$\left(\frac{|G|}{|H|}\right)^2 \leq |C_1 \cap C_G^-(t_\alpha)| \sum_{i=1}^{s} \frac{|G|}{|C_G(t_i)|} < |C_1 \cap C_G^-(t_\alpha)||G|$$

なので，

$$|G| < |C_1 \cap C_G^-(t_\alpha)||H|^2$$

となる．それゆえ，もし $t_\alpha$ が $\pi$-元となるか，$|C_1 \cap C_G^-(t_\alpha)| \leq |H|$ となるなら，希望の結果(実際にはより強い結果) $|G| < m_\pi |H|^2$ を得る．

それゆえ，以下では次のことを仮定する．

仮定　　$t_\alpha$ は $\pi_1$-元で，$|C_1 \cap C_G^-(t_\alpha)| > |H|$ が成り立つ．

この時，あきらかに $|C_G(t_\alpha)| > |H|$ であり，
$|C_G(t_\alpha)|$ と $|H|$ は互いに素なので，$|C_G(t_\alpha)||H|$ は $|G|$ の約数となる．故に，$|G| = a|C_G(t_\alpha)||H|$ となる整数 $a$ があるが，上の結果から $a < |H|$ である．特に，$G$ のある元 $g$ に対して，$(|C_G(g)|, |C_G(t_\alpha)||H|) = 1$ となるなら，$|C_G(g)| < |H|$ を満たす．

$j = r+1, \ldots, s$ に対して，$B_j = C_G(t_j)$ とおく．

**補題 3.1** $j = r+1, \ldots, s$ に対して次が成り立つ．
*(a).* $g \in G$ に対して，$B_j \cap B_j^g = 1$ か $B_j \neq B_j^g$ のどちらかが成り立つ．*(i.e.* $B_j$ はいわゆる *TI (trivial intersection)*-部分群である*.)*
*(b).* $B_j$ は $G$ の可換 *Hall* 部分群である．
*(c).* $\pi(B_j)$ は素数グラフ $\Gamma(G)$ の一つの連結成分となる．
*(d).* もし $|B_j| \geq |H|$ なら，$B_j = B_\alpha = C_G(t_\alpha)$ である．
*(e).* もし $g \in G$ が $\pi$-元でなく，$B_\alpha - \{1\}$ のどの元とも $G$-共役でなければ，$|C_G(g)| < |H|$ である．

証明　主張 (a), (b), (c) は良く知られた結果で，たぶん最初，ブラワー，鈴木，その他の人の結果として 1950 年代に出てきている．共役をとって，$t$ が $t_j$ と仮定してよい．$t$ は $B_j$ に固定点無しとして作用するるので，$t$ は $B_j$ のすべての元を逆元に移すことになるが，それが自己同型なので，$B_j$ が可換群であることが分かる．もし $1 \neq h \in B_j$ なら，同じ性質が $C_G(h)$ に対しても成り立ち，$C_G(h)$ も可換である．特に，すべての $1 \neq h \in B_j$ に対して $C_G(h) = B_j$ であり．それゆえ，$B_j$ は $G$ の Hall 部分群で，かつ TI 部分群であることがわかる．(c) はこれらの結果から自動的に出てくる．(d) に対しては，仮定から $t_\alpha$ が $\pi_1$-元で，$C_G(t_\alpha)| > |H|$ が成り立っている．それゆえ，$|B_\alpha| > |H|$ となる．ここで，$B_{j'} \neq B_\alpha$ を選ぶと，$|B_{j'}|$ と $|B_\alpha||H|$ は互いに素であり，それゆえ，この補題の前に述べたコメントから，$|B_{j'}| < |H|$ なので，(d) が出てくる．(e) も同じように出てくる．　∎

$\pi_1 = \pi_{1,1} \cup \cdots \cup \pi_{1,k}$ を素数の集合 $\pi_1 \subset \pi(G)$ の素数グラフ $\Gamma(G)$ の連結成分への分割とする．必要なら $j = r+1, \ldots, s$ の順番を変えて，$t_{r+i}$ $(i = 1, \ldots, k)$ は $\pi_{1,i}$-元としてよい．もし $g$ が $\pi_{1,i}$-元なら，$C_G(g)$ は $G$ において，$C_G(t_{r+i})$. に共役である．

$(|N_G(B_j)/B_j|, |B_j|) = 1$ なので，部分群 $W_j$ で $N_G(B_j)$ が $B_j$ の $W_j$ による半直積となるものがある．

**補題 3.2** 次が成り立つ。

$$\left(\frac{|G|}{|H|}\right)^2 = \frac{|C_1 \cap H||G|}{|H|} + \sum_{i=2}^{r} \frac{|C_1 \cap C_G^-(t_i)||G|}{|C_G(t_i)|} + \sum_{j=r+1}^{r+k} \frac{(|B_j|-1)|G|}{|W_j|}$$

**証明** $j \in \{r+1, r+2, \ldots, s\}$ に対して，$B_j$ は $G$ の TI 部分群なので，$b$ とその共役 $g^{-1}bg$ の両方が $B_j$ に含まれていることと，$g \in N_G(B_j)$ であることは同値である．また，$B_j$ は可換群なので，$N_G(B_j)$ における $B_j$ の元同士の共役関係は $W_j$ の元の作用によって決まる．それゆえ，$B_j - \{1\}$ の共通点を持つ $G$ の共役類の個数は $(|B_j|-1)/|W_j|$ となる．しかも $t$ は $B_j = C_G(t_j)$ の元を逆元に移し，$C_1 \cap C_G^-(t_j) = tC_G(t_j)$ なので，

$$a_j|C_j| = |C_1 \cap C_G^-(t_j)||C_j| = |C_G(t_j)|\frac{|G|}{|C_G(t_j)|} = |G|$$

となることが分かる．$G$ のすべての $\pi_1$-元は $B_j, j \in \{r+1, \ldots, r+k\}$ のどれか（丁度）1 つの中の元と共役になるので，希望の結果が出て来る． ∎

$m_j = |B_j|$, $w_j = |W_j|$, $n_j = (|B_j|-1)/|W_j|$ と置く．次の命題が鍵となる．

**命題 3.3** すべての $j = r+1, \ldots, s$ に対して，$n_j \leq |H|$ が成り立つ．

定理 1.1 はこの命題の簡単な帰結となるので，先に命題 3.3 が正しいとして定理 1.1 の証明を紹介する．

**定理 1.1 の証明** $G$ の $\pi$-元の個数は $|G| - \sum_{j=r+1}^{r+k}(|B_j|-1)\frac{|G|}{|B_j||W_j|}$ を越えないので，

$$\left(\frac{|G|}{|H|}\right)^2 < m_\pi \left(|G| - \sum_{j=r+1}^{r+k}(|B_j|-1)\frac{|G|}{|B_j||W_j|}\right) + \sum_{j=r+1}^{r+k}\frac{|B_j|-1}{|W_j|}|G|$$

である．それゆえ，

$$\begin{aligned}
\frac{|G|}{|H|^2} &< m_\pi - m_\pi \sum_{j=r+1}^{r+k}\frac{|B_j|-1}{|B_j||W_j|} + \sum_{j=r+1}^{r+k}\frac{|B_j|-1}{|W_j|} \\
&= m_\pi + \sum_{j=r+1}^{r+k}\frac{|B_j|-1}{|W_j|}\left(1 - \frac{m_\pi}{|B_j|}\right) \\
&\leq m_\pi + \frac{|B_\alpha|-1}{|W_\alpha|}\left(1 - \frac{m_\pi}{|B_\alpha|}\right) \\
&\quad (\text{なぜなら } r+1 \leq j \neq \alpha \leq r+k \text{ に対して } 1 - \frac{m_\pi}{|B_j|} \leq 0 \\
&\leq m_\pi + \frac{|B_\alpha|-1}{|W_\alpha|} \leq m_\pi + |H| \quad (\text{命題 3.3 より}).
\end{aligned}$$

となり，定理 1.1 が出て来る．

それでは，命題 3.3 の証明を始める．

命題 3.3 の証明　命題 3.3 がある $j$ に対して正しくないと仮定する．すなわち，$|B_j| = n_j|W_j| + 1 > |H|$ とする．そのような $B_j$ は補題 3.1 より一意的に定まり，$B_j = B_\alpha$ である．$B_\alpha = C_G(t_\alpha)$ となる一意的な $j = \alpha \in \{r+1, \dots, r+k\}$ がある．記号を簡単にするために，$B = B_\alpha$, $W = W_\alpha$, $n = (|B_\alpha| - 1)/|W_\alpha|$ と書くことにする．$n > |H|$ と仮定して矛盾を導びこう．手法はフロベニウス群 $N = N_G(B) = BW$ から定義される例外指標の理論である．

$\mathrm{Irr}(B) = \{1_B = \theta_0, \theta_i^j \mid i = 1, \dots, n, j = 1, \dots, w\}$ で $B$ の既約指標全体を表すことにする．$B$ は可換群なので，既約指標はすべて次数 1 であり，$|\mathrm{Irr}(B)| = |B|$ である．また，$W$ は $B$ に固定点無しで作用しているので，自明でない既約指標全体 $\mathrm{Irr}(B) - 1_B$ は長さ $w = |W|$ の軌道に分解する．この事実から，$N = BW$ のすべての既約表現をすべて決定できる．実際，$\mathrm{Irr}(N) = \mathrm{Irr}(N/B) \cup \{(\theta_i^j)^N \mid i = 1, 2, \dots, n\}$ である．ここで $j$ は $\{1, 2, \dots, w\}$ の中の一つで，$(\theta_i^j)^N$ は誘導指標を表す．$(\theta_i^j)^N$ は $j$ に依存していない．$\theta_i = \theta_i^1$ とおく．このとき，$\sum_{j=1}^{w} \theta_i^j = \theta_i^N{}_{|B}$ であり，$\mathrm{Irr}(N) = \mathrm{Irr}(N/B) \cup \{\theta_i^N \mid i = 1, 2, \dots, n\}$ である．

鈴木先生の結果 [S] より，フロベニウス部分群 $N = BW$ に対応する $G$ の例外指標 $\chi_1, \dots, \chi_n$ があり，次の条件を満たす．

(a) $\{\chi_1, \dots, \chi_n\} \subset \mathrm{Irr}(G)$.

(b) $g \notin \cup_{g \in G} g^{-1}Bg - \{1\}$ と $i = 1, \dots, n$ に対して，$\chi_i(g) = \chi_1(g) \in \mathbb{Z}$ である．

(c) $i, j = 1, \dots, n$ に対して $\theta_i^G - \theta_j^G = \epsilon(\chi_i - \chi_j)$ となる．ここで $\epsilon$ は $\pm 1$ のどちらか．

では，$\chi_{k|B}$ を計算してみよう．フロベニウスの相互法則により，

$$\delta_{k,i} - \delta_{k,j} = \langle \chi_k, \chi_i - \chi_j \rangle = \epsilon \langle \chi_k, \theta_i^G - \theta_j^G \rangle = \epsilon \langle \chi_{k|B}, \theta_i - \theta_j \rangle$$

なので，$j \neq k$ に対しては，$\langle \chi_{k|B}, \theta_k - \theta_j \rangle = \epsilon$ を得る．それゆえ，$\chi_{k|B}$ における $\theta_k^j$ $(j = 1, 2, \dots, w)$ の重複度は $i, j, k \neq s$ に対して $\theta_s^i$ の重複度と丁度 $\epsilon$ だけ違う．それゆえ，次の式を満たす非負整数 $\lambda_0$ と $\lambda_1$ がある．

$$\chi_{k|B} = \lambda_0 1_B + \epsilon \sum_{i=1}^{w} \theta_k^i + \lambda_1 \left( \sum_{j=1}^{n} \sum_{i=1}^{w} \theta_j^i \right)$$

**補題 3.4** $\lambda_1 = 0$ で $\epsilon = 1$ となる．

証明　$\lambda_1 \neq 0$ と仮定すると，$n > |H|$ と仮定したので，$\deg(\chi_k) \geq (\epsilon|W| + |B| - 1) \geq |B| - |W| - 1 = n|W| - |W| = (n-1)|W| \geq |H||W|$ を得る．それゆえ，

$$|G| > \sum_{k=1}^{n} \chi_k(1)^2 \geq n(|H||W|)^2 = |H|^2|W|(|B| - 1)$$

である．一方，$|G| < |C_1 \cap C_G(t_\alpha)||H|^2 \leq |B||H|^2$ なので，$|W|(|B| - 1) < |B|$ が出て来る．しかし $|W| \geq 2$ かつ $|B| \geq 3$ なので，これは矛盾である．$\theta_k^i$ の $\chi_{k|B}$ における重複度は非負なので，$\epsilon = 1$ であることは自明であり、故に補題が成り立つ．∎

最後の補題から，$\chi_{k|B} = \lambda_0 1_B + \sum_{i=1}^{w} \theta_k^i$ であり，

$$\langle \chi_k, \theta_j^G \rangle = \langle \chi_{k|B}, \theta_j \rangle = \langle \lambda_0 1_B + \sum_{i=1}^{w} \theta_k^i, \theta_j \rangle = \delta_{k,j}$$

である．すなわち，$\theta_j^G$ の既約分解は $\chi_j$ を丁度 1 つ持ち，$k \neq j$ に対しては $\chi_k$ を含んでいない．すなわち，$j = 1, \dots, n$ に対して，

$$\theta_i^G = \chi_i + \phi,$$

かつ $\langle\phi,\chi_j\rangle=0$ となる指標 $\phi$ がある．

定理 1.1 の仮定から，$G$ のシロー 2 部分群 $P$ は巡回群でも一般 4 元数群でもないので (即ち、2 ランク 1 ではない)，$P$ は $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2Z$ を含む．一方，フロベニウス部分群 $N=BW$ の補群である $W$ は 2-ランク 1 であり，中心に位数 2 の元を含んでいる．それゆえ，一般性を失うことなく，$W\subset H$ と仮定して問題ない．しかし $N=BW$ は $G$ のシロー 2 部分群を含んでいないので，$|W|\leq|H|/2$ が成り立つ．

この事実を使って，最終的な矛盾を得るための次の補題を証明しよう．

**補題 3.5** すべての $i=1,...,n$ に対して $\deg\chi_i=|W|$ である．

証明　$G=N\cup(\cup_{i=1}^{p}Ng_iB)$ を double coset 分解とする．$B$ は TI 部分群なので，$i=1,...,p$ に対して $N^{g_i}\cap B=\{1\}$ である．ここで，$N$ の任意の指標 $\xi$ に Mackey 分解定理を適用すると，

$$\xi^G{}_{|B}=\xi_{|B}+\sum_{i=1}^{p}(\xi_{|N^{g_i}\cap B})^B$$

となる．それゆえ，

$$\xi^G{}_{|B}=\xi_{|B}+p\cdot\deg(\xi)\rho_B,$$

である．ここで，$\rho_B$ は $B$ の正則指標である．

この公式を $\xi=(1_B)^N$ と $\xi=\theta_i^N$ に適用して計算すると，

$$\langle(1_B)^G-\theta_i^G,(1_B)^G-\theta_i^G\rangle=\langle w1_B-\sum_{j=1}^{w}\theta_i^j,1_B-\theta_i\rangle=w+1. \tag{2.1}$$

を得る．ここで，$\deg((1_B)^N)=w=\deg(\theta_i^N)$ であり，$((1_B)^G-\theta_i^G)_{|B}=(1_B)^N{}_{|B}-\theta_i^N{}_{|B}$ となっていることに注意すること．

補題 3.4 から $\lambda_1=0$ なので，$\chi_{k|B}=\lambda_0 1_B+\sum_{i=1}^{w}\theta_k^i$ なっていることに注意．もし $\lambda_0\neq0$ なら，$(1_B)^G$ の既約分解は $1_G,\chi_1,...,\chi_n$ を正係数で含むが，補題 3.4 の証明の後で述べたように，$\theta_j^G$ は $i\neq j$ ならどの $\chi_i$ も含まない．それゆえ，$1_B^G-\theta_j^G$ の既約分解は $1_G,\chi_i\ (i\neq j)$ の各々を正係数で含む．これは $1+(n-1)=n\leq|W|+1\leq|H|/2+1\leq|H|$ を意味するが，我々の仮定 $n>|H|$ に矛盾している．

それゆえ，$\lambda_0=0$ であり，$\chi_{k|B}=\sum_{i=1}^{w}\theta_k^i$ となる．これは $k\in\{1,2,\ldots,n\}$ に対して，$\deg(\chi_k)=|W|=w$ であることを意味している．∎

さて，仮定 $n>|H|$ に対する最終的な矛盾を導こう．上で見たように，$g\in G$ が $B-\{1\}$ の元に共役でないとすると，値 $\chi_i(g)$ は有理整数であり，$i$ に依存していない．特に，もし $g\neq1$ が 2-元なら，

$$|C_G(g)|=\sum_{\chi\in Irr(G)}\chi(g)\overline{\chi(g)}>\sum_{i=1}^{n}\chi_i(g)^2=n\chi_1(g)^2$$

である．仮定から，$|C_G(g)|\leq|H|<n$ なので，すべての 2 元 $g\neq1$ に対して，$\chi_i(g)=0$ を得る．これは $P$ を $G$ のシロー 2 群とすると，$\chi_{i|P}$ が $P$ の正則表現の倍数となっていることを意味する．特に，$\chi_i(1)$ は $|P|$ の倍数となるが，これは $P$ が $W$ を割らないので，$\chi_i(1)=|W|$ であることに矛盾する．

これで命題 3.3 と定理 1.1 の証明が完成した．

## 4 予想

では，実際に，$G$ の位数 $|G|$ と $|H| = |C_G(t)|$ との関係はどのぐらいになっているのだろうか？
直接の計算から，$|G| = |H|^e$ ・として $e$ を求めると右図のようになる．

| $G$ | $e$ | $G$ | $e$ |
|---|---|---|---|
| $A_5$ | 2.9534 | $A_6$ | 2.8305 |
| $A_7$ | 2.4644 | $PSL(2,q)$ | $\leq 3, \to 3$ |
| $M_11$ | 2.3190 | $M_22$ | 2.1851 |
| $M_23$ | 2.0437 | $J_1$ | 2.5224 |
| $J_3$ | 2.3455 | $Mc$ | 2.0800 |
| $Ly$ | 2.1989 | $Th$ | 2.1283 |
| $O'Nan$ | 2.2396 | $Mc$ | 1.9440 |

ということで，予想を提起しよう。

予想 1(K.Harada). $G$ を 2-ランクが 2 以上の任意の有限とする．このとき，ある involution $t$ があって，$|G| \leq |C_G(t)|^3$ となる．

予想 2 (Lyons). いかなる involution $t$ に対してもそれを含む 4 部分群 $V$ が存在して $\prod_{g \in V^\times} |C_G(g)| \geq |G|$ が成り立つ．

予想 3 (K.Harada). いかなる 4 部分群 $V$ に対しても $\prod_{g \in V^\times} |C_G(g)| \geq |G|$ が成り立つ．

予想 4 (M.Miyamoto). 任意の基本アーベル 2 部分群 $V$ に対して，$\prod_{[V:T]=2} |C_G(T)| \geq |G|$ が成り立つ．

## References


[A] M. Aschbacher, *Finite Group Theory*, second edition, Cambridge studies in advanced mathematics, Cambridge University Press, 2000.

[BF] R. Brauer and K. A. Fowler, On groups of even order, Annals of Mathematics, Vol. 62, (1955) 565-583.

[L] R. Lyons, Evidence for a New Finite Simple Group, Jour. Algebra, Vol. 20, (1972), 540-569.

[M] G. A. Michler, Theory of Finite Simple Groups, in preparation.

[P] D. Parrott, On Thompson's Simple Group, Jour.Algebra, Vol.46, (1977), 389-404.

[S] M. Suzuki, On finite groups with cyclic Sylow subgroups for all odd primes, Amer. Jour. Math., 77 (1955), 657-691.

# 有限置換群と自己直交符号

室蘭工業大学・工学部　千吉良直紀 (Naoki Chigira)
Muroran Institute of Technology
山形大学・理学部　原田昌晃 (Masaaki Harada)
Yamagata University
千葉大学・理学部　北詰正顕 (Masaaki Kitazume) [1]
Chiba University

この講演に関する研究は，タイトルに記した3名の共同研究である。また，多くの計算を MAGMA [1] によっている。本稿に現れる code について，群の情報からの code の構成，次元・最小重さの決定，自己同型群の計算等は基本的に MAGMA によるものである。

## 1　定義と例

昨年 (2004 年)12 月の京都での研究集会「代数的組合せ論」において，我々は $J_2:2$ を自己同型群に持つ（新しい）self-dual code $C_{10}$ について発表した [3]。その重要な性質の一つが，$C_{10}$ が weight 14 の codeword 全体で生成されることであり，この weight 14 の codeword は，実は outer involution の固定点の集合として得られるものだった ([11]) ということである。一方，有名な例として Mathieu 群 $M_{24}$ を自己同型群とする extended binary Golay code は，$M_{24}$ の $2A$ と呼ばれる involution の固定点が weight 8 の codeword になっており，それらによって code が生成されている。

このような observation を契機に，一般の次数 $n$ の置換群について，その involution の固定点の生成する code について考えた結果，以下のような結果を得た。これは，先述の集会でも，いくつかの例と共に報告済みである。

[1]講演者であり，本稿の文責を負う。

$(G,\Omega)$ を次数 $n(=|\Omega|)$ の置換群とする。$\Omega$ の部分集合全体を，和を対称差 $A+B=(A\cup B)\setminus(A\cap B)$ で定義することで，2元体上の $n$ 次元ベクトル空間とみなす。このとき，$G$ の位数2の元 $\sigma$ の固定点 $Fix(\sigma)$ の生成する code の直交補空間を $C(G,\Omega)$ と表す。

$$C(G,\Omega):=\langle Fix(\sigma)\mid \sigma\in I(G)\rangle^{\perp}$$

その次数で置換表現が一意に決まるなら，これを $C(G,n)$ と表すことにする。

**定理 1 ([4]).** $C$ を $G$ の $\Omega$ への作用で不変な，長さ $n$ の self-orthogonal code とするとき，

$$C\subset C(G,\Omega)$$

が成り立つ。

*Proof.* $X\in C$ と $\sigma\in I(G)$ を任意に取ると，$\sigma^2=1$ であることから，$\langle\sigma\rangle$ は $X\cap X^{\sigma}$ に作用する。また $C$ が self-orthogonal であるという仮定から $|X\cap X^{\sigma}|$ は偶数である。さて $X\cap X^{\sigma}\supseteq Fix(\sigma)\cap X$ であることに注意して，$Y=(X\cap X^{\sigma})\setminus(Fix(\sigma)\cap X)$ とおく。$Y$ は $\{a,a^{\sigma}\}$ $(a\in Y)$ という形の部分集合の disjoint union になり，$|Y|$ が偶数であることがわかり，従って $|Fix(\sigma)\cap X|$ も偶数である。すなわち，任意の $Fix(\sigma)$ と $X$ が直交するので定理を得る。 □

証明は非常に易しい。しかしながら，次の例1に述べた $C(J_2:2,100)$ が過去の文献に見あたらない（グラフから作る例2の code が文献にあるにもかかわらず）ところを見ると，これまでに着目された対象ではないのだろうと思う。

**例 1.** $G=J_2:2$ (resp. $M_{24}$) のとき，冒頭に書いた code は $C(J_2:2,100)$ (resp. $(M_{24},24)$) と一致している。従って，この code が $G$ の作用する「唯一の」長さ 100 (resp. 24) の self-dual であることがわかる。

**例 2 ($C(J_2,100)$).** $G=J_2$ とすると，$C(J_2,100)$ は少し大きく $[100,63,8]$ code になる。実は，直交補空間を取る前の，$\langle Fix(\sigma)\mid\sigma\in I(G)\rangle$ の方がよく知られていて，これは，$J_2$ の作用する rank 3 graph の近傍 (36点集合) によって生成される $[100,36,16]$ code (これは，Key-Moori [8] によって計算された) に全体集合 $\Omega$ を付け加えた doubly even $[100,37,16]$ code になっている。しかし，$C(J_2,100)$ はずっと大きいから，もっと大きな self-dual が存在しうるわけで，実際，$J_2$ を自己同型群に持つ $[100,50,16]$ code $C_{16}$ を構成することが出来る。さらに，$C(J_2,100)$ に含まれる $J_2$ 不変な self-dual code が，$C_{10},C_{16}$，および，$C_{16}$ と同値な $C'_{16}$ に限ることも証明することが出来た。

$C(G,\Omega)$ は一般に self-orthogonal ではない。しかし，$C(G,\Omega)$ 自体が self-orthogonal である場合もいくつかあって，過去に知られていた多くの（散在型単純群に関連する）例を含んでいる。これを以下に例示しておこう。

例 3 ($C(HS,100)$). Higman-Sims の群 $HS$ は，やはり 100 次の rank 3 の置換群であり，rank 3 graph の近傍 (22 点集合) で生成させた code $C$ は $[100,22,22]$ code となる。この code の自己同型群は graph の自己同型群と一致し $HS:2$ となるが，$C(HS:2,100)$ が上記の code $C$ と一致する。$C(HS,100)$ は少し大きくなって $[100,23,22]$ code となり，上記の $C(HS:2,100)$ の他に，$HS$ 不変な 2 つの互いに同値な $[100,22,32]$ code を含んでいる[2]。これらの code は [12] で述べられているものである。

例 4 ($C(HS,176)$). Higman's design として知られている 2-$(176,50,14)$ design がある [7]。そのブロックで生成される code は self-orthogonal $[176,22,50]$ code で，Calderbank-Wales [2] で構成されたものであり，$C(HS,176)$ と一致する。その自己同型群は，デザイン，code 共に，Higman-Sims の群 $HS$ である。

この Higman's design は，Mathieu 群 $M_{22}$ の言葉だけで定義されていて，そこから $HS$ が自己同型群として得られるところに面白さがあると思う。今回の code について言うと，$C(HS,176)=C(M_{22},176)$ が成立している。

例 5 ($C(Co_3,276), C(McL,275)$). Conway 群 $Co_3$ は 276 次の 2 重可移表現を持つ。その 1 点の固定部分群は McLaughlin の群の拡大 $McL{:}2$ で 275 点上ランク 3 に作用している。このときの $C(Co_3,276)$, $C(McL{:}2,275)$ は，共に doubly even で $[276,23,100]$, $[275,22,100]$ というパラメータを持つ。また自己同型群は元の群 $Co_3$, $McL{:}2$ に一致する。これらの code は [6] で構成されていたものである。

例 6 (**Reed-Muller codes**). 無限系列である Reed-Muller code は，$2^n:L_n(2)$ の $2^n$ 次の置換表現から得られる。

$$C(2^n{:}L_n(2),2^n)=R(n-[n/2]-1,n)$$

Reed-Muller code は $n$ を定めた上で，有限系列として得られるが，ここに現れるのは，その中で self-orthogonal である最大のものである。特に $n$ が奇数なら self-dual である。

もう一つの，よく知られている self-dual code の無限系列である，平方剰余符号については，我々の $C(G,\Omega)$ は役立たない。$G=L_2(q)$ の $\Omega=GF(q)\cup\{\infty\}$

[2]2005 年春の学会での講演および予稿集は，この記述が間違っている。

への作用において，位数2の元が固定点を持たないので $C(G,\Omega)$ が全空間になってしまうからである。

次に，$C(G,\Omega)$（自体ではなく）が self-dual code を含む場合を一般的に考察しておこう。次の補題は，容易に示される。

**補題 1.** $C$ $(\subset \mathcal{P}(\Omega))$ が $G$-不変な長さ $n$ の self-dual code ならば，$C(G,\Omega)^{\perp}$ は self-orthogonal で

$$C(G,\Omega) \supset C \supset C(G,\Omega)^{\perp}$$

が成立する。

$C(G,\Omega)^{\perp}$ が self-orthogonal であるという条件は，$\chi$ を置換表現 $(G,\Omega)$ の指標を表すものとすると，次のように言い換えられる。

**補題 2.** $C(G,\Omega)^{\perp}$ が self-orthogonal であるための必要十分条件は，$G$ の任意の involution $\sigma,\tau$ に対し，

$$\chi(\sigma\tau) \equiv 0 \pmod 2$$

が成立することである。

*Proof.* $C(G,\Omega)^{\perp}$ とは，$\langle Fix(\sigma) | \sigma \in I(G) \rangle$, すなわち（dual を取る前の）固定点によって生成される code であるから，これが self-orthogonal であることは，任意の $\sigma,\tau \in I(G)$ に対し，

$$|Fix(\sigma) \cap Fix(\tau)| \equiv 0 \pmod 2$$

であることを意味している。一方，$\chi(\sigma\tau) = |Fix(\sigma\tau)|$ であるが，右辺を書き直すと

$$\chi(\sigma\tau) = \#\{a \in \Omega \mid \sigma(a) = \tau(a) = a\} + \#\{a \in \Omega \mid \sigma(a) = \tau(a) \neq a\}$$

となるが，第2項は $\{a,\sigma(a)\}$ の形の集合の disjoint union になるから偶数である。従って，

$$\chi(\sigma\tau) \equiv \#\{a \in \Omega \mid \sigma(a) = \tau(a) = a\} \equiv |Fix(\sigma) \cap Fix(\tau)| \pmod 2$$

を得る。 □

$C(G,\Omega)$ が self-dual code を含む場合の例については，次節以降に掲げることにする。

## 2 原始置換群の場合

最初の $M_{24}, J_2 : 2$ の例に鑑みて，self-dual code の話から始める。まずは，$C(G,\Omega)$ が self-dual になっているのは，どれくらいの場合があるのかを述べる。結論から言うと，数少ない例しか存在しない。実際，我々が知っているのは，原始的な置換群については，次の場合に限る。

- $G_{24} = C(M_{24}, 24)$ : the extended Golay code
- $C_{10} = C(J_2 : 2, 100)$ : [CHK]
- $C(M_{22}{:}2, 330)$ : self-dual $[330, 165, 10]$, Aut $\cong M_{22}{:}2$ (New!)
- $C(2^{2m+1}{:}L_{2m+1}(2), 2^{2m+1}) = R(m, 2m+1)$ : the Reed-Muller code

「原始的」という条件については，次節で述べることにして，以下では，原始置換群に限って話を進めることにする。

次に，$C(G,\Omega)$ が self-dual code を含む場合について，例を挙げる。

**例 7** ($(J_2, 100)$). 前節で述べたとおり，$C(J_2,100)^\perp$ は doubly even (従って self-orthogonal) である。$C(J_2,100)$ は $J_2$ 不変な self-dual code をちょうど3つ ($C_{10}$, $C_{16}, C'_{16}$) 含んでいる。

**例 8** ($(S_4(3), 40)$). $G = S_4(3) \cong O_5(3) \cong U_4(2)$ として，その部分群 $H = 3^{1+2} : 2A_4$ を考えると，これは原始的な $40(= [G : H])$ 次の置換表現を与える。このとき，$C(G, G/H) = [40, 25, 4]$ code で，$C(G, G/H)^\perp$ は self-orthogonal $[40, 15, 8]$ code である。しかし，$C(G, G/H)$ は $G$ 不変な self-dual code を含んでいないことが示される。

さて，補題 1, 2 の条件を満たす（すなわち，$G$ 不変な self-dual code が存在する可能性のある）原始置換群は，どれくらいあるだろうか。これもまた，実は，限られた場合にすぎないことが分かった。(なお，以下の2つの命題で $C(G,\Omega)^\perp$ に ($\neq \{0\}$) いう注釈を付けた。これは，位数2の元が固定点を持たず $C(G,\Omega)$ が全空間になる場合を除いたものである。)

**命題 1** (小さい次数の原始置換群). $(G,\Omega)$ を次数 100 以下の原始置換群とする。このとき，$C(G,\Omega)^\perp (\neq \{0\})$ が self-orthogonal となるのは，以下のいずれかに限る。

$$G_{24}, C_{10}, R(m, 2m+1)\ (m = 1, 2), C(S_4(3), 40), C(J_2, 100),$$

および

$$C(2^6{:}X, 64)\ (X \cong U_3(3), A_8, S_4(3), \{2,3\}\text{-group}, \cdots).$$

□

すなわち，既に述べた例を除けば次数 64 のところに集中しているということである[3]。$X$ の構造は可解群の場合がいくつもあって，煩雑であるので省略する。さらに次数の大きい範囲まで探索することはできて，次に沢山の例が集中して現れるのは 256 次の場合である。ここでは，一般に高い次数を考えるのは避けて，話を単純群の周辺に絞ってみよう。

**命題 2.** $(G, \Omega)$ を 次数 1000 以下 の原始置換群とし，$G$ は almost simple で，かつ，その simple part が ATLAS [5] に掲載されている群 とする。このとき，$C(G,\Omega)^{\perp}(\neq \{0\})$ が self-orthogonal となるのは，以下のいずれかに限る。

$$G_{24}, C_{10}, C(M_{22}:2, 330), C(S_4(3), 40), C(J_2, 100),$$

$$C(M_{12}, 144), C(M_{12}, 220), C(M_{22}, 330), C(M_{22}, 672).$$

ただし，以下の場合については計算していない。

$$C(O_{10}^{+}(2), 527), C(O_{10}^{-}(2), 528)$$

□

"ATLAS に掲載されている" という条件は，もちろん本質的ではない。しかし，その範囲で調べただけでも，"有限単純群を自己同型群に持つ self-dual code" というものがいかに希なものかがわかる。

なお，次数が 1000 を超えると，計算できない場合が増えてしまう。例えば，散在型単純群の場合だと，

$$C(McL, 2025), C(He, 2058), C(Ru, 4060)$$

$$C(Suz, 1782), C(Co_2, 2300), C(F_{22}, 3510)$$

などは未計算である。計算可能だった例の中では，

$$C(M_{12}:2, 1584), C(M_{24}, 2024), C(J_2(:2), 10080)$$

が self-dual を含む可能性を残していた。

命題 2 の中からひとつとって，self-dual code の決定と，その自己同型群の計算例を示しておく。

[3]これについては，2005 年 10 月の京都での集会で発表した（講演者は千吉良氏）。

例 9 ($C(M_{12},220)$). $C=C(M_{12},220)$ は $[220,111,18]$ code となる。さらに $C^{\perp}$ は doubly even で，次元を見れば $\dim(C/C^{\perp})=2$ であることが分かる。よって，$C$ は丁度 3 つの self-dual code $C_1,C_2,C_3$ を含んでおり，$\mathrm{Aut}(C_i)\subset\mathrm{Aut}(C)$ である。なぜなら，$C_i$ の weight が 4 の倍数である codeword 全体が $C^{\perp}$ を生成するからである。

さて，$M_{12}$ の 220 次の作用は原始的であるから $\mathrm{Aut}(C)$ の作用も原始的である。1000 次未満の原始的な置換群は分類されていて，そのデータベースが MAGMA に組み込まれている [10]。この分類によれば，$\mathrm{Aut}(C)$ は，$M_{12},A_{12},S_{12},A_{220},S_{220}$ のいずれかと同型になる。このうち，$\mathrm{Aut}(C)\neq A_{220},S_{220}$ は明らかである。次に $C(A_{12},220)$ と $C(S_{12},220)$ を計算してみると，この 2 つは一致して $[220,55,28]$-code であることがわかり，$C_i\subset C\not\subset C(A_{12},220)=C(S_{12},220)$ となるから，$\mathrm{Aut}(C)\neq A_{12},S_{12}$ を得る。よって，$\mathrm{Aut}(C)=\mathrm{Aut}(C_i)\cong M_{12}$ $(i=1,2,3)$ である。

## 3 非原始的な場合

ここでは，非原始的な場合について述べる。実は，「原始的」より少し弱い，以下の条件が重要である。

条件. $N:=N_G(I(H))=H$.

原始性を仮定すれば，$H$ が極大部分群になるので，上の条件は成立する。

補題 3. $\sigma\in I(G)$ とする。ある $a\in N$ に対し $\sigma(aH)=aH$ ならば，全ての $b\in N$ に対し $\sigma(bH)=bH$ である。

*Proof.* $\sigma(aH)=aH$ とすると $a^{-1}\sigma a\in I(H)$ より $\sigma\in I(H)$ となり $b^{-1}\sigma b\in I(H)\subset H$ を得る。従って $\sigma(bH)=bb^{-1}\sigma(bH)=bH$ である。 □

従って，$G/H$ の coset のうち $N=N_G(I(H))$ に含まれるものは，全体が involution の固定点になるか，involution によっては 1 点も固定されないかのいずれかである。つまり記号を整理して書くと，

$$G/N=\{g_1N,\dots,g_rN\}\ (r=[G:N])$$
$$X_i=g_i(N/H)=\{g_iaH\mid a\in N\}\ (|X_i|=n/r=|N:H|)$$

とおけば，$\Omega=X_1\cup\cdots\cup X_r$ となるが，$\sigma\in I(G)$ の固定点 $Fix(\sigma)$ は，いくつかの $X_i$ 達の和集合になる。このとき，$X_i$ の 2 点部分集合は明らかに $X_i$ 達と直交

するので，$C(G,G/H)$ に含まれる。これより，上記の条件が成り立たないときは，$C(G,G/H)$ の minimum weight が 2 になることがわかる。(容易な議論で，逆も成立することがわかる。)

そこで，

$$F_1(\sigma) := \{g_iN \mid X_i \subset Fix(\sigma)\} \subset G/N$$

$$C' = \langle F_1(\sigma) \mid \sigma \in I(G)\rangle^{\perp} \subset \mathcal{P}(G/N).$$

とおく。$C'$ は長さ $r = |G/N|$ $(\leq n = |G/H|)$ の code である。このとき，自己同型群の計算は $C'$ に帰着できる。すなわち，

$$\mathrm{Aut}(C(G,\Omega)) \cong S_{n/r} \wr \mathrm{Aut}(C')$$

が成り立つ。さらに，$n/r$ が奇数の場合は $C' = C(G,G/N)$ となって，$C'$ 自体が置換表現から作られる code になるのである。なお，$|X_i| = n/r$ が偶数の場合は $C(G,\Omega)^{\perp}$ は self-orthogonal になるが，この場合に $C(G,\Omega)$ がどんな self-dual code を含んでいるかは，(今のところ) 追求していない。

ここでは，原始的でないが上記の条件をみたす場合として，次のような状況を考えてみよう。

(1) $G = K\langle\rho\rangle \supset K \supset H$ $(\rho^2 = 1)$

(2) $N_G(I(H)) = H$

(1) により $K \supset H$ なので $G$ の $G/H$ への作用は原始的ではない。(2) が，今考えていた条件である。これにより，$N_G(H) = H$ であり，$H$ と $H^{\rho}$ は $K$ では共役でない。

このとき，$\chi$ を $(K,K/H)$ の置換表現の指標とすると，$(G,G/H)$ の置換表現の指標は $\chi + \chi^{\rho}$ となる。従って，補題 2 より，$C(G,G/H)^{\perp}$ が self-orthogonal であるための条件は，

$$\chi(\sigma\tau) \equiv \chi^{\rho}(\sigma\tau) \pmod 2 \ (\forall \sigma,\tau \in I(G))$$

となる。

ここでは，(あくまで経験的法則として) 一つのことだけを述べたいと思う。上の合同式が成立しない (従って $C(G,G/H)$ は self-orthogonal でない) 場合というのが，わずかな例しか存在しないということである。$\chi$ と $\chi^{\rho}$ が等しければ当然成り立つ式である。わずかしかないと書いたのは，$\chi \neq \chi^{\rho}$ であっても，上の合同式だけは成立する場合が多いということである。

例 10. 我々が知る限りでは，$C(G, G/H)$ が self-orthogonal でないのは，次の例だけである。これらの例を特長付けることは出来ないだろうか。

(1) $G = PGL(2,9)$ or $M_{10}$ $(K = A_6)$ に対する $C(G,12), C(G,30)$.

(2) $G = U_3(5) : 2$ に対する $C(G,100), C(G,350)$.

例 11 $(C(M_{12} : 2, 24))$. $G = M_{12} : 2, H = M_{11}$ の場合，$\chi \neq \chi^\rho$ は有名な事実であるが，上の合同式は成立して，$C(G,24)$ としては extended Golay code $G_{24}$ が出てくるのである。

## 参考文献


[1] W. Bosma and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[2] A.R. Calderbank and D.B. Wales, A global code invariant under the Higman–Sims group, *J. Algebra* **75** (1982), 233–260.

[3] N. Chigira, M. Harada and M. Kitazume, Some Self-Dual Codes Invariant under the Hall–Janko Group, submitted.

[4] N. Chigira, M. Harada and M. Kitazume, Finite permutation groups and self-orthogonal codes, submitted.

[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[6] W.H. Haemers, C. Parker, V. Pless and V. Tonchev, A design and a code invariant under the simple group $Co_3$, *J. Combin. Theory Ser. A* **62** (1993), 225–233.

[7] G. Higman, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* **13** (1969), 74–80.

[8] J.D. Key and J. Moori, Codes, designs and graphs from the Janko groups $J_1$ and $J_2$, *J. Combin. Math. Combin. Comput.* **40** (2002), 143–159.

[9] J. Moori and B.G. Rodrigues, A self-orthogonal doubly even code invariant under $M^cL:2$, *J. Combin. Theory Ser. A* **110** (2005), 53–69.

[10] C.M. Roney-Dougal and W.R. Unger, The affine primitive permutation groups of degree less than 1000, *J. Symbolic Comput.* **35** (2003), 421–439.

[11] J. Tits, Le groupe de Janko d'ordere 604,800, in "Theory of Finite Groups (R. Brauer and C. Sah eds.)", 91–95, Benjamin, New York-Amsterdam, 1969.

[12] V.D. Tonchev, Binary codes derived from the Hoffmon–Singleton and Higman–Sims graphs, *IEEE Trans. Inform. Theory* **43** (1997), 1021–1025.

# On a 5-design related to an extremal doubly-even self-dual code

山形大学・理学部
原田 昌晃*

## 1 序論

長さ $n$ の doubly-even self-dual code の minimum weight $d$ は $d \leq 4[n/24]+4$ を満たし [5], $d = 4[n/24]+4$ の場合 extremal とよばれる. 長さが $24m$ の場合の extremal doubly-even self-dual code については, 長さ 24 と 48 についてのみ code の存在が知られているが, その他の場合での存在は知られていない (ただし, $m \geq 154$ の場合には非存在が分かっている). 例えば長さ 72 の場合に存在を決める問題は非常に有名な問題で未だに未解決である [7]. 確かに難しい問題なので何とかアプローチする方法を見付けたい訳であるがなかなかうまく行かない. ここでは次のようなことを考えてみた.

$C$ を長さ $24m$ の extremal doubly-even self-dual code とすると, Assmus-Mattson の定理 [1] によって minimum weight の codeword は 5-design $D$ をなすことが分かる. さらに $C$ が self-dual であることから, この design $D$ は self-orthogonal になる. ここで一般に $t$-$(v,k,\lambda)$ design が self-orthogonal であるとは, 全ての異なる block の共通部分の濃度と block size $k$ の偶奇が一致する場合をいう [8]. 上の逆の状況を考えると次のようになる.

**問題.** $C$ を長さ $24m$ の extremal doubly-even self-dual code とし, $D$ を $C$ の minimum weight の codeword がなす self-orthogonal 5-design とする. $E$ を $D$ と同じパラメータをもつ任意の self-orthogonal 5-design とし

*Email: mharada@sci.kj.yamagata-u.ac.jp

たとき $E$ の incidence matrix の行が生成する code は extremal doubly-even self-dual code になるか？

Steiner system $S(5,8,24)$ が self-orthogonal design でその incidence matrix の行が生成する code が extended Golay $[24,12,8]$ code になることは良く知られた事実であるので，$m=1$ のときの答えは正しい．$m=2,3$ の場合にも正しいことが最近分かった [4], [3]．ここでは論文 [2] に基づいて $m=4$ のときも正しいことの証明を，$m\leq 3$ の場合との相違点を含めて，行なう．一般的によく使われている用語を用いているが，紹介していない用語については [2], [3], [4], [8] などを見ていただきたい．

## 2 主結果とその証明

$C$ を長さ 96 の extremal doubly-even self-dual code とすると，Assmus-Mattson の定理 [1] によって minimum weight の codeword は 5-$(96,20,816)$ design $D$ をなす．さらに $C$ が self-dual であることから，この design $D$ は self-orthogonal になる．この原稿での主結果は次である．

**定理 1.** $E$ を任意の self-orthogonal 5-$(96,20,816)$ design とし，$F$ を $E$ の incidence matrix $A$ の行が生成する code とする．このとき $F$ は長さ 96 の extremal doubly-even self-dual code になる．

一般に $t$-$(v,k,\lambda)$ design は $s$-$(v,k,\lambda_s)$ design $(s\leq t)$ となることが知られている．5-$(96,20,816)$ design の場合は

$$\lambda_0=3217056,\lambda_1=670220,\lambda_2=134044,$$
$$\lambda_3=25668,\lambda_4=4692,\lambda_5=816$$

となる．$E$ は self-orthogonal でその block size は 20 であることから得られる code $F$ は doubly-even self-orthogonal になることが直ちに分かる．次に $w\in F^{\perp}$ を weight $m>0$ の vector とし，$S$ をその support とする．$E$ の incidence matrix $A$ において $S$ での 1 の個数が $i$ である行の個数を $n_i$ で表すことにする．$E$ が 5-design であることから，次の連立方程式が成り立つ (例えば [3], [8] を参照):

$$\sum_{i=0}^{[m/2]}\binom{2i}{j}n_{2i}=\lambda_j\binom{m}{j}\quad(j=0,1,\ldots,5). \tag{1}$$

**補題 2.** $m \not\equiv 0 \pmod 4$ の場合, 連立方程式 (1) は非負整数からなる解 $(n_0, n_2, \ldots)$ を持たない.

**証明.** (1) を解くと

$$n_{10} = -6n_{12} - 21n_{14} - 56n_{16} - 126n_{18} - 252n_{20} + \alpha_{10}$$

ただし

$$\alpha_{10} = \frac{1}{320}(7254912m - 1508060m^2 + 122095m^3 - 4590m^4 + 68m^5)$$

となる. ここで, $m \not\equiv 0 \pmod 4$ の場合 $\alpha_{10}$ の分子は 32 で割り切れないことが分かる. □

上の補題が述べていることは $F^\perp$ には weight $\not\equiv 0 \pmod 4$ なる codeword がないことであり, これは $F^\perp$ が doubly-even であることを示している. ここで一般に doubly-even code は self-orthogonal であることから $F^\perp$ が self-orthogonal になることが分かり, $F$ が self-dual になる. したがって $F$ は doubly-even self-dual code になる.

**補題 3.** $m = 4, 8$ の場合, 連立方程式 (1) は非負整数からなる解 $(n_0, n_2, \ldots)$ を持たない. また $m = 12$ の場合, 連立方程式 (1) は仮定 $n_{12} = 0$ のもとで非負整数からなる解 $(n_0, n_2, \ldots)$ を持たない.

**証明.** $m = 4, 8$ の場合は (1) は解自体を持たない. $m = 12$ の場合は (1) は次の解のみを持つ:

$$n_0 = 284025, n_2 = 1986474, n_4 = 773010,$$
$$n_6 = 213552, n_8 = -48195, n_{10} = 8190.$$

したがって, 示された. □

補題 3 より直接 $F^\perp$ $(= F)$ が weight 4, 8 の codeword を含まないことが分かる. $m = 12$ の場合を考える. もし $n_{12} \neq 0$ であれば $E$ の block に対応する codeword (weight 20) と $w$ の和が weight 8 になるので $n_{12} = 0$ でなければいけない. 再び, 補題 3 より $F^\perp$ $(= F)$ は weight 12 の codeword を含まないことが分かる. 以上から $F$ は doubly-even self-dual $[96, 48, d = 16$ または $20]$ code であることが分かった.

**注意 4.** 残念ながら $m=16$ の場合 (1) は例えば次のような解を持つ:

$$n_0 = 101872, n_2 = 1282800, n_4 = 1436400, n_6 = 379680,$$
$$n_8 = 14400, n_{10} = 1904, n_{12} = \cdots = n_{20} = 0.$$

したがって (1) からは直接 weight 16 の codeword が存在しないことを示すことは出来ない. この部分は長さ 72 までの場合 [3], [4] (または [9] を参照) との大きな違いである. この辺りから, 最初に述べた問題を一般的に解決するにはこのままのアプローチでは無理のように思える.

次に doubly-even self-dual $[96, 48, d \geq 16]$ code の weight enumerator $W$ を考える. Gleason の定理 ([5] や [6, Theorem 13] を参照) によって, 長さ $n$ の doubly-even self-dual code の weight enumerator は整数 $a_i$ を用いて

$$\sum_{i=0}^{[n/24]} a_i (x^8 + 14x^4y^4 + y^8)^{n/8-3i} (x^4y^4(x^4 - y^4)^4)^i$$

と表せる. したがって, 今回の場合は $d \geq 16$ であることから $a_0, a_1, a_2, a_3$ は一意に決まり

$$W = x^{96} + (-28086 + a_4)x^{80}y^{16} + (3666432 - 16a_4)x^{76}y^{20}$$
$$+ (366474560 + 120a_4)x^{72}y^{24} + (18658567680 - 560a_4)x^{68}y^{28} + \cdots$$

と整数 $a_4$ のみを用いて表せることが分かる. ここで $A_i$ を $x^{96-i}y^i$ の係数とする (この数は weight $i$ の codeword の個数を表す). $A_{16} \geq 0$ であることから $a_4 \geq 28086$ となる. したがって $A_{20} \leq 3217056$ となり $A_{20} = 3217056$ であることと $d = 20$ であることが同値になる. ここで, 5-design $E$ の block の総数は 3217056 であることから $F$ は少なくとも 3217056 個の weight 20 の codeword を含まなければならない. したがって $A_{20} = 3217056$ となり $d = 20$ が得られる. 以上より定理 1 が証明できた. □

定理 1 よりただちに次を得る.

**系 5.** もし, 長さ 96 の extremal doubly-even self-dual code が存在すれば minimum weight の codeword によって生成される.

長さ 96 の extremal doubly-even self-dual code の存在性を調べるために self-orthogonal 5-(96, 20, 816) design の性質を調べていきたい. ここではその幾つかを挙げる. 次の系は定理 1 よりただちに得られる.

**系 6.** 任意の self-orthogonal 5-(96, 20, 816) design の 2-rank は丁度 48 になる.

**命題 7.** 任意の self-orthogonal 5-(96, 20, 816) design の異なる block の共通部分の濃度 (block intersection number) は $0, 2, 4, 6, 8, 10$ となる.

**証明.** $D$ を任意の self-orthogonal 5-(96, 20, 816) design とする. $B$ を $D$ の任意の block とする. $B$ と $i$ point で交わる $B$ 以外の block の総数を $m_i$ と表す. 上で考えた通り code $F$ は minimum weight 20 なので $m_{12} = m_{14} = m_{16} = m_{18} = 0$ でなければならない. 5-design であることから

$$\sum_{i=0}^{5} \binom{2i}{j} m_{2i} = (\lambda_j - 1)\binom{20}{j} \quad (j = 0, 1, \ldots, 5)$$

を得る. この場合, 唯一つの解

$$m_0 = 32505, m_2 = 708300, m_4 = 1561845,$$
$$m_6 = 792900, m_8 = 116025, m_{10} = 5480$$

を持つことから命題を得る. □

## 3 最後に

以上で, 最初に挙げた問題が $m \leq 4$ の場合には正しいことが分かった. $m \geq 5$ において正しいのだろうか (著者は正しくあって欲しいという願望をもっているが). 証明の中で主に考えたことは連立方程式 (1) を用いることであったが, これは考えている design $E$ が 5-design である性質を十分反映させていると思う. 注意 4 で述べた通り, 長さ 72 までは, 連立方程式 (1) だけを考えれば十分であった ([9] を参照) が, 長さ 96 ではそれだけでは不十分であった. 最初に挙げた問題を一般的に考えるには, まだまだ何かが足りないように思えるので, 今後その辺りを考えて行きたい.

また, 上記問題を考えることは extremal doubly-even self-dual code の存在性を決定するのに有効なアプローチであって欲しいと願っているが,

今のところ, 全く分からない. 何とか長さ 72 の場合の存在性の決定への足掛かりを見つけたいと思っているが, 現在のところ, 簡単には行きそうにありません.

## 参考文献


[1] E.F. Assmus, Jr. and H.F. Mattson, Jr., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.

[2] M. Harada, Remark on a 5-design related to a putative extremal doubly-even self-dual [96, 48, 20] code, *Designs, Codes and Cryptogr.* (2005), to appear.

[3] M. Harada, M. Kitazume and A. Munemasa, On a 5-design related to an extremal doubly even self-dual code of length 72, *J. Combin. Theory Ser. 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, *Ann. Combin.* **9** (2005), 189–198.

[5] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[6] E. Rains and N.J.A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177–294.

[7] N.J.A. Sloane, Is there a (72, 36) $d = 16$ self-dual code? *IEEE Trans. Inform. Theory* **19** (1973), 251.

[8] V.D. Tonchev, A characterization of designs related to the Witt system $S(5, 8, 24)$, *Math. Z.* **191** (1986), 225–230.

[9] 原田昌晃, 北詰正顕, 宗政昭弘, 長さ 72 の extremal doubly-even self-dual code に関係した 5-design について, 第 21 回代数的組合せ論シンポジウム報告集 (2004), 88–94.

# Delsarte Clique Graphs

**S. Bang** *
Faculty of Mathematics, Graduate School, Kyushu University 6-10-1 Hakozaki, Higashiku, Fukuoka 812-8581 Japan e-mail: sjbang@math.kyushu-u.ac.jp
**A. Hiraki**†
Division of Mathematical Sciences, Osaka Kyoiku University Asahigaoka 4-698-1 Kashiwara, Osaka 582-8582 Japan e-mail: hiraki@cc.osaka-kyoiku.ac.jp
**J. H. Koolen** ‡
Department of Mathematics, Pohang University of Science and Technology Hyoja-dong, Namgu Pohang 790-784 Korea e-mail: jhk@com2mac.postech.ac.kr

September 28, 2005

**Abstract**

In this paper, we consider the class of Delsarte clique graphs, i.e. the class of distance-regular graphs with the property that each edge lies in a constant number of Delsarte cliques. There are many examples of Delsarte clique graphs such as the Hamming graphs, the Johnson graphs and the Grassmann graphs. Our main result is that, under mild conditions, for given $s \geq 2$ there are finitely many Delsarte clique graphs which contain Delsarte cliques with size $s+1$. Further we classify the Delsarte clique graphs with small $s$.

## 1 Introduction

Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D$. Let $\theta_0 > \theta_1 > \cdots > \theta_D$ be the eigenvalues of $\Gamma$. If $C$ is a clique of $\Gamma$ then $C$ has at most $(1 - \frac{k}{\theta_D})$ vertices ([1, Proposition 4.4.6]). A clique $C$ containing $(1 - \frac{k}{\theta_D})$ vertices is called a *Delsarte clique* of $\Gamma$. It is known that each Delsarte clique $C$ of $\Gamma$ is a maximal clique and a completely regular code in the sense of [1, p.345]. Moreover the parameters of a Delsarte clique, as a completely regular code, depend not on the particular Delsarte clique but only on the intersection numbers of $\Gamma$.

*Corresponding author. This work was supported by the Post-doctoral Fellowship Program of Korea Science and Engineering Foundation (KOSEF). She also thanks to faculty of Mathematics, Graduate School at Kyushu University for the warm hospitality.

†This work was supported by the Grant-in-Aid for Scientific Research, the Ministry of Education, Science and Culture, JAPAN

‡This work was done while Jack Koolen was at the Division of Applied Mathematics of KAIST, Teajon, South-Korea. He also acknowledge the partial support received from Com$^2$MaC-KOSEF, South-Korea.

In this paper, we consider the class of Delsarte clique graphs (see Definition 1.1). There are many examples of Delsarte clique graphs such as the Hamming graphs, the Johnson graphs and the Grassmann graphs.

**Definition 1.1** *Let $\Gamma$ be a non-complete distance-regular graph and $\mathcal{C}$ be a nonempty family of cliques of $\Gamma$.*
*(a) The pair $(\Gamma, \mathcal{C})$ is called a* Delsarte pair *with parameters $(k, s_C, n_C)$, where $k \geq 2, s_C \geq 1$ and $n_C \geq 1$ are integers, if $(\Gamma, \mathcal{C})$ satisfies the following properties:*

*(i) the valency of $\Gamma$ equals $k$;*

*(ii) $|C| = s_C + 1$ for all $C \in \mathcal{C}$;*

*(iii) $\Gamma$ has an eigenvalue $-\frac{k}{s_C}$;*

*(iv) Each edge $(x, y)$ of $\Gamma$ is contained in exactly $n_C$ cliques of $\mathcal{C}$.*

*Then $\mathcal{C}$ is called a* Delsarte set *of $\Gamma$ with parameters $(s_C, n_C)$. A Delsarte set $\mathcal{C}$ is called* full *if $\mathcal{C} = \{C \mid C$ is a clique of size $s_C + 1$ in $\Gamma\}$.*
*(b) A non-complete graph $\Gamma$ with valency $k$ is called a* Delsarte clique graph *with parameters $(k, s, n)$ if $\Gamma$ contains a full Delsarte set $\mathcal{C}$ with parameters $(s, n) = (s_C, n_C)$, where $k \geq 2, s_C \geq 1$ and $n_C \geq 1$ are integers.*

**Remark 1.2** *(i) Let $(\Gamma, \mathcal{C})$ be a Delsarte pair with parameters $(k, s_C, n_C)$. Then by [1, Proposition 4.4.6(i)], $-\frac{k}{s_C}$ is the smallest eigenvalue of $\Gamma$ and each clique of size $s_C + 1$ in $\Gamma$ is a Delsarte clique. Moreover any vertex of $\Gamma$ lies in exactly $\frac{kn_C}{s_C}$ Delsarte cliques of $\mathcal{C}$.*

*(ii) If $(\Gamma, \mathcal{C})$ and $(\Gamma, \mathcal{C}')$ are two Delsarte pairs with parameters $(k, s_C, n_C)$ and $(k, s_{C'}, n_{C'})$, respectively, then $s_C = s_{C'}$ must hold as $\theta_D = -\frac{k}{s_C} = -\frac{k}{s_{C'}}$. Hence in this paper, for any Delsarte pair $(\Gamma, \mathcal{C})$ on a given distance-regular graph $\Gamma$, denote $(k, s, n_C) := (k, s_C, n_C)$.*

*(iii) Let $(\Gamma, \mathcal{C})$ be a Delsarte pair and $\Gamma'$ be a distance-regular graph with the same intersection numbers as $\Gamma$. Then $\Gamma'$ does not have to contain a Delsarte set $\mathcal{C}'$. Examples for this case are Doob graphs ([1, §9.2]), the three Chang graphs ([1, §3.11]) and the recently found distance-regular graphs by Van Dam and Koolen ([4]).*

Note that a Delsarte pair $(\Gamma, \mathcal{C})$ with $s = 1$ is exactly the same as a pair of a bipartite distance-regular graph and the set of edges $\mathcal{C}$. We call a Delsarte set or a Delsarte pair *thick* if $s$ is at least 2. A graph $\Gamma$ is called *coconnected* if the complement of $\Gamma$ is connected. Note that distance-regular graphs which are not coconnected are exactly the complete multipartite graphs.

Our first main result is that for a thick Delsarte pair $(\Gamma, \mathcal{C})$ with parameters $(k, s, n_C)$, either $\Gamma$ is not coconnected or the valency $k$ of $\Gamma$ is bounded by a function of $s$ and the diameter $D$.

**Theorem 1.3** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a thick Delsarte set $C$ with parameters $(s, n_C)$. If $\Gamma$ is coconnected then*

$$k < s + s^{\frac{4D}{h}}$$

*holds where $h := |\{i \mid (c_i, a_i, b_i) = (c_1, a_1, b_1)\}|$.*

In the rest of the paper we will concentrate on a thick Delsarte pair $(\Gamma, C)$ such that $\Gamma$ is coconnected and has an induced subgraph $K_{2,1,1}$. Note that a distance-regular graph $\Gamma$ has no induced subgraph $K_{2,1,1}$ if and only if $\Gamma$ is of order $(s,t)$ with $s = a_1 + 1$ and $t = \frac{b_1}{s}$. We will show that for given $s \geq 2$ there are finitely many coconnected distance-regular graphs $\Gamma$ which have an induced subgraph $K_{2,1,1}$ and a family $C$ of Delsarte cliques of size $s+1$ such that $(\Gamma, C)$ is a Delsarte pair. We will show this by showing that the diameter and valency of $\Gamma$ is bounded above by $s$.

**Theorem 1.4** *Let $\Gamma$ be a non-complete coconnected distance-regular graph containing a Delsarte clique of size $s+1 \geq 3$ and an induced subgraph $K_{2,1,1}$. If $\Gamma$ contains a Delsarte set, then*

*(i)* $D \leq s$;

*(ii)* $k < \binom{s}{\lfloor \frac{s}{2} \rfloor}^4$.

*In particular, for fixed $s \geq 2$ there are finitely many coconnected distance-regular graphs $\Gamma$ which have an induced subgraph $K_{2,1,1}$ and contain a Delsarte set $C$ with parameters $(s, n_C)$.*

**Remark 1.5** *The diameter bound $D \leq s$ is tight. For instance, the Johnson graphs $J(2s, s)$ are Delsarte clique graphs with parameters $(s^2, s, 2)$ and diameter $D = s$.*

This paper is organized as follows. In Section 2, we set up the notation of distance-regular graphs. In Section 3, we introduce and calculate parameters for a Delsarte pair, and then prove Theorem 1.3. In Section 4, we use the notions of the third section to illustrate combinatorial properties for a distance-regular graph having a Delsarte set. We then prove Theorem 1.4. In Section 5, we classify distance-regular graphs containing a Delsarte set with $s = 2, 3$, respectively.

## 2 Preliminary

For background information about distance-regular graphs we refer the reader to [1]. Now, suppose that $\Gamma$ is a distance-regular graph with valency $k \geq 2$, diameter $D \geq 2$ and intersection array $\iota(\Gamma) := \{b_0, b_1, \ldots, b_{D-1}; c_1, c_2, \ldots, c_D\}$. Let $\theta_0 > \theta_1 > \cdots > \theta_D$ be the eigenvalues of $\Gamma$. The standard sequence $(u_i(\theta))_{0 \leq i \leq D}$ corresponding to an eigenvalue $\theta$ of $\Gamma$ is a sequence satisfying the following recurrence relation:

$$u_0(\theta) = 1, \; u_1(\theta) = \theta/k,$$

$$c_i u_{i-1}(\theta) + a_i u_i(\theta) + b_i u_{i+1}(\theta) = \theta u_i(\theta) \quad (1 \le i \le D).$$

Then the multiplicity of the eigenvalue is given by

$$m(\theta) = \frac{|V(\Gamma)|}{\sum_{i=0}^{D} k_i u_i^2(\theta)} \tag{1}$$

where $k_i := |\Gamma_i(x)|$ for a vertex $x \in V(\Gamma)$.

## 3 Delsarte pairs

In this section, we calculate the parameters for any Delsarte pair $(\Gamma, C)$, and then show Theorem 1.3 which states that valency $k$ is bounded in terms of the size of a clique in $C$ for a coconnected thick Delsarte pair $(\Gamma, C)$.

Let $\Gamma$ be a distance-regular graph of diameter $D \ge 2$. Let $C$ be a Delsarte clique of $\Gamma$, and define $C_i := \{x \in V(\Gamma) \mid d(x, C) = i\}$ for each $1 \le i \le \rho(C)$ where $\rho(C) := \max\{i \mid C_i \ne \emptyset\}$ and $C_0 = C$. Then by [5, §13.7], $\rho := \rho(C) = D - 1$ holds and there exist nonnegative integers $\gamma_i(C)$, $\alpha_i(C)$ and $\beta_i(C)$ $(i = 0, 1, \ldots, D-1)$ for the number of neighbors of $x \in C_i$ in $C_{i-1}$, $C_i$ and $C_{i+1}$, respectively, where $\beta_\rho(C) = \gamma_0(C) = 0$. For $0 \le i \le D-1$ and a vertex $x \in C_i$, define

$$\psi_i(x, C) := |\{y \in C \mid d(x, y) = i\}|.$$

By [5, §11.7], the numbers $\psi_i(x, C)$ $(0 \le i \le D-1)$ depend not on the pair $(x, C)$ but only on the distance $i = d(x, C)$. Hence let

$$\psi_i := \psi_i(x, C) \quad (0 \le i \le D-1).$$

By an easy induction argument, one can see that the numbers $\alpha_i(C), \beta_i(C), \gamma_i(C)$ are not depending on the particular Delsarte clique $C$ and hence we define $\alpha_i := \alpha_i(C), \beta_i := \beta_i(C), \gamma_i := \gamma_i(C)$.
If we say a graph $\Gamma$ has a Delsarte set with $\psi_1 = p$ for some positive integer $p$, then we mean that each Delsarte clique in $\Gamma$ has $\psi_1 = p$.
Now let $(\Gamma, C)$ be a Delsarte pair with parameters $(k, s, n_C)$. For $x, y \in V(\Gamma)$ with $d(x, y) = i$ $(1 \le i \le D)$ define $\tau_i(x, y; C)$ as the number of a clique $C$ in $\mathcal{C}$ containing $x$ with $d(y, C) = i - 1$.

**Lemma 3.1** *The number $\tau_i(x, y; C)$ $(1 \le i \le D)$ depends not on the specific pair $(x, y)$ but only on the distance $i = d(x, y)$ and $C$.*

*Proof:* Let $x, y \in V(\Gamma)$ with $d(x, y) = i$ $(1 \le i \le D)$. By counting the number of pairs $(z, C)$, where $z \in \Gamma_{i-1}(y) \cap \Gamma_1(x)$ and $C$ is a clique containing $x$ and $z$ in $\mathcal{C}$, in two ways, we find $c_i n_C = \psi_{i-1} \tau_i(x, y; C)$. It follows that

$$\tau_i(x, y; C) = \frac{c_i n_C}{\psi_{i-1}}, \tag{2}$$

and hence the number $\tau_i(x, y; C)$ depends not on the pair $(x, y)$ but only on the distance $d(x, y) = i$ and $n_C$. ∎

By previous lemma, we may put for $1 \leq i \leq D$,

$$\tau_i(C) := \tau_i(x, y; C)$$

where $(x, y)$ is any pair of vertices with $d(x, y) = i$ and $(\Gamma, C)$ is a Delsarte pair. Now we will derive a generalization of [6, Lemma 4] for distance-regular graphs which contain a Delsarte set.

**Proposition 3.2** *Let $\Gamma$ be a non-complete distance-regular graph with valency $k$ containing a Delsarte set $C$ with parameters $(s, n_C)$. Let $m$ be the multiplicity of the smallest eigenvalue $\frac{-k}{s}$ of $\Gamma$. Then the following hold for $\Gamma$:*
*(i)* $c_j = \frac{\tau_j(C)\psi_{j-1}}{n_C}$ $(1 \leq j \leq D)$ *and* $b_j = \left(\frac{k}{s} - \frac{\tau_j(C)}{n_C}\right)(s + 1 - \psi_j)$ $(1 \leq j \leq D-1)$.
*(ii) Let* $u_j := u_j\left(-\frac{k}{s}\right)$ *for* $0 \leq j \leq D$. *Then*

$$u_j = \frac{-\psi_{j-1}}{s + 1 - \psi_{j-1}} u_{j-1}. \tag{3}$$

*In particular*

$$u_j^2 \geq s^{-2j}. \tag{4}$$

*(iii)* $m \leq s^{2D}$. *Moreover the equality holds if and only if* $s = 1$.

*Proof:* (i) Let $x, y$ be two vertices at distance $j$. By counting the number of pairs $(z, C)$, where $z \in \Gamma_1(x) \cap \Gamma_{j+1}(y)$ and $C$ a clique containing $x$ and $z$ in $C$, in two ways, we obtain the equation

$$b_j n_C = (s + 1 - \psi_j)\left(\frac{k n_C}{s} - \tau_j(C)\right).$$

This implies the formula for $b_j$ and by (2) the formula for $c_j$ holds.
(ii) We prove Equation (3) by induction on $j$. As $u_0 = 1$, $u_1 = -\frac{1}{s}$ and $\psi_0 = 1$, the result holds for the case $j = 1$. Let $1 \leq j \leq D-1$ and assume that

$$(s + 1 - \psi_{j-1})u_j = -\psi_{j-1}u_{j-1}.$$

Then the following holds:

$$b_j u_{j+1} = \left(-\frac{k}{s} - a_j\right)u_j - c_j u_{j-1} = \left\{-\frac{k}{s} - a_j + \frac{c_j(s + 1 - \psi_{j-1})}{\psi_{j-1}}\right\}u_j = -\psi_j\left(\frac{k}{s} - \frac{\tau_j(C)}{n_C}\right)u_j.$$

Hence Equation (3) holds for $j + 1$ by (i). This shows that Equation (3) holds for all $1 \leq j \leq D$. Equation (4) follows immediately from (3).
(iii) This follows immediately from

$$m = \frac{|V(\Gamma)|}{\sum_{j=0}^{D} k_j u_j^2} \leq \frac{|V(\Gamma)|}{\left(\frac{1}{s}\right)^{2D} \sum_{j=0}^{D} k_j} = s^{2D}$$

and the inequality is attained if and only if $s = 1$. ∎

**Proof of Theorem 1.3:** If $\Gamma$ does not contain an induced subgraph $K_{2,1,1}$, then $\Gamma$ is a distance-regular graph of order $\left(s, \frac{k}{s} - 1\right)$ with the smallest eigenvalue $-\frac{k}{s}$ and $s > 1$. Hence by [6, Theorem 1] we obtain $\frac{k}{s} - 1 < s^{\frac{4D}{h} - 1}$ and the result follows in this case. So we may assume that $\Gamma$ has an induced subgraph $K_{2,1,1}$. Then $c_2 \geq 2$ and $h = 1$. Let $m$ be the multiplicity of an eigenvalue $-\frac{k}{s}$. Note that by [1, Proposition 4.4.8], $m > 2$ holds as $s \geq 2$ and $D \geq 2$. Since $\Gamma$ is coconnected, we have $k \leq \frac{1}{2}(m-1)(m+2)$ by [1, Theorem 5.3.2]. The theorem now follows in this case by Proposition 3.2 (iii). This completes the proof. ∎

## 4 Combinatorial Properties

**Lemma 4.1** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a Delsarte clique $C$ of size $s+1$. Then the following hold:*
*(i)*

$$s(a_1 - s + 1) = (k - s)(\psi_1 - 1).$$

*In particular, $\psi_1 = 1$ if and only if $C$ has size $a_1 + 2$.*
*(ii) $c_2 = \psi_1$ if and only if $c_2 = 1$.*
*(iii) If $c_2 > 1$ then $\Gamma$ contains quadrangles.*

*Proof:* (i) Let $x \in C$. This follows by counting the number of edges between $C \setminus \{x\}$ and $\Gamma_1(x) \setminus C$.
(ii) ($\Rightarrow$): We assume $c_2 = \psi_1$. Let $x \in C$ and $y \in \Gamma_1(x) \setminus C$. Define $U := \Gamma_1(y) \cap C$. We prove $(\Gamma_1(x) \cap \Gamma_1(y)) \cup \{x, y\}$ is a clique of size $a_1 + 2$. Suppose there exists $z \neq z' \in (\Gamma_1(x) \cap \Gamma_1(y))$ which are not adjacent. We may assume that $z \notin U$. Then $\Gamma_1(z) \cap C = U$, as otherwise there exists $w \in (\Gamma_1(z) \cap C) \setminus U$, and thus $\{z\} \cup U \subseteq \Gamma_1(w) \cap \Gamma_1(y)$, which contradicts to $c_2 = \psi_1$. This implies that $z' \notin U$ and $\Gamma_1(z) \cap C = U$, as before. Then $\{y\} \cup U \subseteq \Gamma_1(z) \cap \Gamma_1(z')$ which contradicts to $c_2 = \psi_1$. It follows that $(\Gamma_1(x) \cap \Gamma_1(y)) \cup \{x, y\}$ is a clique of size $a_1 + 2$, and hence it must be a Delsarte clique. This implies that $c_2 = \psi_1 = 1$ from (i).
($\Leftarrow$): If $c_2 = 1$ then $\psi_1 \leq 1$, hence $\psi_1 = 1$.
(iii) Let $x \in C$ and let $y \in C_1$ at distance 2 from $x$. By (ii) there exists a common neighbor $z$ of $x$ and $y$ which is not in $C$. As $z$ is adjacent to $x$ there exists a vertex $w$ in $C$ which is connected to $y$ but not to $z$. Now the induced subgraph on $\{x, w, y, z\}$ forms an induced quadrangle. ∎

**Lemma 4.2** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a Delsarte clique $C$ of size $s+1$. Then the following hold:*
*(i) Let $i$ and $j$ be positive integers such that $i + j \leq D - 1$. Then $\psi_i + \psi_j \leq s + 1$.*
*(ii) If $\psi_1 > \frac{s+1}{2}$ then $D = 2$.*
*(iii) Suppose $\psi_1 > 1$. Then for all $x \in C$ the local graph $\Delta(x)$ is connected and its second largest eigenvalue equals $s - \psi_1$. Moreover if $D = 2$ then $\Gamma$ has eigenvalues $k, s - \psi_1, -\frac{k}{s}$.*

*Proof:* (i) Let $x \neq y \in C$. Take $z \in \Gamma_i(x) \cap \Gamma_{i+1}(y)$ and $z' \in \Gamma_j(y) \cap \Gamma_{i+j+1}(z)$. Then $C \cap \Gamma_i(z)$ and $C \cap \Gamma_j(z')$ are disjoint. Hence we have

$$\psi_i + \psi_j = |C \cap \Gamma_i(z)| + |C \cap \Gamma_j(z')| \leq |C| = s + 1.$$

(ii) Assume $D \geq 3$. Then we have $2\psi_1 \leq s + 1$, by putting $i = j = 1$ in (i). This is a contradiction.
(iii) Let $\Delta(x)$ be the subgraph induced on $\Gamma_1(x)$. Then the partition $\{C \setminus \{x\}, \Delta(x) \setminus C\}$ of $\Delta(x)$ is equitable with the quotient matrix

$$Q = \begin{pmatrix} s-1 & a_1 - s + 1 \\ \psi_1 - 1 & a_1 - \psi_1 + 1 \end{pmatrix}.$$

As $Q$ has eigenvalues $a_1$ and $s - \psi_1$, it follows that $\Delta(x)$ has an eigenvalue $s - \psi_1$. Lemma 4.1 (i) implies that $sb_1 = s(k - 1 - a_1) = (k - s)(s - \psi_1 + 1)$. By [1, Theorem 4.4.3]

$$-1 - \frac{b_1}{\theta_D + 1} = -1 + \frac{sb_1}{k - s} = s - \psi_1$$

is an upper bound for the second largest eigenvalue of $\Delta(x)$. Since $a_1 \geq s-1 > s-\psi_1$, the second largest eigenvalue of $\Delta(x)$ equals $s-\psi_1$ and $\Delta(x)$ is connected.
Moreover if $D=2$, then the partition $\{C, V(\Gamma)\setminus C\}$ of $V(\Gamma)$ is equitable with quotient matrix

$$Q' = \begin{pmatrix} s & k-s \\ \psi_1 & k-\psi_1 \end{pmatrix},$$

and $Q'$ has eigenvalues $k$, $s-\psi_1$. This completes the proof. ∎

**Theorem 4.3** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a thick Delsarte set $C$ with parameters $(s, n_C)$. Then the following hold:*
*(i) $\psi_1 = 1$ holds if and only if $\Gamma$ is of order $(s, \frac{k}{s}-1)$ with the smallest eigenvalue $-\frac{k}{s}$.*
*(ii) If $\psi_1 \geq 2$ then for all $x \in V(\Gamma)$ the local graph $\Delta(x)$ is connected and its second largest eigenvalue equals $s-\psi_1$.*
*(iii) If $c_2 \geq 2$ then $\Gamma$ contains quadrangles and $\tau_2(C) \geq 2n_C$ holds. In particular $c_2 \geq 2\psi_1$ holds.*
*(iv) If $\psi_i + \psi_{D-i-1} = s+1$ holds for all $i = 0, 1, \ldots, D-1$, then $\Gamma$ is an antipodal cover. Moreover, if $D$ is odd then $\Gamma$ is an antipodal 2-cover.*

*Proof:* (i),(ii) These are follows from Lemma 4.1 (i) and Lemma 4.2 (iii).
(iii) As $\Gamma$ contains quadrangles from Lemma 4.1(iii), consider the induced quadrangle on $\{x, y, u, w\}$ with $d(x,y) = d(u,w) = 2$. Then $\tau_2(C) = \tau_2(x, y; C) \geq 2n_C$ holds by considering the Delsarte cliques of $C$ containing the edge $(x,u)$ and the Delsarte cliques of $C$ containing the edge $(x,w)$. From the equation $c_2 = \tau_2(C)\psi_1/n_C$, the result follows.
(iv) We find $u_D := u_D(\theta_D) = (-1)^D$ by Proposition 3.2 and our assumption. Then [1, Proposition 4.4.7] implies that $\Gamma$ must be antipodal as $\Gamma$ is not bipartite. Moreover if $D$ is odd then we have $u_D = -1$. Let $x$ and $y$ be vertices of $\Gamma$ at distance $D$. Then $(\bar{x}, \bar{y}) = u_D = -1$ and thus $\bar{x} = -\bar{y}$, where $\bar{}$ denote the standard representation corresponding to $\theta_D$. ( See [1, Propsotion 4.4.1]. ) If there exists $z \in \Gamma_D(x) \cap \Gamma_D(y)$ then $\bar{x} = -\bar{z} = \bar{y}$ which is a contradiction. Hence $\Gamma_D(x) \cap \Gamma_D(y) = \emptyset$ and $\Gamma$ must be an antipodal 2-cover. ∎

**Lemma 4.4** *Let $\Gamma$ be a distance-regular graph with diameter $D \geq 2$. Let $C$ and $C'$ be distinct Delsarte cliques in $\Gamma$ such that $C \cap C' \neq \emptyset$ hold. Then one of the following holds.*
*(i) $|C \cap C'| = \psi_1$.*
*(ii) $|C \cap C'| \leq \psi_i - \psi_{i-1}$ for all $i = 2, \ldots, D-1$.*

*Proof:* Let $s+1$ be the size of Delsarte cliques. Let $T := C \cap C'$ and $t := |T| > 0$. Since $C \neq C'$, there exists $x \in C' \setminus C$ and

$$1 \leq t = |T| \leq |C \cap \Gamma_1(x)| = \psi_1.$$

Suppose $t < \psi_1$ and we show that (ii) holds.
For each $i = 2, \ldots, D-1$, take $y \in \Gamma_{i-1}(x) \cap C_i$. Then $y \in C'_{i-1}$. Set $M := C \cap \Gamma_i(y)$ and $N := C \setminus M$. Then $|M| = \psi_i$, $|N| = s+1-\psi_i$ and $T \subseteq M$. Set $P := C' \cap \Gamma_{i-1}(y)$ and $Q := C' \setminus (P \cup T)$. Then $P \cap T = \emptyset$, $|P| = \psi_{i-1}$ and $|Q| = s+1-\psi_{i-1}-t$. Note that there are no edges between $N$ and $P$ as $N \subseteq \Gamma_{i+1}(y)$ and $P \subseteq \Gamma_{i-1}(y)$. By counting the number of edges between $N$ and $Q$ we have

$$|N|(\psi_1 - t) = \sum_{u \in N} |Q \cap \Gamma_1(u)| = \sum_{w \in Q} |N \cap \Gamma_1(w)| \leq |Q|(\psi_1 - t).$$

Since $t < \psi_1$, we have $s+1-\psi_i = |N| \leq |Q| = s+1-\psi_{i-1}-t$. This shows that (ii) holds. This completes the proof. ∎

**Theorem 4.5** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a thick Delsarte set $C$ with parameters $(s, n_C)$. Suppose $\psi_1 > 1$. Then*

$$1 < \psi_1 < \cdots < \psi_{D-1}.$$

*In particular, $D \leq s$.*

*Proof:* Suppose $\psi_{i-1} = \psi_i$ for some $2 \leq i \leq D-1$. Then Lemma 4.4 implies that any two intersecting Delsarte cliques have exactly $\psi_1$ common vertices. Let $C$ be a Delsarte clique in $\mathcal{C}$ and $x \in C_1$. Set $W := C \cap \Gamma_1(x)$. As $|W| = \psi_1 \geq 2$, there are two vertices $w \neq w' \in W$. Let $C^{(1)}, \ldots, C^{(n_C)}$ be the all Delsarte cliques in $\mathcal{C}$ containing the edge $(x, w)$. Since $|C \cap C^{(j)}| = \psi_1$ holds, $C \cap C^{(j)} = C \cap \Gamma_1(x)$ and thus $w, w' \in C \cap C^{(j)}$ for all $1 \leq j \leq n_C$. Thus there are $n_C+1$ Delsarte cliques $C^{(1)}, \ldots, C^{(n_C)}, C \in \mathcal{C}$ containing the edge $(w, w')$. This is a contradiction. Therefore $1 < \psi_1 < \cdots < \psi_{D-1}$. Moreover $j \leq \psi_{j-1}$ $(2 \leq j \leq D)$ holds by induction on $j$. Hence $D \leq \psi_{D-1} \leq s$ holds. This shows the theorem. ∎

**Proof of Theorem 1.4:** (i) This follows immediately from Theorems 4.3 and 4.5.
(ii) By Theorem 4.5, we have $\psi_i < \psi_{i+1}$. Let $u_j = u_j(-\frac{k}{s})$. By induction on $j$, it follows that for each $0 \leq j \leq D$ we have

$$|u_j| \geq \frac{1 \cdot 2 \cdots \lfloor \frac{s}{2} \rfloor}{s \cdot (s-1) \cdots (s+1-\lfloor \frac{s}{2} \rfloor)} = \binom{s}{\lfloor \frac{s}{2} \rfloor}^{-1}. \tag{5}$$

Let $m$ be the multiplicity of an eigenvalue $-\frac{k}{s}$ of $\Gamma$. As $s \geq 2$ and $D \geq 2$, $m > 2$ holds by [1, Proposition 4.4.8]. As $\Gamma$ is coconnected, we have $k \leq \frac{1}{2}(m-1)(m+2)$ by [1, Theorem 5.3.2]. Substituting Equation (5) in Biggs' Formula (1) for $m$ , the result follows. This completes the proof. ∎

# 5 Classifications

In this section we will classify distance-regular graphs containing a Delsarte set with $\psi_1 = s \geq 2$ and $\psi_1 = s-1 \geq 2$, respectively. As an application we will classify distance-regular graphs containing a Delsarte set with small $s$.

**Proposition 5.1** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a Delsarte clique $C$ with size $s+1 \geq 3$. Then $\psi_1 = s$ holds if and only if $\Gamma$ is a complete multipartite graph $K_{(s+1)\times\frac{k}{s}}$.*

*Proof:* Suppose $\psi_1 = s$. Then $D = 2$ holds from Lemma 4.2(ii) as $s \geq 2$. It follows, by Lemma 4.2(iii), that $\Gamma$ has eigenvalues $k, 0, -\frac{k}{s}$, and hence $\Gamma$ is a complete multipartite graph $K_{(s+1)\times\frac{k}{s}}$. Clearly if $\Gamma$ is complete multipartite, then $\psi_1 = s$. This shows the proposition. ∎

**Theorem 5.2** *Let $\Gamma$ be a non-complete distance-regular graph with valency $k$, containing a Delsarte clique of size $s+1$ with $\psi_1 = s-1 \geq 2$. Then $\Gamma$ contains a Delsarte set if and only if $\Gamma$ is one of the following graphs:*

*(i) the complement of the triangular graph $T(2\ell)$ for $\ell \geq 4$.*

*(ii) the complement of square grid $\ell \times \ell$ for $\ell \geq 4$.*

*(iii) the complement of the Shrikhande graph.*

*(iv) the Johnson graph $J(5,2)$.*

*(v) the Johnson graph $J(6,3)$.*

*(vi) the distance 2 graph of halved 6-cube.*

*(vii) the distance 2 graph of the Gosset graph.*

*Proof:* Suppose $\Gamma$ contain a Delsarte set. Let us first assume $D = 2$. By Lemma 4.2(iii), the second largest eigenvalue of $\Gamma$ is 1 as $\psi_1 = s-1$. Then the complement of $\Gamma$ is a strongly regular graph with the smallest eigenvalue $-2$. Hence $\Gamma$ is the complement of one of the graphs shown in [1, Theorem 3.12.4(i)]. It is easy to see that the complement of the Clebsch graph, i.e. the folded 5-cube, and the complements of the triangular graphs $T(2\ell+1)$ do not contain any Delsarte clique. The complement of square grid $3 \times 3$, the complement of the triangular graph $T(6)$ and the complement of the Schläfli graph are the generalized quadrangle $GQ(2,1), GQ(2,2)$ and $GQ(2,4)$, respectively, and hence $\psi_1 = 1$ in these cases, which do not satisfy our assumption. It can be checked that the complements of the three Chang graphs do not contain any Delsarte sets. And the complement of Petersen graph is the Johnson graph $J(5,2)$. Hence $\Gamma$ is one of the graphs (i)(ii)(iii) and (iv) in this case

Now let us assume $D \geq 3$. Lemma 4.2(ii) shows that $2 \leq s-1 \leq \frac{s+1}{2}$ holds and hence $s = 3$. Then $\Gamma$ is an antipodal 2-cover of diameter 3 and valency $k = 3(a_1 - 1)$, by Lemma 4.1 (i), Theorem 4.5. Hence $\Gamma$ is a Taylor graph with intersection array $\{3a_1 - 3, 2a_1 - 4, 1; 1, 2a_1 - 4, 3a_1 - 3\}$ and the distance 2 graph $\hat{\Gamma}$ of $\Gamma$ is also a Taylor graph with intersection array $\{3a_1 - 3, a_1, 1; 1, a_1, 3a_1 - 3\}$ ([1, p.431]). It follows from [1, Corollary 1.15.3] that $a_1 \in \{4, 6, 10\}$. Therefore $\hat{\Gamma}$ is the Johnson graph $J(6,3)$, the halved 6-cube and the Gosset graph for $a_1 = 4, 6$ and 10, respectively. Note that $\Gamma$ is also the distance 2 graph of $\hat{\Gamma}$ and the distance 2 graph of the Johnson graph $J(6,3)$ is itself. Hence $\Gamma$ is one of the graphs (v), (vi), (vii) in this case.

The theorem follows from the fact that the seven families of graphs all contain a Delsarte set. ∎

**Proposition 5.3** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a Delsarte set $C$ with parameters $(2, n_C)$. Then $\Gamma$ is either a graph of order $(2, \frac{k}{2}-1)$ with the smallest eigenvalue $-\frac{k}{2}$, or the complete multipartite graph $K_{3\times\frac{k}{2}}$.*

*Proof:* Note that $1 \leq \psi_1 \leq s = 2$. By Theorem 4.3(i) and Proposition 5.1 the result follows. ∎

**Theorem 5.4** *Let $\Gamma$ be a distance-regular graph with valency $k$ and diameter $D \geq 2$, containing a Delsarte set $C$ with parameters $(3, n_C)$. Then $\Gamma$ is one of the following graphs:*
*(i) distance-regular graphs of order $\left(3, \frac{k}{3} - 1\right)$ with the smallest eigenvalue $-\frac{k}{3}$.*
*(ii) the complete multipartite graph $K_{4\times\ell}$ for $\ell \geq 2$.*
*(iii) the complement of the triangular graph $T(8)$*
*(iv) the complement of square grid $4 \times 4$.*
*(v) the complement of the Shrikhande graph.*
*(vi) the Johnson graph $J(5,2)$.*
*(vii) the Johnson graph $J(6,3)$.*
*(viii) the distance 2 graph of halved 6-cube.*
*(ix) the distance 2 graph of the Gosset graph.*

*Proof:* Note that $1 \leq \psi_1 \leq s = 3$. Then by Theorem 4.3(i), Proposition 5.1 and Theorem 5.2 the result follows. ∎

## References


[1] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-Regular Graphs, *Springer-Verlag, Berlin,* 1989

[2] A. E. Brouwer and J. Hemmeter, A new family of distance-regular graphs and the $\{0,1,2\}$-cliques in dual polar graphs, *European J. Combin.* 13 (1992) no. 2, 71-79

[3] A. E. Brouwer, J. H. Koolen and R. J. Riebeek, A new distance-regular graph associated to the Mathieu group $M_{10}$, *J. Algebraic Combin.* 8 (1998) no. 2, 153-156

[4] E. van Dam and J. Koolen, A new family of distance-regular graphs with unbounded diameter, accepted by *Invent. Math.*

[5] C. D. Godsil, Algebraic Combinatorics, *Chapman and Hall, Inc.* 1993

[6] A. Hiraki and J. Koolen, A Higman-Haemers inequality for thick regular near polygons, *J. Algebraic Combin.* 20 (2004), 87-92

[7] J. H. Koolen, The distance-regular graphs with intersection number $a_1 \neq 0$ and with an eigenvalue $-1 - (b_1/2)$, *Combinatorica* 18 (1998), 227-234

[8] J. J. Seidel, Strongly regular graphs with $(-1,1,0)$ adjacency matrix having eigenvalue 3, *Lin. Alg. Appl.* 1 (1968) 281-298

# $STD_{\frac{k}{3}}[k;3]$'s

秋山献之 (福岡大 理学部)、末竹 千博 (大分大学 工学部)

## 1. 動機

最初に、講演のときに使った記号、用語を若干変更させていただいたことをお断りします。また、証明が間違っている命題もありました。お侘びいたします。

### 1.1 定義

$STD_\lambda[k;u]$ (symmetric transversal design) とは、次の4つの条件を満たす結合構造 $\mathcal{D}=(\mathcal{P},\mathcal{B})$ のことである。

(i) 各ブロックは、丁度 $k$ 個の点を含む。
(ii) $|(P,Q)|$ を、異なる2点 $P,Q\in\mathcal{P}$ を通るブロックの個数とすると、$|(P,Q)|=0,\ \lambda$ である。
(iii) $\mathcal{P}$ は、次の条件を満たす、等しいサイズ $u$ を持つ $k$ 個の部分集合 $\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$ に分割される。すなわち、$|(P,Q)|=0$ であるための必要十分条件は、$P$ と $Q$ がある同一の $\mathcal{P}_i$ に含まれることである。ここで、$\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$ は $\mathcal{D}$ の**point groups**と呼ばれる。
(iv) $\mathcal{D}$ の双対構造もまた、条件 (i),(ii),(iii) を満たす。この双対構造における point groops は、$\mathcal{D}$ の**block groups**と呼ばれる。

この定義において、$|\mathcal{P}|=|\mathcal{B}|=ku,\ k=\lambda u$ であることが、簡単に示される。

- $\Pi$ を $(P,l)-$elations(点 $P$ と直線 $l$ は固定) からなる自己同型群 $G$ を持つ位数 $k$ の射影平面とすると、$STD_{|G|}[k;\frac{k}{|G|}]$ が存在する。

- 位数12の射影平面 $\Pi$ が存在したとすると、$\Pi$ の自己同型群の位数は9の約数かまたは8の約数である。もし、位数2の自己同型を持つ位数12の射影平面が存在したとすると $STD_2[12;6]$ が存在する。もちろん、$STD_2[12;6]$ の存在は知られていない。

- $STD_1[k;k]$ は位数 $k$ の射影平面の部分構造であり、任意の $STD_1[k;k]$ $\mathcal{D}$ を部分構造として持つ位数 $k$ の射影平面が唯一つ存在する。

- $STD_{\frac{k}{2}}[k;2]$ の存在は位数 $k$ のアダマール行列の存在と同値である。

• 位数$k$のアダマール行列に一番「近い」$STD$は$STD_{\frac{k}{3}}[k;3]$である。それ故、我々は$STD_{\frac{k}{3}}[k;3]$に興味を持った。

## 2. $GL-$正則$STD$

### 2.1 定義

$\mathcal{D}=(\mathcal{P},\mathcal{B})$を$STD_{\frac{k}{u}}[k;u]$とする。$\Omega=\{\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}\}$を$\mathcal{D}$のpoint groupsからなる集合で、$\Delta=\{\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}\}$を$\mathcal{D}$のblock groupsからなる集合とする。$K$を$\mathcal{D}$の自己同型群で、$\Omega$と$\Delta$の両方の上に正則に作用するものとする。このとき、$\mathcal{D}$を$K$に関して$GL-$正則$STD_{\frac{k}{u}}[k;u]$と呼ぶ。この場合、$K$の位数は$k$となる。

D. Jungnikelによって定義された正則STDの定義は次のようなものであった。

### 2.2 定義

$\mathcal{D}=(\mathcal{P},\mathcal{B})$を$STD_{\frac{k}{u}}[k;u]$とする。$\Omega=\{\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}\}$を$\mathcal{D}$のpoint groupsからなる集合で、$\Delta=\{\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}\}$を$\mathcal{D}$のblock groupsからなる集合とする。$U$を$\mathcal{D}$の自己同型群とし、$U$は各$\mathcal{P}_i$と$\mathcal{B}_j$を、それぞれ集合として固定し、各$\mathcal{P}_i$上と各$\mathcal{B}_j$上に正則に作用するとする。このとき、$\mathcal{D}$を$U-$正則という。この場合、$U$の位数は$u$となる。

定義2.2は、generalized Hadamard matrix $GH(k;U)$同値な概念である。次の予想は、講演のときに簡単に証明できると申しましたが、誤りでした。

### 2.3 予想(平峰[2])

$\mathcal{D}=(\mathcal{P},\mathcal{B})$を$STD_{\frac{k}{u}}[k;u]$とする。$\Omega=\{\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}\}$を$\mathcal{D}$のpoint groupsからなる集合で、$\Delta=\{\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}\}$を$\mathcal{D}$のblock groupsからなる集合とする。$K$と$U$を$\mathcal{D}$の2つの自己同型群で、$\mathcal{D}$が$K$に関して$GL-$正則で、かつ$U-$正則とする。このとき、
$[K,U]=1$で、$KU$は$\mathcal{P}$と$\mathcal{B}$両方の上で正則に作用する。

この予想に関して最近次が証明された。

### 2.4 定理(平峰[2])

$\mathcal{D}=(\mathcal{P},\mathcal{B})$を$STD_{\frac{k}{u}}[k;u]$とする。$\Omega=\{\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}\}$を$\mathcal{D}$のpoint groupsからなる集合で、$\Delta=\{\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}\}$を$\mathcal{D}$のblock groupsからなる集合とする。$K$と$U$を$\mathcal{D}$の2つの自己同型群で、$\mathcal{D}$が$K$に関して$GL-$

正則で、かつ$U-$正則とする。このとき、
$K$は$U$を正規化し、$KU$は$\mathcal{P}$と$\mathcal{B}$両方の上で正則に作用する。

定義 2.1 が妥当であることを示すため、一つの例をあげる。

**2.5 例**
$q$を素数べきとする。$F=GF(q)$とする。$PG(2,q)$から点$<(0,0,1)>$を通る直線全体と$<(0,0,1),(0,1,0)>$上の点全体を除いて出来る$PG(2,F)$の部分構造を$\mathcal{S}=(\mathcal{P},\mathcal{B})$とすると、$\mathcal{S}$は$STD_1[q;q]$である。この場合、$\mathcal{P}_a=\{<(1,a,x)|x\in F>\}$ $(a\in F)$はpoint groupsで、$\mathcal{B}_a=\{l|l$は$(0,1,a)$を通る直線、$l\neq<(0,0,1),(0,1,0)>\}$ $(a\in F)$はblock groupsになる。
このとき
(i) $q$が奇素数べきならば、
$U=\{\begin{pmatrix}1&2x&x^2\\0&1&x\\0&0&1\end{pmatrix}|x\in F\}$, $K=\{\begin{pmatrix}1&0&x\\0&1&0\\0&0&1\end{pmatrix}|x\in F\}$, とおくと、
$[U,K]=1$で$UK$は$\mathcal{P}$と$\mathcal{L}$上に正則に作用する。更に、$U$は$\{\mathcal{P}_a|a\in F\}$と$\{\mathcal{B}_a|a\in F\}$上に正則に作用する。

(ii) $q$が2べきであるとき、
$\{\begin{pmatrix}1&x&y\\0&1&x\\0&0&1\end{pmatrix}|x,y\in F\}$ は$\mathcal{P}$と$\mathcal{L}$上に正則に作用する。

## 3. $GL-$正則$STD_{\frac{k}{3}}[k;3]$

この節では、$k\leq 39$に対して$STD_{\frac{k}{3}}[k;3]$を扱う。CREハンドブックによると、$k<39$に対しては$STD_{\frac{k}{3}}[k;3]$の存在非存在は知られている。そして、分類は$k\leq 15$でなされている。我々は$GL-$正則$STD_{\frac{k}{3}}[k;3]$を調べて、$STD_{\frac{k}{3}}[k;3]$の無限系列を構成するヒントとしたい。しかしながら、現時点では成功していない。得られている結果を表でまとめると、次のようになる。

| $k$ | $STD_{\frac{k}{3}}[k;3]$ の個数 | $GH$ の個数 | $GL-$ 正則群の存在 | 備考 |
|---|---|---|---|---|
| 3 | 1個 | 1個 | 1種類 | |
| 6 | 1個 | 1個 | 非存在 | |
| 9 | 4個 | 2個 | 存在 | [4] |
| 12 | 1個 | 1個 | 3種類存在 | [6] |
| 15 | 非存在 | 非存在 | 非存在 | [1] |
| 18 | $\geq 1$ | $\geq 1$ | 非存在 | |
| 21 | $\geq 1$ | $\geq 1$ | 存在 | [5] |
| 24 | $\geq 1$ | $\geq 1$ | ? | |
| 27 | $\geq 1$ | $\geq 1$ | 存在 | [3] |
| 30 | $\geq 1$ | $\geq 1$ | ? | |
| 33 | ? | 非存在 | ? | |
| 36 | $\geq 1$ | $\geq 1$ | ? | |
| 39 | ? | ? | ? | |

$\mathcal{D} = (\mathcal{P}, \mathcal{B})$ を $STD_{\frac{k}{3}}[k;3]$ とする。
$\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{k-1}$ を $\mathcal{D}$ のpoint groups とする。
$\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{k-1}$ を $\mathcal{D}$ のblock groups とする。
$\Omega = \{\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{k-1}\}$, $\Delta = \{\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{k-1}\}$ とおく。
$K \leq \mathrm{Aut}\mathcal{D}$ とする。$\mathcal{D}$ が $K$ に関して $GL-$ 正則とする。
$\mathcal{P} = \{P_0, P_1, \cdots, P_{3k-1}\}$,
$\mathcal{P}_0 = \{P_0, P_1, P_2\}$, $\mathcal{P}_1 = \{P_3, P_4, P_5\}, \cdots, \mathcal{P}_{k-1} = \{P_{3k-3}, P_{3k-2}, P_{3k-1}\}$
$\mathcal{B} = \{B_0, B_1, \cdots, B_{3k-1}\}$,
$\mathcal{B}_0 = \{B_0, B_1, B_2\}$, $\mathcal{B}_1 = \{B_3, B_4, B_5\}, \cdots, \mathcal{B}_{k-1} = \{B_{3k-3}, B_{3k-2}, B_{3k-1}\}$ とする。

$L = (l_{ij})_{0 \leq i,j \leq 3k-1}$ を $\mathcal{D}$ を上記の点とブロックの番号付けに対する $\mathcal{D}$ の結合行列とする。

$$L = \begin{pmatrix} L_{0\,0} & L_{0\,1} & \cdots & L_{0\,k-1} \\ L_{1\,0} & L_{1\,1} & \cdots & L_{1\,k-1} \\ \vdots & \vdots & & \vdots \\ L_{k-1\,0} & L_{k-1\,1} & \cdots & L_{k-1\,k-1} \end{pmatrix}$$

とかける。
ここで、各 $L_i$ $(0 \leq i,j \leq k-1)$ は3次の置換行列である。

次が成り立つ。

• $I$ を3次の単位行列、$J$ を $3\times 3$ 全1行列とする。このとき、

$$(*)\quad LL^t=\begin{pmatrix} kI & \frac{k}{3}J & \cdots & \frac{k}{3}J & \frac{k}{3}J \\ \frac{k}{3}J & kI & \cdots & \frac{k}{3}J & \frac{k}{3}J \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ \frac{k}{3}J & \frac{k}{3}J & \cdots & \frac{k}{3}J & kI \end{pmatrix}$$

である。

• $LL^t=L^tL$

3次の置換行列を次のように、数0,1,2,3,4,5と対応させる。(計算機で計算するため。)

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\longleftrightarrow 0,\quad \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\longleftrightarrow 1,\quad \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\longleftrightarrow 2,$$

$$\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}\longleftrightarrow 3,\quad \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}\longleftrightarrow 4,\quad \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\longleftrightarrow 5$$

従って、$L$ は $\{0,1,2,3,4,5\}$ 上の $k$ 次の正方行列になる。

次の補題は以下の節の考察で有用である。

### 3.1 補題

$\sigma=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$, $\tau=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$, $\delta=\begin{pmatrix}1&1&1\\1&1&1\\1&1&1\end{pmatrix}$ とする。

$k_0,k_1,k_2,l_0,l_1,l_2,l\in Z$ で $k_0+k_1\sigma+k_2\sigma^2+l_0\tau+l_1\sigma\tau+l_2\sigma^2\tau=l\delta$ とする。
このとき、$k_0=k_1=k_2,\ l_0=l_1=l_2$ である。

以下、
$GL-$正則$STD_6[18;3]$が非存在であることと、$GL-$正則$STD_7[21;3]$の構成(この$STD$は点とblock上に正則に作用する自己同型群を持つ。)について述べる。

$\mathcal{D}=(\mathcal{P},\mathcal{B})$ を $STD_6[18;3]$ とする。
$L_j=L_{0\,j}$ $(0\le j\le 8)$ とおく。
同型を無視して、$K$ の可能性は5通り。
(I) $K=<\varphi|\varphi^{18}=1>$ のとき
$\varphi$ の $\mathcal{P}$ 上の作用を
$\varphi=(P_0,P_3,P_6,\cdots,P_{48},P_{51})(P_1,P_4,P_7,\cdots,P_{49},P_{52})(P_2,P_5,P_8,\cdots,P_{50},P_{53})$
$\varphi$ の $\mathcal{B}$ 上の作用を
$\varphi=(B_0,B_3,B_6,\cdots,B_{48},B_{51})(B_1,B_4,B_7,\cdots,B_{49},B_{52})(B_2,B_5,B_8,\cdots,B_{50},B_{53})$ とする。

$$L=\begin{pmatrix}
L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17}\\
L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16}\\
L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15}\\
L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14}\\
L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13}\\
L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12}\\
L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11}\\
L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10}\\
L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9\\
L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8\\
L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7\\
L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6\\
L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5\\
L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4\\
L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3\\
L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2\\
L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1\\
L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0
\end{pmatrix}$$

(II) $K=<\varphi,\ \tau|\varphi^6=1,\ \tau^3=1,\ \varphi^\tau=\varphi>$ のとき
$\varphi$ の $\mathcal{P}$ 上の作用を
$\varphi=(P_0,P_3,P_6,P_9,P_{12},P_{15})\ (P_1,P_4,P_7,P_{10},P_{13},P_{16})\ (P_2,P_5,P_8,P_{11},P_{14},P_{17})$
$(P_{18},P_{21},P_{24},P_{27},P_{30},P_{33})\ (P_{19},P_{22},P_{25},P_{28},P_{31},P_{34})\ (P_{20},P_{23},P_{26},P_{29},P_{32},P_{35})$
$(P_{36},P_{39},P_{42},P_{45},P_{48},P_{51})\ (P_{37},P_{40},P_{43},P_{46},P_{49},P_{52})\ (P_{38},P_{41},P_{44},P_{47},P_{50},P_{53})$
$\varphi$ の $\mathcal{B}$ 上の作用を
$\varphi=(B_0,B_3,B_6,B_9,B_{12},B_{15})\ (B_1,B_4,B_7,B_{10},B_{13},B_{16})\ (B_2,B_5,B_8,B_{11},B_{14},B_{17})$
$(B_{18},B_{21},B_{24},B_{27},B_{30},B_{33})\ (B_{19},B_{22},B_{25},B_{28},B_{31},B_{34})\ (B_{20},B_{23},B_{26},B_{29},B_{32},B_{35})$
$(B_{36},B_{39},B_{42},B_{45},B_{48},B_{51})\ (B_{37},B_{40},B_{43},B_{46},B_{49},B_{52})\ (B_{38},B_{41},B_{44},B_{47},B_{50},B_{53})$ とする。
$\tau$ の $\mathcal{P}$ 上の作用を $\tau=(P_0,P_{18},P_{36})(P_1,P_{19},P_{37})(P_2,P_{20},P_{38})\cdots$ とし、
$\tau$ の $\mathcal{B}$ 上の作用を $\tau=(B_0,B_{18},B_{36})(B_1,B_{19},B_{37})(B_2,B_{20},B_{38})\cdots$ とする。

$\tau=(P_0,P_{18},P_{36})(P_1,P_{19},P_{37})(P_2,P_{20},P_{38})$
$(P_3,P_{21},P_{39})(P_4,P_{22},P_{40})(P_5,P_{23},P_{41})$
$(P_6,P_{24},P_{42})(P_7,P_{25},P_{43})(P_8,P_{26},P_{44})$
$(P_9,P_{27},P_{45})(P_{10},P_{28},P_{46})(P_{11},P_{29},P_{47})$
$(P_{12},P_{30},P_{48})(P_{13},P_{31},P_{49})(P_{14},P_{32},P_{50})$
$(P_{15},P_{33},P_{51})(P_{16},P_{34},P_{52})(P_{17},P_{35},P_{53})$

$\tau=(B_0,B_{18},B_{36})(B_1,B_{19},B_{37})(B_2,B_{20},B_{38})$
$(B_3,B_{21},B_{39})(B_4,B_{22},B_{40})(B_5,B_{23},B_{41})$
$(B_6,B_{24},B_{42})(B_7,B_{25},B_{43})(B_8,B_{26},B_{44})$
$(B_9,B_{27},B_{45})(B_{10},B_{28},B_{46})(B_{11},B_{29},B_{47})$
$(B_{12},B_{30},B_{48})(B_{13},B_{31},B_{49})(B_{14},B_{32},B_{50})$
$(B_{15},B_{33},B_{51})(B_{16},B_{34},B_{52})(B_{17},B_{35},B_{53})$

$$L=\left(\begin{array}{cccccc|cccccc|cccccc}
L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17}\\
L_5 & L_0 & L_1 & L_2 & L_3 & L_4 & L_{11} & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{17} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16}\\
L_4 & L_5 & L_0 & L_1 & L_2 & L_3 & L_{10} & L_{11} & L_6 & L_7 & L_8 & L_9 & L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_{15}\\
L_3 & L_4 & L_5 & L_0 & L_1 & L_2 & L_9 & L_{10} & L_{11} & L_6 & L_7 & L_8 & L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_{14}\\
L_2 & L_3 & L_4 & L_5 & L_0 & L_1 & L_8 & L_9 & L_{10} & L_{11} & L_6 & L_7 & L_{14} & L_{15} & L_{16} & L_{17} & L_{12} & L_{13}\\
L_1 & L_2 & L_3 & L_4 & L_5 & L_0 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_6 & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_{12}\\
\hline
L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11}\\
L_{17} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_5 & L_0 & L_1 & L_2 & L_3 & L_4 & L_{11} & L_6 & L_7 & L_8 & L_9 & L_{10}\\
L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_{15} & L_4 & L_5 & L_0 & L_1 & L_2 & L_3 & L_{10} & L_{11} & L_6 & L_7 & L_8 & L_9\\
L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_3 & L_4 & L_5 & L_0 & L_1 & L_2 & L_9 & L_{10} & L_{11} & L_6 & L_7 & L_8\\
L_{14} & L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_2 & L_3 & L_4 & L_5 & L_0 & L_1 & L_8 & L_9 & L_{10} & L_{11} & L_6 & L_7\\
L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_{12} & L_1 & L_2 & L_3 & L_4 & L_5 & L_0 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_6\\
\hline
L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_0 & L_1 & L_2 & L_3 & L_4 & L_5\\
L_{11} & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{17} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_5 & L_0 & L_1 & L_2 & L_3 & L_4\\
L_{10} & L_{11} & L_6 & L_7 & L_8 & L_9 & L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_{15} & L_4 & L_5 & L_0 & L_1 & L_2 & L_3\\
L_9 & L_{10} & L_{11} & L_6 & L_7 & L_8 & L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_3 & L_4 & L_5 & L_0 & L_1 & L_2\\
L_8 & L_9 & L_{10} & L_{11} & L_6 & L_7 & L_{14} & L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_2 & L_3 & L_4 & L_5 & L_0 & L_1\\
L_7 & L_8 & L_9 & L_{10} & L_{11} & L_6 & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_{12} & L_1 & L_2 & L_3 & L_4 & L_5 & L_0
\end{array}\right)$$

(iii) $K=<\varphi,\ \tau|\varphi^9=1,\ \tau^2=1,\ \varphi^\tau=\varphi^{-1}>$ のとき
上の(i),(ii)と同様な議論をすると $\mathcal{D}$ の結合行列 $L$ は次のような形をしていることがわかる。

$$L=\left(\begin{array}{ccccccccc|ccccccccc}
L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} \\
L_8 & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_{17} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} \\
L_7 & L_8 & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_{16} & L_{17} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} \\
L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} \\
L_5 & L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_3 & L_4 & L_{14} & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} \\
L_4 & L_5 & L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_3 & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} & L_{12} \\
L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} \\
L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_0 & L_1 & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_9 & L_{10} \\
L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_0 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_9 \\
\hline
L_9 & L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_0 & L_8 & L_7 & L_6 & L_5 & L_4 & L_3 & L_2 & L_1 \\
L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_{11} & L_1 & L_0 & L_8 & L_7 & L_6 & L_5 & L_4 & L_3 & L_2 \\
L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_2 & L_1 & L_0 & L_8 & L_7 & L_6 & L_5 & L_4 & L_3 \\
L_{12} & L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_3 & L_2 & L_1 & L_0 & L_8 & L_7 & L_6 & L_5 & L_4 \\
L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_{14} & L_4 & L_3 & L_2 & L_1 & L_0 & L_8 & L_7 & L_6 & L_5 \\
L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_5 & L_4 & L_3 & L_2 & L_1 & L_0 & L_8 & L_7 & L_6 \\
L_{15} & L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_6 & L_5 & L_4 & L_3 & L_2 & L_1 & L_0 & L_8 & L_7 \\
L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_{17} & L_7 & L_6 & L_5 & L_4 & L_3 & L_2 & L_1 & L_0 & L_8 \\
L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_8 & L_7 & L_6 & L_5 & L_4 & L_3 & L_2 & L_1 & L_0
\end{array}\right)$$

(iv) $K=<\varphi,\ \tau,\ \mu|\varphi^3=1,\ \tau^3=1,\ \mu^2=1,\ \varphi^\tau=\varphi,\ \varphi^\mu=\varphi,\ \tau^\mu=\tau^{-1}>$ のとき
$\mathcal{D}$ の結合行列 $L$ は次のような形をしていることがわかる。

$$L=\left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc}
L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} \\
L_2 & L_0 & L_1 & L_5 & L_3 & L_4 & L_8 & L_6 & L_7 & L_{11} & L_9 & L_{10} & L_{14} & L_{12} & L_{13} & L_{17} & L_{15} & L_{16} \\
L_1 & L_2 & L_0 & L_4 & L_5 & L_3 & L_7 & L_8 & L_6 & L_{10} & L_{11} & L_9 & L_{13} & L_{14} & L_{12} & L_{16} & L_{17} & L_{15} \\
\hline
L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} \\
L_8 & L_6 & L_7 & L_2 & L_0 & L_1 & L_5 & L_3 & L_4 & L_{17} & L_{15} & L_{16} & L_{11} & L_9 & L_{10} & L_{14} & L_{12} & L_{13} \\
L_7 & L_8 & L_6 & L_1 & L_2 & L_0 & L_4 & L_5 & L_3 & L_{16} & L_{17} & L_{15} & L_{10} & L_{11} & L_9 & L_{13} & L_{14} & L_{12} \\
\hline
L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} \\
L_5 & L_3 & L_4 & L_8 & L_6 & L_7 & L_2 & L_0 & L_1 & L_{14} & L_{12} & L_{13} & L_{17} & L_{15} & L_{16} & L_{11} & L_9 & L_{10} \\
L_4 & L_5 & L_3 & L_7 & L_8 & L_6 & L_1 & L_2 & L_0 & L_{13} & L_{14} & L_{12} & L_{16} & L_{17} & L_{15} & L_{10} & L_{11} & L_9 \\
\hline
L_9 & L_{10} & L_{11} & L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_0 & L_1 & L_2 & L_6 & L_7 & L_8 & L_3 & L_4 & L_5 \\
L_{11} & L_9 & L_{10} & L_{17} & L_{15} & L_{16} & L_{14} & L_{12} & L_{13} & L_2 & L_0 & L_1 & L_8 & L_6 & L_7 & L_5 & L_3 & L_4 \\
L_{10} & L_{11} & L_9 & L_{16} & L_{17} & L_{15} & L_{13} & L_{14} & L_{12} & L_1 & L_2 & L_0 & L_7 & L_8 & L_6 & L_4 & L_5 & L_3 \\
\hline
L_{12} & L_{13} & L_{14} & L_9 & L_{10} & L_{11} & L_{15} & L_{16} & L_{17} & L_3 & L_4 & L_5 & L_0 & L_1 & L_2 & L_6 & L_7 & L_8 \\
L_{14} & L_{12} & L_{13} & L_{11} & L_9 & L_{10} & L_{17} & L_{15} & L_{16} & L_5 & L_3 & L_4 & L_2 & L_0 & L_1 & L_8 & L_6 & L_7 \\
L_{13} & L_{14} & L_{12} & L_{10} & L_{11} & L_9 & L_{16} & L_{17} & L_{15} & L_4 & L_5 & L_3 & L_1 & L_2 & L_0 & L_7 & L_8 & L_6 \\
\hline
L_{15} & L_{16} & L_{17} & L_{12} & L_{13} & L_{14} & L_9 & L_{10} & L_{11} & L_6 & L_7 & L_8 & L_3 & L_4 & L_5 & L_0 & L_1 & L_2 \\
L_{17} & L_{15} & L_{16} & L_{14} & L_{12} & L_{13} & L_{11} & L_9 & L_{10} & L_8 & L_6 & L_7 & L_5 & L_3 & L_4 & L_2 & L_0 & L_1 \\
L_{16} & L_{17} & L_{15} & L_{13} & L_{14} & L_{12} & L_{10} & L_{11} & L_9 & L_7 & L_8 & L_6 & L_4 & L_5 & L_3 & L_1 & L_2 & L_0
\end{array}\right)$$

(v) $K=<\varphi,\ \tau,\ \mu|\varphi^3=1,\ \tau^3=1,\ \mu^2=1,\ \varphi^\tau=\varphi,\ \varphi^\mu=\varphi^{-1},\ \tau^\mu=\tau^{-1}>$ のとき
$\mathcal{D}$ の結合行列 $L$ は次のような形をしていることがわかる。

$$L=\left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc}
L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} \\
L_2 & L_0 & L_1 & L_5 & L_3 & L_4 & L_8 & L_6 & L_7 & L_{11} & L_9 & L_{10} & L_{14} & L_{12} & L_{13} & L_{17} & L_{15} & L_{16} \\
L_1 & L_2 & L_0 & L_4 & L_5 & L_3 & L_7 & L_8 & L_6 & L_{10} & L_{11} & L_9 & L_{13} & L_{14} & L_{12} & L_{16} & L_{17} & L_{15} \\
\hline
L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_{14} \\
L_8 & L_6 & L_7 & L_2 & L_0 & L_1 & L_5 & L_3 & L_4 & L_{17} & L_{15} & L_{16} & L_{11} & L_9 & L_{10} & L_{14} & L_{12} & L_{13} \\
L_7 & L_8 & L_6 & L_1 & L_2 & L_0 & L_4 & L_5 & L_3 & L_{16} & L_{17} & L_{15} & L_{10} & L_{11} & L_9 & L_{13} & L_{14} & L_{12} \\
\hline
L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_0 & L_1 & L_2 & L_{12} & L_{13} & L_{14} & L_{15} & L_{16} & L_{17} & L_9 & L_{10} & L_{11} \\
L_5 & L_3 & L_4 & L_8 & L_6 & L_7 & L_2 & L_0 & L_1 & L_{14} & L_{12} & L_{13} & L_{17} & L_{15} & L_{16} & L_{11} & L_9 & L_{10} \\
L_4 & L_5 & L_3 & L_7 & L_8 & L_6 & L_1 & L_2 & L_0 & L_{13} & L_{14} & L_{12} & L_{16} & L_{17} & L_{15} & L_{10} & L_{11} & L_9 \\
\hline
L_9 & L_{11} & L_{10} & L_{15} & L_{17} & L_{16} & L_{12} & L_{14} & L_{13} & L_0 & L_2 & L_1 & L_6 & L_8 & L_7 & L_3 & L_5 & L_4 \\
L_{10} & L_9 & L_{11} & L_{16} & L_{15} & L_{17} & L_{13} & L_{12} & L_{14} & L_1 & L_0 & L_2 & L_7 & L_6 & L_8 & L_4 & L_3 & L_6 \\
L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_2 & L_1 & L_0 & L_8 & L_7 & L_6 & L_5 & L_4 & L_3 \\
\hline
L_{12} & L_{14} & L_{13} & L_9 & L_{11} & L_{10} & L_{15} & L_{17} & L_{16} & L_3 & L_5 & L_4 & L_0 & L_2 & L_1 & L_6 & L_8 & L_7 \\
L_{13} & L_{12} & L_{14} & L_{10} & L_9 & L_{11} & L_{16} & L_{15} & L_{17} & L_4 & L_3 & L_5 & L_1 & L_0 & L_2 & L_7 & L_6 & L_8 \\
L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_{17} & L_{16} & L_{15} & L_5 & L_4 & L_3 & L_2 & L_1 & L_0 & L_8 & L_7 & L_6 \\
\hline
L_{15} & L_{17} & L_{16} & L_{12} & L_{14} & L_{13} & L_9 & L_{11} & L_{10} & L_6 & L_8 & L_7 & L_3 & L_5 & L_4 & L_0 & L_2 & L_1 \\
L_{16} & L_{15} & L_{17} & L_{13} & L_{12} & L_{14} & L_{10} & L_9 & L_{11} & L_7 & L_6 & L_8 & L_4 & L_3 & L_5 & L_1 & L_0 & L_2 \\
L_{17} & L_{16} & L_{15} & L_{14} & L_{13} & L_{12} & L_{11} & L_{10} & L_9 & L_8 & L_7 & L_6 & L_5 & L_4 & L_3 & L_2 & L_1 & L_0
\end{array}\right)$$

コンピュータを使って (i) から (v) はすべて非存在であることがわかる。

次に $\mathcal{D}=(\mathcal{P},\mathcal{B})$ を $STD_7[21;3]$ とする。$L_j=L_{0\,j}$ $(0\leq j\leq 20)$ とおく。
$K\leq \mathrm{Aut}\mathcal{D}$ とし、2.1を仮定する。同型を無視して、$K$ の可能性は2通り。
(i) $K$ が位数21の巡回群のとき
まだ、調べていません。予想は非存在です。
(ii) $K=<\varphi,\ \tau|\tau^{-1}\varphi\tau=\varphi^2,\varphi^7=1,\ \tau^3=1>$ のとき
$\varphi$ の $\mathcal{P}$ 上の作用を
$\varphi=(P_0,P_3,P_6,P_9,P_{12},P_{15},P_{18})$
$(P_1,P_4,P_7,P_{10},P_{13},P_{16},P_{19})$
$(P_2,P_5,P_8,P_{11},P_{14},P_{17},P_{20})$
$(P_{21},P_{24},P_{27},P_{30},P_{33},P_{36},P_{39})$
$(P_{22},P_{25},P_{28},P_{31},P_{34},P_{37},P_{40})$
$(P_{23},P_{26},P_{29},P_{32},P_{35},P_{38},P_{41})$
$(P_{42},P_{45},P_{48},P_{51},P_{54},P_{57},P_{60})$
$(P_{43},P_{46},P_{49},P_{52},P_{55},P_{58},P_{61})$
$(P_{44},P_{47},P_{50},P_{53},P_{56},P_{59},P_{62})$
$\varphi$ の $\mathcal{B}$ 上の作用を
$\varphi=(B_0,B_3,B_6,B_9,B_{12},B_{15},B_{18})$
$(B_1,B_4,B_7,B_{10},B_{13},B_{16},B_{19})$
$(B_2,B_5,B_8,B_{11},B_{14},B_{17},B_{20})$
$(B_{21},B_{24},B_{27},B_{30},B_{33},B_{36},B_{39})$
$(B_{22},B_{25},B_{28},B_{31},B_{34},B_{37},B_{40})$
$(B_{23},B_{26},B_{29},B_{32},B_{35},B_{38},B_{41})$
$(B_{42},B_{45},B_{48},B_{51},B_{54},B_{57},B_{60})$
$(B_{43},B_{46},B_{49},B_{52},B_{55},B_{58},B_{61})$
$(B_{44},B_{47},B_{50},B_{53},B_{56},B_{59},B_{62})$
とする。
$\tau$ の $\mathcal{P}$ 上の作用を
$\varphi=(P_0,P_{21},P_{42})(P_1,P_{22},P_{43})(P_2,P_{23},P_{44})\cdots$
とし、$\tau$ の $\mathcal{B}$ 上の作用を
$\varphi=(B_0,B_{21},B_{42})(B_1,B_{22},B_{43})(B_2,B_{23},B_{44})\cdots$
とする。
$\tau=(P_0,P_{21},P_{42})(P_1,P_{22},P_{43})(P_2,P_{23},P_{44})$
$(P_3,P_{27},P_{54})(P_4,P_{28},P_{55})(P_5,P_{29},P_{56})$
$(P_6,P_{33},P_{45})(P_7,P_{34},P_{46})(P_8,P_{35},P_{47})$
$(P_9,P_{39},P_{57})(P_{10},P_{40},P_{58})(P_{11},P_{41},P_{59})$
$(P_{12},P_{24},P_{48})(P_{13},P_{25},P_{49})(P_{14},P_{26},P_{50})$
$(P_{15},P_{30},P_{60})(P_{16},P_{31},P_{61})(P_{17},P_{32},P_{62})$
$(P_{18},P_{36},P_{51})(P_{19},P_{37},P_{52})(P_{20},P_{38},P_{53})$
で
$\tau=(B_0,B_{21},B_{42})(B_1,B_{22},B_{43})(B_2,B_{23},B_{44})$
$(B_3,B_{27},B_{54})(B_4,B_{28},B_{55})(B_5,B_{29},B_{56})$
$(B_6,B_{33},B_{45})(B_7,B_{34},B_{46})(B_8,B_{35},B_{47})$
$(B_9,B_{39},B_{57})(B_{10},B_{40},B_{58})(B_{11},B_{41},B_{59})$
$(B_{12},B_{24},B_{48})(B_{13},B_{25},B_{49})(B_{14},B_{26},B_{50})$
$(B_{15},B_{30},B_{60})(B_{16},B_{31},B_{61})(B_{17},B_{32},B_{62})$

$(B_{18}, B_{36}, B_{51})(B_{19}, B_{37}, B_{52})(B_{20}, B_{38}, B_{53})$
となる。

$$L = \begin{pmatrix} M_{0\,0} & M_{0\,1} & M_{0\,2} \\ M_{1\,0} & M_{1\,1} & M_{1\,2} \\ M_{2\,0} & M_{2\,1} & M_{2\,2} \end{pmatrix},$$

とかける。
ここで、

$$M_{0\,0} = \begin{pmatrix} L_0 & L_1 & L_2 & L_3 & L_4 & L_5 & L_6 \\ L_6 & L_0 & L_1 & L_2 & L_3 & L_4 & L_5 \\ L_5 & L_6 & L_0 & L_1 & L_2 & L_3 & L_4 \\ L_4 & L_5 & L_6 & L_0 & L_1 & L_2 & L_3 \\ L_3 & L_4 & L_5 & L_6 & L_0 & L_1 & L_2 \\ L_2 & L_3 & L_4 & L_5 & L_6 & L_0 & L_1 \\ L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_0 \end{pmatrix}, \quad M_{0\,1} = \begin{pmatrix} L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} \\ L_{13} & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} \\ L_{12} & L_{13} & L_7 & L_8 & L_9 & L_{10} & L_{11} \\ L_{11} & L_{12} & L_{13} & L_7 & L_8 & L_9 & L_{10} \\ L_{10} & L_{11} & L_{12} & L_{13} & L_7 & L_8 & L_9 \\ L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_7 & L_8 \\ L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} & L_7 \end{pmatrix},$$

$$M_{0\,2} = \begin{pmatrix} L_{14} & L_{15} & L_{16} & L_{17} & L_{18} & L_{19} & L_{20} \\ L_{20} & L_{14} & L_{15} & L_{16} & L_{17} & L_{18} & L_{19} \\ L_{19} & L_{20} & L_{14} & L_{15} & L_{16} & L_{17} & L_{18} \\ L_{18} & L_{19} & L_{20} & L_{14} & L_{15} & L_{16} & L_{17} \\ L_{17} & L_{18} & L_{19} & L_{20} & L_{14} & L_{15} & L_{16} \\ L_{16} & L_{17} & L_{18} & L_{19} & L_{20} & L_{14} & L_{15} \\ L_{15} & L_{16} & L_{17} & L_{18} & L_{19} & L_{20} & L_{14} \end{pmatrix}, \quad M_{1\,0} = \begin{pmatrix} L_{14} & L_{18} & L_{15} & L_{19} & L_{16} & L_{20} & L_{17} \\ L_{17} & L_{14} & L_{18} & L_{15} & L_{19} & L_{16} & L_{20} \\ L_{20} & L_{17} & L_{14} & L_{18} & L_{15} & L_{19} & L_{16} \\ L_{16} & L_{20} & L_{17} & L_{14} & L_{18} & L_{15} & L_{19} \\ L_{19} & L_{16} & L_{20} & L_{17} & L_{14} & L_{18} & L_{15} \\ L_{15} & L_{19} & L_{16} & L_{20} & L_{17} & L_{14} & L_{18} \\ L_{18} & L_{15} & L_{19} & L_{16} & L_{20} & L_{17} & L_{14} \end{pmatrix},$$

$$M_{1\,1} = \begin{pmatrix} L_0 & L_4 & L_1 & L_5 & L_2 & L_6 & L_3 \\ L_3 & L_0 & L_4 & L_1 & L_5 & L_2 & L_6 \\ L_6 & L_3 & L_0 & L_4 & L_1 & L_5 & L_2 \\ L_2 & L_6 & L_3 & L_0 & L_4 & L_1 & L_5 \\ L_5 & L_2 & L_6 & L_3 & L_0 & L_4 & L_1 \\ L_1 & L_5 & L_2 & L_6 & L_3 & L_0 & L_4 \\ L_4 & L_1 & L_5 & L_2 & L_6 & L_3 & L_0 \end{pmatrix}, \quad M_{1\,2} = \begin{pmatrix} L_7 & L_{11} & L_8 & L_{12} & L_9 & L_{13} & L_{10} \\ L_{10} & L_7 & L_{11} & L_8 & L_{12} & L_9 & L_{13} \\ L_{13} & L_{10} & L_7 & L_{11} & L_8 & L_{12} & L_9 \\ L_9 & L_{13} & L_{10} & L_7 & L_{11} & L_8 & L_{12} \\ L_{12} & L_9 & L_{13} & L_{10} & L_7 & L_{11} & L_8 \\ L_8 & L_{12} & L_9 & L_{13} & L_{10} & L_7 & L_{11} \\ L_{11} & L_8 & L_{12} & L_9 & L_{13} & L_{10} & L_7 \end{pmatrix},$$

$$M_{2\,0} = \begin{pmatrix} L_7 & L_9 & L_{11} & L_{13} & L_8 & L_{10} & L_{12} \\ L_{12} & L_7 & L_9 & L_{11} & L_{13} & L_8 & L_{10} \\ L_{10} & L_{12} & L_7 & L_9 & L_{11} & L_{13} & L_8 \\ L_8 & L_{10} & L_{12} & L_7 & L_9 & L_{11} & L_{13} \\ L_{13} & L_8 & L_{10} & L_{12} & L_7 & L_9 & L_{11} \\ L_{11} & L_{13} & L_8 & L_{10} & L_{12} & L_7 & L_9 \\ L_9 & L_{11} & L_{13} & L_8 & L_{10} & L_{12} & L_7 \end{pmatrix}, \quad M_{2\,1} = \begin{pmatrix} L_{14} & L_{16} & L_{18} & L_{20} & L_{15} & L_{17} & L_{19} \\ L_{19} & L_{14} & L_{16} & L_{18} & L_{20} & L_{15} & L_{17} \\ L_{17} & L_{19} & L_{14} & L_{16} & L_{18} & L_{20} & L_{15} \\ L_{15} & L_{17} & L_{19} & L_{14} & L_{16} & L_{18} & L_{20} \\ L_{20} & L_{15} & L_{17} & L_{19} & L_{14} & L_{16} & L_{18} \\ L_{18} & L_{20} & L_{15} & L_{17} & L_{19} & L_{14} & L_{16} \\ L_{16} & L_{18} & L_{20} & L_{15} & L_{17} & L_{19} & L_{14} \end{pmatrix},$$

$$M_{2\,2} = \begin{pmatrix} L_0 & L_2 & L_4 & L_6 & L_1 & L_3 & L_5 \\ L_5 & L_0 & L_2 & L_4 & L_6 & L_1 & L_3 \\ L_3 & L_5 & L_0 & L_2 & L_4 & L_6 & L_1 \\ L_1 & L_3 & L_5 & L_0 & L_2 & L_4 & L_6 \\ L_6 & L_1 & L_3 & L_5 & L_0 & L_2 & L_4 \\ L_4 & L_6 & L_1 & L_3 & L_5 & L_0 & L_2 \\ L_2 & L_4 & L_6 & L_1 & L_3 & L_5 & L_0 \end{pmatrix}$$

$L$は $\{0, 1, 2, 3, 4, 5\}$ 上の21次の正方行列になる。

$L$の各成分が$\{0,1,2\}$の元であるときを調べる。存在する。例えば、

$$L=\left(\begin{array}{ccccccc|ccccccc|ccccccc}
1&1&0&0&0&0&0&0&0&2&1&0&1&2&0&0&2&1&2&1&2\\
0&1&1&0&0&0&0&2&0&0&2&1&0&1&2&0&0&2&1&2&1\\
0&0&1&1&0&0&0&1&2&0&0&2&1&0&1&2&0&0&2&1&2\\
0&0&0&1&1&0&0&0&1&2&0&0&2&1&2&1&2&0&0&2&1\\
0&0&0&0&1&1&0&1&0&1&2&0&0&2&1&2&1&2&0&0&2\\
0&0&0&0&0&1&1&2&1&0&1&2&0&0&2&1&2&1&2&0&0\\
1&0&0&0&0&0&1&0&2&1&0&1&2&0&0&2&1&2&1&2&0\\
\hline
0&2&0&1&2&2&1&1&0&1&0&0&0&0&0&0&0&1&2&2&1\\
1&0&2&0&1&2&2&0&1&0&1&0&0&0&1&0&0&0&1&2&2\\
2&1&0&2&0&1&2&0&0&1&0&1&0&0&2&1&0&0&0&1&2\\
2&2&1&0&2&0&1&0&0&0&1&0&1&0&2&2&1&0&0&0&1\\
1&2&2&1&0&2&0&0&0&0&0&1&0&1&1&2&2&1&0&0&0\\
0&1&2&2&1&0&2&1&0&0&0&0&1&0&0&1&2&2&1&0&0\\
2&0&1&2&2&1&0&0&1&0&0&0&0&1&0&0&1&2&2&1&0\\
\hline
0&2&0&2&0&1&1&0&2&2&2&0&1&1&1&0&0&0&1&0&0\\
1&0&2&0&2&0&1&1&0&2&2&2&0&1&0&1&0&0&0&1&0\\
1&1&0&2&0&2&0&1&1&0&2&2&2&0&0&0&1&0&0&0&1\\
0&1&1&0&2&0&2&0&1&1&0&2&2&2&1&0&0&1&0&0&0\\
2&0&1&1&0&2&0&2&0&1&1&0&2&2&0&1&0&0&1&0&0\\
0&2&0&1&1&0&2&2&2&0&1&1&0&2&0&0&1&0&0&1&0\\
2&0&2&0&1&1&0&2&2&2&0&1&1&0&0&0&0&1&0&0&1
\end{array}\right)$$

## 参考文献


[1] Willem H. Haemers, Conditions for singular incidence matrices, *Journal of Algebraic Combinatrices* **21**, Number 2 (2005), 179-183

[2] Y. Hiramine. A personal comunication.

[3] K. Kawamoto　修士論文　有限群における相対差集合について

[4] V. C. Mavron and V. D. Tonchev, On symmetric nets and generalized Hadamard matrices from affine designs, *J. geometry* **67**(2000), 180-187.

[5] Murray and Brock. A personal comunication.

[6] C. Suetake, The classification of symmetric transversal designs $STD_4[12;3]$'s, *Designs, Codes and Cryptography.***37**(2005), 293-304.

[7] C. Suetake, The existence of a symmetric transversal design $STD_7[21;3]$, to appear in *Designs, Codes and Cryptography.*

位数 $p^4$ の可換 $p$-群における半正則相対差集合
–Ma-Schmidt の予想について–

熊本大学教育学部
平峰 豊

# 1 Introduction

**Definition 1.1** 群 $G$ の部分集合 $D$ が部分群 $U$ に関する $(u\lambda, u, u\lambda, \lambda)$-差集合 (半正則相対差集合) であるとは次の 2 条件がみたされることをいう.

(i) $|U| = u$ かつ $D$ が $G/U$ の完全代表系である.

(ii) $xy^{-1}$ $(x, y \in D,\ x \neq y)$ が $G \setminus U$ の各元を $\lambda$ 回重複して表す.

上の $(u\lambda, u, u\lambda, \lambda)$-差集合は $(m, u, k, \lambda)$-差集合の特別な場合 ([10] 参照) であるがここでは $(u\lambda, u, u\lambda, \lambda)$-差集合に限定して述べるので以下では簡単のために $(u\lambda, u, u\lambda, \lambda)$-差集合を $(u, \lambda)$-差集合 と省略して呼ぶことにする. また, 以下では 群はアーベル群だけを考える.

上の条件 (i) より $|G| = u|D|$, (ii) より $|D|(|D| - 1) = \lambda(|G| - u)$ が成り立つので直ちに次が分かる : $|G| = u^2\lambda$, $|D| = u\lambda$.

**Notation 1.2** 有限群 $G$ の空でない部分集合 $X$ に対して次のように記号を定める.

$$X^{(-1)} = \{x^{-1} \mid x \in X\}.$$

また, $X$ と $\widehat{X} = \sum_{x \in X} x \in \mathbb{C}[G]$ を同一視する.

$(u, \lambda)$-差集合の条件 (i)(ii) をこの記号を用いて群環 $\mathbb{C}[G]$ の言葉で述べれば次のようになる.

$$DD^{(-1)} = u\lambda + \lambda(G - U) \tag{1}$$

次のことが知られている.

- $(u, 1)$-差集合の存在 $\iff$ quasiregular 群をもつ位数 $u$ の射影平面の存在
- $(2, \lambda)$-差集合の存在 $\iff$ 位数 $4\lambda$ の Hadamard 群の存在
  $\iff$ ある種の位数 $2\lambda$ の Hadamard 行列の存在

$u > 2$ のとき既知の例では $u\lambda$ は次の形 :

$u\lambda = p^a$ ($p$ は任意の素数) Elliot-Butson 1968 [4]
$u\lambda = 2^a p^b$ ($p$ はメルセンヌ素数) Davis, et al. 1998 [2]
$u\lambda = 3 \cdot 7$ 秋山, 末竹 2005

## 可換 $p$-群のときの exponent bound について

$(u,\lambda)$ 差集合に関して数多くの結果が知られている．初期の頃は $U$ の exponent に関係する形で $G$ の exponent が研究された．後に $U$ の exponent に関係しない $G$ の exponent の評価式が得られてきた．既知の主要な定理をいくつかあげると次のようになる．

**Theorem 1.3** (Davis 1992 [1]) $(p^a,p^b)$ 差集合において

(i) $a+b\equiv 0 \pmod 2 \implies \exp(G)\le p^{\frac{a+b}{2}}\exp(U)$.

(ii) $a+b\equiv 1 \pmod 2,\ p=2 \implies \exp(G)\le p^{\frac{a+b-1}{2}}\exp(U)$

**Theorem 1.4** (Pott 1994 [9])

(i) $\exp(G)\le p^{\lceil\frac{a+b}{2}\rceil}\exp(U)$.

(ii) $\exp(G)\le p^{a+b}$ (ただし $(p,a,b)\neq(2,1,0)$).

(iii) $\exp(G)\le p^{2a+b-\lfloor\frac{a+b}{2}\rfloor}$.

**Theorem 1.5** (Ma-Pott 1995 [6]) $a+b\equiv 1 \pmod 2 \implies \exp(G)\le p^{\frac{a+b+1}{2}}$

**Theorem 1.6** (Ma-Schmidt 2000 [7]) $a+b\equiv 0 \pmod 2 \implies \exp(G)\le p^{\frac{a+b}{2}+1}$

一般に $U$ の任意の部分群 $N$ に対して $G\longrightarrow G/N$ なる準同型写像を考えることで "$D=(p^a,p^b)$ 差集合 $\implies DN/N=(p^{a-t},p^{b+t})$ 差集合" が成り立つことが容易に分かるから，$t=a-1$ (i.e. $U\simeq Z_p$) のときがある意味で存在・非存在判定のひとつの基準となる．これに関しては次の結果が知られている．

**Theorem 1.7** (Ma-Schmidt 1995 [8])

(i) $c\equiv 1 \pmod 2$ のとき $\exists(p,p^c)$ 差集合 $\iff \exp(G)\le\frac{c+1}{2}+1$.

(ii) $c\equiv 0 \pmod 2$ のとき $\exists(2,2^c)$ 差集合 $\iff \exp(G)\le 2^{\frac{c}{2}+2}$

**Theorem 1.8** (Davis-Jedwab 1997 [2]) $p>2$ かつ $c=2a$ のとき
$\exists(p,p^{2a})$ 差集合 $\iff \exp(G)\le p^{a+1}$
ただし，次の Case I, Case (II) を除外する．
Case I $G\simeq\mathbb{Z}_{p^{a+1}}\times\mathbb{Z}_{p^{a+1}}(\ge U\simeq\mathbb{Z}_p)$,
Case II $G\simeq\mathbb{Z}_{p^{a+1}}\times\mathbb{Z}_{p^a}\times U(\simeq\mathbb{Z}_p),\ a>1$

**Remark 1.9** (i) Ma-Schmidt 1995 により $c$ が奇数のときは $(p, p^c)$ 差集合の存在問題は決着がついたといえる．$p = 2$ なら $c$ が偶数についても決着がついているといえる．どちらの場合も，実際に存在を示す部分では有限局所環やある種の直積が利用されている．
(ii) Davis-Jedwab 1997 [2] により $c$ が偶数の場合でもおおよそ決着がついているのであるが二つの重要な場合 (Case I, II) がまだ残されているのが現状である．

上の Remark にのべた Case I, II について，Ma-Schmidt 2000 によればアーベル群 $G$ が"High exponent & Low rank" である場合はある種の差集合については困難が生じる傾向があるという．この点から見ても今の二つの場合について完全な解決はまだ難しそうに感じる．とくに CASE II についてはその後新しいことは得られていないように思われる．一方，CASE I ではこれまでに $a = 1$ の場合 (i.e. $G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$) に関して次が分かっている．

**Theorem 1.10** (C. Remling 1996 cf. Remark of [7]) $\mathbb{Z}_9 \times \mathbb{Z}_9$ には $(3, 9)$ 差集合は非存在．

Remling の結果は次の Ma と Schmidt の論文に"manuscript"として引用されているので上記はそこからの再引用であるが，MathSciNet で検索しても得られない．おそらく論文として発表されていないのではないかと推測する．

**Theorem 1.11** (Ma-Schmidt 2000 [7]) 奇素数 $p$ に対して群 $G = \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ の $(p, p^2)$-差集合 $D$ は次の形に表される．

$$D = \sum_{0 \le i,j \le p-1} a^i b^j \sum_{x \in \mathbb{Z}_p} (a^p)^x (b^p)^{u_{ij}x^2 + v_{ij}x + w_{ij}},\ \exists u_{ij}, v_{ij}, w_{ij} \in \mathbb{Z}_p,\ u_{ij} \neq 0$$

上記の論文ではさらに $D$ が存在するための必要十分条件を関数の形に表している．

Ma-Schmidt, 2000 ([7])
$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ における $(p, p^2)$ 差集合の存在
$\iff$ ある種の関数 $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p$ の存在

Remling の結果はこの関数を用いて $p = 3$ のときの非存在をコンピュータでチェックしたものと考えられる．

$p = 3$ の場合をコンピュータ使用を最小限にして別の方法でチェックした河本健二による次の結果がある (修士論文 [5])．

**Theorem 1.12** (K. Kawamoto 2005) $\mathbb{Z}_9 \times \mathbb{Z}_9$ は $(3,9)$ 差集合を持たない.

この問題に関して Ma と Schmidt は次の予想をたてている.

**Conjecture** (Ma-Schmidt [7]) $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ $(p > 2)$ には $(p, p^2)$ 差集合は存在しない.

これに関して得た最近の結果を次に述べる.

**Theorem 1.13** Ma-Schmidt の予想は正しい.

次の節ではこの証明の概略を述べる.

## 2 Theorem 1.13 の証明の概略

$p(>3)$ を素数, 群 $G$ を $G = \langle a \rangle \times \langle b \rangle$ $(\simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2})$ とし $U = \langle b^p \rangle$ とおく. このとき $(p, p^2)$ 差集合 $D$ を $D = \{a^{r_i} b^{s_i} | 1 \leq i \leq p^3\}$ とおく. また (1) より次が成り立つ.

$$DD^{(-1)} = p^3 + p^2(G - N). \tag{2}$$

以下で記号 $I_m$ $(= \{0, 1, \cdots, m-1\})$ を用いるがしばしば $\mathbb{Z}_m$ と同一視する. $G$ の指標 $\chi$ $(= \chi_\ell)$ で次のものを考える : $\chi(a) = \theta^\ell$, $\chi(b) = \theta$ $(\theta = \zeta_{p^2})$

このとき (2) より次を得る.

$$\chi(D)\overline{\chi(D)} = p^3 \tag{3}$$

また, $n_j = |\{i \mid \chi(a^{r_i} b^{s_i}) = \theta^j\}|$ とおけば次は明らかである.

$$\chi(D) = \sum_{i \in I_{p^2}} n_i \theta^i. \tag{4}$$

ここで 各 $n_j$ の値は $\ell$ に依存して決まる.

一方では Theorem 1.11 より次を得る.

$$\chi(D) = \sum_{i,j \in I_p} \theta^{i\ell + j} \sum_{x \in I_p} (\theta^p)^{u_{ij}x^2 + (v_{ij} + \ell)x + w_{ij}} \tag{5}$$

(5) を用いてとくに次が成り立つ

**Lemma 2.1** $n_k + n_{k+p} + \cdots + n_{k+(p-1)p} = p^2$ $(\forall k \in I_p)$.

代数体 $\mathbb{Q}(\mathbb{Z}_{p^2})$ における (3) の両辺の素イデアル分解より次が分かる.

**Lemma 2.2** $\exists r_\ell \in I_{p^2}$ $\exists e_\ell \in \{\pm 1\}$

$\chi(D) = e_\ell p\sqrt{p^*}\,\theta^{r_\ell}, \quad p^* = (-1)^{\frac{p-1}{2}}p.$

Lemma 2.2 と (4) および Lemma 2.1 より次が分かる.

**Lemma 2.3** $r = r_\ell$, $e = e_\ell$ とおくとき,

(i) $i \not\equiv r \pmod p \implies n_i = p.$

(ii) $n_{jp+r} = (1 + e(\frac{j}{p}))p \in \{0, p, 2p\} \quad \forall j \in I_p$

**Notation 2.4** 非負整数 $n \in \mathbb{N} \cup \{0\}$ に対して次のようにと定める.

$$n := ((n))p + \ll n \gg \quad (0 \leq \ll n \gg < p))$$

また, multiset $T = \{(\theta^p)^{m_1}, \cdots, (\theta^p)^{m_d}\}$ に対して関数 $f$ を次のように定める.

$$f(T) = \{m_1, m_2, \cdots, m_d\} \pmod p \quad \text{(multiset)}$$

以下では集合は multiset とする

任意の multiset $S$ に対して $S + z := \{x + z \mid x \in S\}$(multiset) と定義する.

$\mu = \psi(\alpha, \beta)$ の定義

$\ell = \alpha p + \beta$, $r = \lambda p + \mu$ $(\alpha, \beta, \lambda, \mu \in I_p, \beta \neq 0)$ とおくとき Lemma 2.2 より $\lambda, \mu$ は $\alpha, \beta$ によりただ一通りに定まるので $\mu = \psi(\alpha, \beta)$ とおける.

$\Omega_\beta(\tau)$ の定義

$\beta, \tau \in I_p$ に対して $\Omega_\beta(\tau)$ を次のように定める.

$$\Omega_\beta(\tau) := \{(i, j) \mid i, j \in I_p, \ \ i\beta + j \equiv \tau \pmod p\}$$

このとき (5) より

$$\chi(D) = \sum_{\tau \in I_p} \sum_{(i,j) \in \Omega_\beta(\tau)} \Big(\theta^{i\alpha p + ((i\beta + j))} \sum_{x \in I} (\theta^p)^{u_{ij}x^2 + (v_{ij} + \beta)x + w_{ij}}\Big)\theta^\tau. \tag{6}$$

$T_{ij\beta} := \{f((\theta^p)^{u_{ij}x^2 + (v_{ij}+\beta)x + w_{ij}} \mid x \in I_p\}, \ \ k_{ij\beta} = \frac{4u_{ij}w_{ij} - (v_{ij}+\beta)^2}{4u_{ij}}.$

と定めれば次が成り立つ.

$$T_{ij\beta} = u_{ij}\Gamma + k_{ij\beta} \quad (\Gamma = \{x^2 \mid x \in \mathbb{Z}_p\}) \tag{7}$$

これより $\Delta = u_{ij}\Gamma + k_{ij\beta} + i\alpha + ((i\beta + j))$ とおけば

$$\chi(D) = \sum_{\tau \in I_p} \Big( \sum_{(i,j) \in \Omega_\beta(\tau)} \sum_{y \in \Delta} (\theta^p)^y \Big)\theta^\tau. \tag{8}$$

従って, Lemma 2.3 より次を得る.

**Lemma 2.5** $\mu := \psi(\alpha,\beta)$ とすると,

(i) $\bigcup_{(i,j)\in\Omega_\beta(\mu)} u_{ij}\Gamma + k_{ij\beta} + i\alpha + ((i\beta+j))$ が含む $\mathbb{Z}_p$ の異なる元は $\frac{p+1}{2}$ .

(ii) $I_p \ni \tau \neq \mu$ ならば $\bigcup_{(i,j)\in\Omega_\beta(\tau)} u_{ij}\Gamma + k_{ij\beta} + i\alpha + ((i\beta+j))$

$$= \underbrace{\{0,\cdots,0\}}_{p\text{-times}} \cup \underbrace{\{1,\cdots,1\}}_{p\text{-times}} \cup \cdots \cup \underbrace{\{p-1,\cdots,p-1\}}_{p\text{-times}}$$

上の Lemma 2.5 は $\mathbb{Z}_p$ の multiset の等式としてはかなり強力な条件のもとでないと成立しそうもないものである. 次の Lemma 2.6 を用いることにより $u_{ij}$ 達は強い条件で束縛されることが分かる.

**Lemma 2.6** $p$:奇素数, $a,b \in \mathbb{Z}_p \setminus \{0\}$
$\Longrightarrow$ 方程式 $x^2 - ay^2 = b$ の解 $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$
の個数は $p - \left(\frac{a}{p}\right)$.

これより,

**Lemma 2.7** $\left(\frac{u_{ij}}{p}\right)$ が一定, 従って $\forall\left(\frac{u_{ij}}{p}\right) = 1$ としてよい.

関数 $\Phi_{\alpha\beta ij}$ を次で定める : $\Phi_{\alpha\beta ij} = \frac{4u_{ij}w_{ij}-(v_{ij}+\beta)^2}{4u_{ij}} + ((i\beta+j)) + i\alpha$.
これに関して次が成り立つ.

**Lemma 2.8** 任意の $\alpha \in \mathbb{Z}_p$ と $\beta \in \mathbb{Z}_p\,(\beta \neq 0)$ ついて,

(i) $(i_1,j_1),(i_2,j_2) \in \Omega_\beta(\psi(\alpha,\beta))$ ならば $\Phi_{\alpha\beta i_1 j_1} = \Phi_{\alpha\beta i_2 j_2}$.

(ii) $\mathbb{Z}_p = \{\Phi_{\alpha\beta ij} \mid (i,j) \in \Omega_\beta(\nu)\}$ $\forall\nu(\neq \psi(\alpha,\beta))$.

**Notation 2.9** $\forall(i,j) \in \Omega_\beta(\psi(\alpha,\beta))$ について

$$\Phi_{\alpha\beta} := \frac{4u_{ij}w_{ij} - (v_{ij}+\beta)^2}{4u_{ij}} + ((i\beta+j)) + i\alpha$$

Lemma 2.8(i) より, $\Phi_{\alpha\beta}$ は $(i,j) \in \Omega_\beta(\psi(\alpha,\beta))$ のとり方によらない.

$(i,j) \in \Omega_\beta(\psi(\alpha,\beta))$ ならば $i\beta + j = \psi(\alpha,\beta)$.
従って,
$\Phi_{\alpha\beta} = \frac{4u_{ij}w_{ij}-(v_{ij}+\beta)^2}{4u_{ij}} + ((i\beta+j)) + i\,\alpha(\beta, i\beta+j)$

**Lemma 2.10** 次が成り立つ.

(i) $\bigcup_{\alpha\in I_p}\Omega_\beta(\psi(\alpha,\beta))=I_p\times I_p \quad \forall\beta$

(ii) $\Lambda(i,j):=\{(\alpha',\beta')\mid (i,j)\in\Omega_{\beta'}(\psi(\alpha',\beta'))\}$ とおくと, $(i_1,j_1),(i_2,j_2)\in\Omega_\beta(\psi(\alpha,\beta))$ ならば $\Lambda(i_1,j_1)\cap\Lambda(i_2,j_2)=\{(\alpha,\beta)\}$.

$$F(j):=\sum_{i\in\mathbb{Z}_p}\sum_{(\alpha,\beta)\in\Lambda(i,j)}\Phi(\alpha,\beta).$$

このとき

**Lemma 2.11** $F(0)=F(1)=\cdots=F(p-1)=\sum_{(\alpha,\beta)\in\mathbb{Z}_p\times\mathbb{Z}_p^*}\Phi(\alpha,\beta)$.

一方では次が成り立つ.

$$F(j)=\sum_{i,\beta\in\mathbb{Z}_p}((i\beta+j))+\sum_{\beta\in\mathbb{Z}_p^*}\beta^{-1}\sum_{k\in\mathbb{Z}_p}k\alpha(\beta,k). \tag{9}$$

第2項は $j$ に依存しない. 従って

**Lemma 2.12** $g(t):=\sum_{i,j\in I_p}((ij+t))\pmod p$ とおくとき, もし $\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}$ に $(p,p^2)$ 差集合が存在すれば $g(0)=g(1)=\cdots=g(p-1)$.

一方では次が容易に証明できる.

**Lemma 2.13** $g(n)=\sum_{i,j\in I_p}((ij+n))\equiv\frac{p-1}{2}-n \pmod p$.

**〈 Theorem 1.13 の証明 〉**

Lemma 2.12 と Lemma 2.13 より矛盾を得る.

Ma-Schmidt の予想が解決したことにより次が目標となる.

**問題1** $a>1$ のとき $\mathbb{Z}_{p^{a+1}}\times\mathbb{Z}_{p^{a+1}}$ $(p>2)$ に $(p,p^{2a})$-差集合は存在するか.

**問題2** $G\simeq\mathbb{Z}_{p^3}\times\mathbb{Z}_{p^2}\times\mathbb{Z}_p$ のとき $\{0\}\times\{0\}\times\mathbb{Z}_p$ に関する $(p,p^4)$-差集合は存在するか.

# References


[1] An Exponent bound of Relative Difference Sets in $p$-groups, *Ars. Combin.* **34** (1992), 318-320.

[2] J.A. Davis and J. Jedwab, A Unifying Construction for Difference Sets, *JCTA* **80** (1997), 13-78.

[3] New Families of Semi-Regular Relative Difference Sets, *DCC* **13** (1998), 131-146.

[4] J.E.H. Elliot and A.T. Butson, Relative difference sets, *Ill. J. Math.* **10** (1968), 517-531.

[5] Kenji Kawamoto, On relative difference sets in finite groups, Master thesis, Kumamoto University, 2005.

[6] S.L. Ma and A. Pott, Relative difference sets, planar function and generalized Hadamard matrices, *J. Algebra* **175** (1995), 505-525.

[7] S.L. Ma and B. Schmid, Relative $(p^a, p^b, p^a, p^{a-b})$-Difference Sets : A Unified Exponent Bound and Local Ring Construction, *Finite Fields and Their Applications* **6** (2000), 1-22.

[8] S.L. Ma and B. Schmid, On $(p^a, p, p^a, p^{a-1})$-Relative Difference Sets, **6**(1995) 57-71.

[9] A. Pott, On the structure of abelian groups admitting divisible difference sets, *JCTA* **65** (1994), 202-213.

[10] A. Pott, "Finite Geometry and Character Theory," Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995)

# Hadamard Matrices について

木村 浩
上武大学ビジネス情報学部

**導入** ： 長い間 428 次の Hdamard matrix の存在がわからなかったが 2004.6 頃 H.Kharaghani and B.Tayfeh-Rezaie によって存在が示された ([2]). Hdamard matrix の分類と構成にかかわってきたのでこれらについての講演をおこなった. その記録である.

**定義** ：$n \times n$ matrix $H = \{\pm 1\}$ が

$$H \cdot H^t = nI$$

をみたすとき $H$ を $n$ 次 Hadamard matrix と云う.

**例**

$$H = \begin{Bmatrix} 1 & 1 \\ 1 & -1 \end{Bmatrix}$$

$$H = \begin{Bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{Bmatrix}$$

**注意** ：以下 H-matrix とは Hadamard matrix を意味する.

**明らかなこと** ：$n$ 次 H-matrix が存在すれば

$$n = 2 \text{ 又は } n \equiv 0 \ (mod\ 4)$$

である.

$H$ を $(H + J)/2$ を同一視する. $J$ はすべて 1 の行列である.

**アダマール予想** ：$n \equiv 0 \ (mod\ 4)$ なる $n$ に対して

$n$ 次 H-matrix が存在する

長い間 428 次の matrix の存在がわからなかったが 2004.6 頃存在が示された ([2]).

**同値類** ： $H_1$ と $H_2$ について $H_1$ の行又は列の符号つき置換で $H_2$ が得られるとき $H_1$ と $H_2$ は同値であるという.

$$H_1 \sim H_2$$

**分類問題** ： H-行列を分類せよ.

| n | 1 | 2 | 4 | 8 | 12 | 16 | 20 | 24 | 27 | 428 | 668 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| # of classes | 1 | 1 | 1 | 1 | 1 | 5 | 3 | 60 | 487 | 1 ? | ? |

$n = 16, 20$ M.Hall.Jr(1961,1965)
$n = 24$ Ito-Longyear-Leon(1979)
Kimura (1989)
$n = 28$ Kimura(1994)
$n = 428$ H.Kharaghani & B.Tayfeh-Rezaie(2004)
存在を示した（分類ではない）

**428 次の matrix について**：昨年6月に4 2 8次の Hadamard Matrix が見つかったとのニュースがもたらされた. H.Kharaghani and B.Tayfeh-Rezaie が構成した matrix の性質を調べてみた. この行列は Hall Set を持っていなかった. ここでは見てわかる簡単な性質を示す.

Hadamard Matrix of order 428

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D^{\overline{t}} & C^{\overline{t}} \\ -C & D^{\overline{t}} & A & -B^{\overline{t}} \\ -D & -C^{\overline{t}} & B^{\overline{t}} & A \end{bmatrix}$$

（図1を参照）
Hadamard Matrix of order 428 (裏から見た行列)

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D^{t} & C^{t} \\ -C & D^{t} & A & -B^{t} \\ -D & -C^{t} & B^{t} & A \end{bmatrix}$$

（図2を参照）
$B^{\overline{t}}$ は行列 $B$ の逆対角線による転置行列

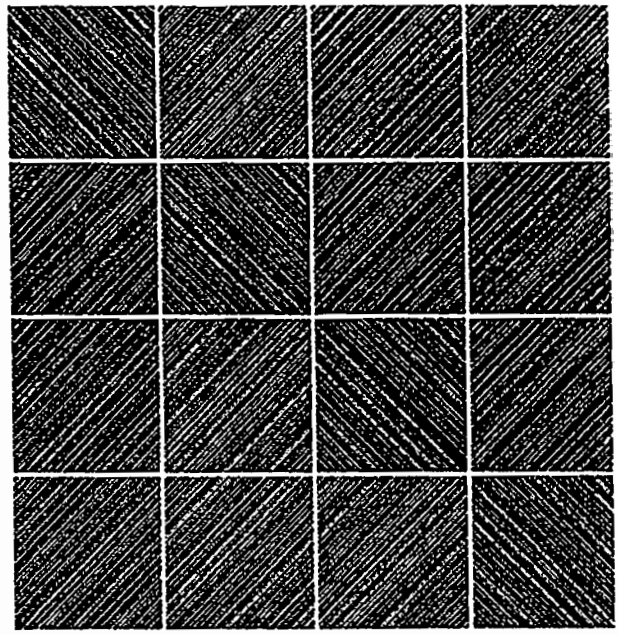


図 1

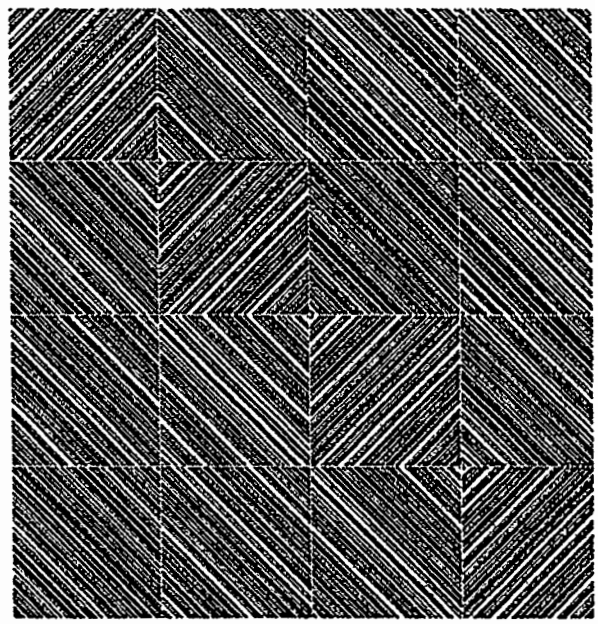


図 2

$n=428$ の H-matrix は作られてしまったが、 28 次の分類の過程で「群」から作れるものがあることがわかった. この方法で他の次数の H-matrix の構成を考えている. これについて述べる.

**問題 1** ：位数 $2p$ の 群を使って $n=8p+4$ 次の H-matrix を作れ.

一部 n については、数論的な方法で解決された ([7]).

**これに対する一つの方法**

$G$ を位数 $p$ の dihedral group とする.

$$G=< x,y\ ;\ |x|=p,\ |y|=2,\ yxy=x^{-1} >$$

$$S\text{: subset of } G \Rightarrow \begin{cases} \overline{S}=G-S \\ S=S_1+S_2y;\ S_1,S_2 \subset < x > \\ S^t=\{g^{-1}|g\in S\} \end{cases}$$

以下 $G$ の部分集合 $S$ と群環 $ZG$ の元

$$\sum_{g\in S} g$$

を同一視する.

次の性質を満たす $G$ の部分群 $A,B,C,D$ を作れ.

**条件 1**

1. $|A|=p-1,\ |B|=|C|=|D|=p$
2. $AA^t+BB^t+CC^t+DD^t=(2p+1)I+2(p-1)J$
3. $A\overline{B}^t+BA^t+CD^t+D\overline{C}^t=(2p-1)J$
4. $A\overline{C}^t+B\overline{D}^t+CA^t+DB^t=(2p-1)J$
5. $AD^t+B\overline{C}^t+CB^t+D\overline{A}^t=2pJ$

$$A\overline{B}^t=(p-1)J-AB^t,\ C\overline{D}^t=pJ-CD^t,\ D\overline{A}^t=pJ-DA^t$$

であるから **条件 1** は次と同値である.

**条件2**

1. $|A| = p-1,\ |B| = |C| = |D| = p$

2. $AA^t + BB^t + CC^t + DD^t = (2p+1)I + 2(p-1)J$

3. $AB^t + DC^t = BA^t + CD^t$

4. $AC^t + BD^t = CA^t + DB^t$

5. $AD^t + CB^t = BC^t + DA^t$

次の仮定をつけて $A, B, C, D$ の構成を考えてみた.

**仮定1**

$$A = A^t,\ B = B^t,\ C = C^t, D = D^t$$

ie.

$$Ay = yA,\ By = yB,\ Cy = yC,\ Dy = yD$$

($A, B, C, D$ は $y$ と可換)

このときには **条件2** の $No\ 3,4,5$ は自動的に満たされる.

**条件3**

$$A^2 + B^2 + C^2 + D^2 = (2p+1)I + 2(p-1)J$$

$G$ の subset $S$ に対して regular representation の行列も表す.

$$H = \begin{bmatrix}
1 & 1 & 1 & 1 & j & j & j & j \\
1 & 1 & \cdot & \cdot & j & j & & \\
1 & \cdot & 1 & \cdot & j & & j & \\
1 & \cdot & \cdot & 1 & & j & j & \\
j^t & j^t & j^t & \cdot & A & B & C & D \\
j^t & j^t & \cdot & j^t & \overline{B} & A & D & \overline{C} \\
j^t & \cdot & j^t & j^t & \overline{C} & \overline{D} & A & B \\
j^t & \cdot & \cdot & \cdot & D & \overline{C} & B & \overline{A}
\end{bmatrix}$$

$$\cdot = 0 and j = (1 \cdots 1)\ (all\ 1's\ vector)$$

と置くと

$$H \text{ は } hadamard \text{ 行列} \Longleftrightarrow A, B, C, D \text{ が } \boxed{\text{条件 3}} \text{ を満たす}$$

さらに

**仮定 2** ：$p$ を素数巾で $|Aut(G)| = 0 \ (mod\ 4)$ とする．さらに $A^2, B^2, C^2, D^2$ は位数 4 の自己同形で不変とする

**問題 2** ：この仮定のもとで H-matrix をつくれ．

$a_1 = |A_1|, a_2 = |A_2|, \cdots, d_1 = |D_1|, d_2 = |D_2|$ と置くと**条件 3** より

**条件 4**

1. $a_1^2 + a_2^2 + b_1^2 + b_2^2 + c_1^2 + c_2^2 + d_1^2 + d_2^2 = 2p^2 + 1$
2. $a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2 = p(p-1)$

条件 4 を満たす $a_1$, $a_2$, $b_1$, $b_2$, $c_1$, $c_2$, $d_1$, $d_2$ について次の結果が得られた．

| p | $a_1$ | $a_2$ | $b_1$ | $b_2$ | $c_1$ | $c_2$ | $d_1$ | $d_2$ | | 存在 |
|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 2 | 2 | 1 | 4 | 3 | 2 | 3 | 2 | 1 | OK |
| 13 | 6 | 6 | 9 | 4 | 7 | 6 | 7 | 6 | 1 | OK |
| 13 | 6 | 6 | 5 | 8 | 5 | 8 | 5 | 8 | 2 | OK |
| 13 | 4 | 8 | 5 | 8 | 7 | 6 | 7 | 6 | 3 | OK |
| 17 | 8 | 8 | 11 | 6 | 7 | 10 | 9 | 8 | 2 | OK |
| 25 | 12 | 12 | 15 | 10 | 15 | 10 | 13 | 12 | 1 | OK |
| 29 | 14 | 14 | 17 | 12 | 17 | 12 | 13 | 16 | 1 | OK |
| 29 | 14 | 14 | 11 | 18 | 13 | 16 | 15 | 14 | 2 | OK |
| 29 | 12 | 16 | 17 | 12 | 13 | 16 | 13 | 16 | 3 | OK |
| 37 | 18 | 18 | 21 | 16 | 21 | 16 | 21 | 16 | 1 | OK |
| 37 | 16 | 20 | 21 | 16 | 21 | 16 | 17 | 20 | 3 | OK |
| 41 | 20 | 20 | 17 | 24 | 23 | 18 | 19 | 22 | 2 | OK |
| 41 | 16 | 24 | 19 | 22 | 19 | 22 | 21 | 20 | 4 | OK |
| 53 | 26 | 26 | 31 | 22 | 29 | 24 | 27 | 26 | 1 | ? |
| 53 | 26 | 26 | 23 | 30 | 23 | 30 | 25 | 28 | 2 | ? |
| 53 | 24 | 28 | 31 | 22 | 25 | 28 | 27 | 26 | 3 | ? |
| 53 | 22 | 30 | 29 | 24 | 25 | 28 | 25 | 28 | 4 | ? |

## 参考文献


[1] Hall Jr, M.: Combinatorial Theory. Wiley, New York, 2nd ed., 1986

[2] Kharaghani, H., Tayfeh-Rezaie, B.: A Hadamard matrix of order 428, J, Combin. Designs, to appear

[3] Kimura, H.: Classification of Hadamard matrices of order 28 with Hall sets. Discrete Math. 128, 257-268(1994)

[4] Kimura, H.: Classification of Hadamard matrices of order 28. Discrete Math. 133, 171-180(1994)

[5] Kimura, H.: Hadamard matrices and dihedral groups. Designs,Codes and Cryptography 9, 71-77(1996)

[6] Kimura, H. and Niwasaki, T.: Some Properties of Hadamard matrices coming from dihedral groups. Graphs and Combinatorics 18, 319-327(2002)

[7] Shinoda, K., Yamada, M.: A family of Hadamard matrices of dihedral group type. Discrete Appl. Math. 102, 141-150(2000)

# 高次元の双対弧 — 平面上の二次曲線の高次元化

吉荒 聡
167-8585 東京都杉並区善福寺 2-6-1
東京女子大学 文理学部 数理学科
yoshiara@lab.twcu.ac.jp

October 13, 2005

この記事は、6月29日(水) 10:00–11:00 に企画公演として行われた筆者の講演「高次元の双対弧 — 平面上の二次曲線の高次元化」をもとに、補足を加えたものである。

講演では、引き続く二つの講演との関連を考慮して、高次元の超卵形という概念への入門に前半部をあてた。射影平面における古典論を紹介 (特に o-多項式の意味) し、高次元の弧という概念が、この古典的な概念の自然な拡張に相当していることの説得に努めた。新しい結果として紹介したのは、「谷口氏により構成された高次元卵形の無限系列 $\mathcal{T}_\sigma(K)$ が Veronese 写像を用いた高次元卵形の無限系列 $\mathcal{V}_d(q)$ の商構造になっている」こととその直接の帰結、関連する有限体上の算術的問題であった。

本論説では、これらの内容のうち前半部を多少敷衍した形で述べ、新しい結果に関しては簡単に触れるにとどめる。

## 1 古典論–射影平面中の弧・卵形・超卵形

この章では、射影平面中の弧、特に卵形・超卵形に関する古典的な結果を概観する。奇標数の係数体における卵形の特徴付け定理 (セグレの定理) を偶標数の係数体の場合に拡張するとき、超卵形を与える o-多項式という概念が登場する。その知られている例や、幾何学的構成についても多少触れたが、これらについての入門レベルからの解説に関しては Cherowitzo 氏の見事なホームページ

http://www-math.cudenver.edu/ wcherowi/

を訪れ、HyperovalPage と Flocks of Cones[1] を開くことを薦める。詳細な情報に関してはそこの参考文献などを参照されたい。

### 1.1 デザルグ的射影平面

$q$ をある素数のべき乗として、ここではデザルグ的射影平面 $PG(2,q)$ のみを考える。すなわち $PG(2,q)$ とは 3 次元ベクトル空間 $V$ 中の 1 次元部分空間の全体 $\binom{V}{1}$ と 2 次元部分空間の全体 $\binom{V}{2}$ に、包含関係 $\subseteq$ を考え合わせた対象 (インシデンス構造) のこととする:

$$PG(2,q) = (\binom{V}{1}, \binom{V}{2}; \subseteq).$$

[1] Flock のイメージがよくわかる

$\binom{V}{1}$ の元のことを射影点、$\binom{V}{2}$ の元のことを射影直線と呼び、$\binom{V}{1} \ni P \subseteq l \in \binom{V}{2}$ であるとき、「直線 $l$ は点 $P$ を通る」ないしは「点 $P$ は直線 $l$ 上にある」と言う。

$V$ の基底 $(\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2)$ を一つ固定したとき、非零ベクトル $\mathbf{x} = \sum_{i=0}^{2} x_i \mathbf{e}_i$ によって生成される 1 次元部分空間 $GF(q)\mathbf{x} = \{\alpha \mathbf{x} \mid \alpha \in GF(q)\}$ を射影点 $P$ と見たものを $[x_0, x_1, x_2]$ と書き、この表示を射影点 $P$ の（基底 $(\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2)$ に関する）同次座標という。任意の $0 \neq \alpha \in GF(q)$ に対して $[\alpha x_0, \alpha x_1, \alpha x_2] = [x_0, x_1, x_2]$ である。$GF(q)$ 係数の 3 変数同次多項式 $f(X_0, X_1, X_2)$ の解 $(x_0, x_1, x_2)$ を取ると、同次性から、任意の $GF(q)$ の元 $\alpha$ に対して $(\alpha x_0, \alpha x_0, \alpha x_2)$ もまた $f(X_0, X_1, X_2)$ の解である。そこで、このとき「射影点 $[x_0, x_1, x_2]$ は同次多項式 $f(X_0, X_1, X_2)$ の解である」という。射影直線 $l$ は 3 次元空間 $V$ の余次元 1 の部分空間なので、ある同次 1 次多項式 $a_0X_0 + a_1X_1 + a_2X_2$ の解ベクトルの全体からなる。この多項式、すなわち列 $(a_0, a_1, a_2)$ は、射影直線 $l$ に対してスカラー倍の違いを除いて一意的に定まるので、同次座標の記号を流用して $l = l[a_0, a_1, a_2]$ と書く。

任意の相異なる 2 個の射影点に対して、それらを通る射影直線は丁度一本存在する。この事実において、直線と点を入れ替えると、「任意の相異なる 2 本の射影直線に対して、それらの上にある射影点は丁度一個存在する」となるが、もう少し直感的な言い方をすると、「任意の相異なる 2 本の射影直線は、丁度 1 点で交わる」ともいえる。この命題も $PG(2, q)$ において成立する。また、一本の射影直線上には $q+1$ 個の射影点があり、一つの射影点を通る射影直線は丁度 $q+1$ 本存在する。

## 1.2 射影平面中の弧・卵形・超卵形とセグレの定理

話は、同次 2 次式の解の全体のなす射影点の集合 $\mathcal{A}$ を幾何学的に考察する事から始まる。射影直線は同次 1 次式で定義されたから、同次 2 次式と連立させたときの解は高々 2 個の射影点からなる。つまり、次が成立する。

> $\mathcal{A}$ は射影点の集合であって、どの射影直線 $l$ を取っても
> その上には $\mathcal{A}$ に属する射影点が高々 2 個存在する:
>
> $$\text{すべての } l \in \binom{V}{2} \text{ に対して} \qquad |l \cap \mathcal{A}| \leq 2. \tag{1}$$

この幾何学的 (座標の取り方、同次多項式といったものに依存しない) 性質のみから出発したとき、何が言えるか?　という自然な問いが原点である。まず、次の事実が示される。

**命題 1** $\mathcal{A}$ が射影平面 $PG(2, q)$ の射影点の集合で、上の性質 *(1)* を満たすならば $|\mathcal{A}| \leq q+2$ である。また、$q$ が奇数であれば、$|\mathcal{A}| \leq q+1$ である。

**証明**　簡単なので、証明を紹介しておく。

$\mathcal{A} = \{P_0, \ldots, P_k\}$ とする。$\mathcal{A}$ 上の一点 $P_0$ とその他の点 $P_i$ $(i = 1, \ldots, k)$ を通る射影直線を $l_i$ とすれば、性質 (1) から、「$1 \leq i \neq j \leq k$ ならば $l_i \neq l_j$」であることがわかる。従って、点 $P_0$ を通る直線が $k$ 本得られたが、1 点を通る射影直線は全部で $q+1$ 本存在するので、$k \leq q+1$, つまり $|\mathcal{A}| = k+1 \leq q+2$ である。

$|\mathcal{A}| = q+2$ とすると、点 $P_0$ を通る射影直線はすべて $\mathcal{A}$ と丁度 2 点で交わる。上の議論は $\mathcal{A}$ のすべての点 $P_0$ について成立するから、「どの射影直線も、$\mathcal{A}$ と丁度 0 点か 2 点で交わる」ということになる。$\mathcal{A}$ に属さぬ点 $Q$ を選ぶ。$Q$ を通る直線で $\mathcal{A}$ の点を含むものの全体を $\mathcal{L}$ とする。$\mathcal{A}$ のどの点もその点と $Q$ を含む直線上にあるから $\mathcal{A}$ は $\mathcal{A} \cap l$ $(l \in \mathcal{L})$ らの直和に分解する。上の注意から $\mathcal{L}$ に属するどの直線に対しても $|l \cap \mathcal{A}| = 2$ であるので、$q+2 = |\mathcal{A}| = \sum_{l \in \mathcal{L}} |\mathcal{A} \cap l| = 2|\mathcal{L}|$ は偶数であり、$q$ も偶数である。　　命題の証明終わり

そこで、次の名称を与えよう。

**定義 2** 射影平面 $PG(2,q)$ の射影点の集合 $\mathcal{A}$ で性質 *(1)* を満たすものを**弧** *(arc)* と呼ぶ。$q+1$ 点からなる弧のことを**卵形** *(oval)* と呼び、$q+2$ 点からなる弧のことを**超卵形** *(hyperoval)* と呼ぶ。超卵形が存在するのは $q$ が 2 のべき乗の時に限る。

**実例**　($PG(2,q)$ を与えるベクトル空間の基底を固定して) 同次 2 次式 $f(X_0, X_1, X_2) = X_0X_2 - X_1^2$ の解射影点の集合を求めると

$$\mathcal{O}(X^2) := \{[1, t, t^2] \mid t \in GF(q)\} \cup \{[0,0,1]\}$$

となる。$\mathcal{O}(X^2)$ は同次 2 次式の解集合だから性質 (1) を満たし、$q+1$ 個の射影点からなるので卵形である。また $q$ が偶数であるとき、これを拡大した点集合

$$\tilde{\mathcal{O}}(X^2) := \mathcal{O}(X^2) \cup \{[0,1,0]\}$$

は超卵形となることがわかる。

一般に、卵形 $\mathcal{O}$ に対して、各点 $P$ に対して $l \cap \mathcal{O} = \{P\}$ を満たす直線 $l$ が丁度一本存在することが示せる (上の証明の議論において $k = q$ として見よ)。この直線 $l$ のことを点 $P$ における $\mathcal{O}$ の**接線**と呼んで $t_P$ と記す。$q$ が偶数であるとき、ある 1 点 $N_{\mathcal{O}}$ が存在して、どの点に対する接線 $t_P$ $(P \in \mathcal{O})$ もこの点を通ることが示せる。(易しくないが、自力で証明を試みると楽しめる。)　この点を卵形 $\mathcal{O}$ の**結節点**と呼ぶ。すると、$\tilde{\mathcal{O}} := \mathcal{O} \cup \{N_{\mathcal{O}}\}$ が超卵形になる。上の例では、$[0,1,0]$ が卵形 $\mathcal{O}(X^2)$ の結節点である。

$q$ が奇数であれば、命題 1 から卵形は最大の大きさを持つ弧である。驚くべきことに、この場合、卵形は本質的には一意に定まることが示せる。Segre によるこの定理がその後の弧に対する研究の原動力となった。

**定理 3** *(Segre, 1955)* $q$ を奇数とする。射影平面 $PG(2,q)$ における卵形 $\mathcal{O}$ に対して、$PG(2,q)$ を与えるベクトル空間 $V$ の適当な基底を取れば、それに関して $\mathcal{O}$ は上の形 $\mathcal{O}(X^2)$ に表示できる。

この定理の証明は、計算中心になるが、なかなか面白い。興味のある方は例えば [7, Lemma 8.11–Theorem 8.14(p.178–180)], その易しい解説として [14] 等を参照されよ。

## 1.3　超卵形と o-多項式

$q$ が偶数のとき、Segre の定理の類似を考察したのは Segre 自身であって、まず次の標準形を見いだした。

命題 4 $q$ を 2 のべき乗とする。射影平面 $PG(2,q)$ 中の超卵形 $\tilde{O}$ に対し、$PG(2,q)$ を与えるベクトル空間 $V$ の適当な基底を選べば $O$ は射影点 $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, $[1,1,1]$ を含む。このとき、$GF(q)$ の元を係数とする以下の性質 *(0),(1),(2)* をすべて満たす多項式 $f(X)$ が存在して $\tilde{O}$ は次の表示を持つ。

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

逆に、下の性質 *(0),(1),(2)* をすべて満たすような任意の多項式 $f(X) \in GF(q)[X]$ に対して、上式の右辺で与えられる射影点の集合 $\tilde{O}(f)$ は, 点 $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, $[1,1,1]$ を含む超卵形である。

*(0)* $f(0)=0$, $f(1)=1$.

*(1)* $f(X)$ は置換多項式である。つまり代入写像 $GF(q) \ni x \mapsto f(x) \in GF(q)$ は全単射。

*(2)* 任意の元 $s \in GF(q)$ に対して $f_s(X) := (f(X+s)+f(s))/X$ により定められる多項式 $f_s(X)$ は、置換多項式である。
*($f_s(X)$ の分子に現れる多項式は 0 を解に持つので $f_s(X)$ は確かに多項式である。)*

**定義 5** 上の命題に述べられた性質 *(0),(1),(2)* をすべて満たす $GF(q)$-係数の多項式 $f(X)$ のことを o-多項式と呼ぶ。($q$ は 2 のべき乗)

そこで、超卵形の研究は o-多項式の研究に帰着される。o-多項式の無限系列が幾つか発見されている。その記述のために、射影同値という言葉を定義しておく。$PG(2,q)$ を与えるベクトル空間を $V$ とするとき、$PG(2,q)$ のインシデンス構造としての自己同型 ($\binom{V}{1} \cup \binom{V}{2}$ 上の全単射で包含関係を保つもの) は $V$ 上の半線形変換 (全単射 $GF(q)$-線形変換と係数体 $GF(q)$ のガロア自己同型の合成写像) から引き起こされたこと (射影幾何の基本定理) を思い出そう。

**定義 6** *(1)* $PG(2,q)$ 中の弧 $\mathcal{A}$ と $\mathcal{B}$ が射影同値であるとは、$PG(2,q)$ を与えるベクトル空間 $V$ 上の半線形変換 $\rho$ が存在して (射影点の集合として) $\mathcal{A}^\rho = \mathcal{B}$ であることとする。

*(2)* 二つの o-多項式 $f(X)$ と $g(X)$ が射影同値であるとは、$V$ の適当な基底 $\mathcal{E}$ に関して $\tilde{O}(f)$ の形に表示される超卵形が、$V$ の適当な基底 $\mathcal{F}$ に関して $\tilde{O}(g)$ の形に表示される超卵形と射影同値であることとする。

すなわち、$V$ 上の半線形変換 $\rho$ 及び $V$ の基底 $\mathcal{E}$ が存在して、$\mathcal{E}$ に関する超卵形 $\tilde{O}(f)$ が基底 $\mathcal{F} = \mathcal{E}^\rho$ に関して $\tilde{O}(g)$ と表示されるとき、$f(X)$ と $g(X)$ は射影同値であるという。

例えば、単項式 $f(X) = X^N$ $(1 \le N \le q-1)$ が o-多項式であれば、$q-1$ と $N$ 及び $q-1$ と $N-1$ は互いに素であり、$q-1$ を法としての逆数 $1/N$, $1/(1-N)$ 等が定義できるが、次の 6 個の単項式

$$X^N,\ X^{1/N},\ X^{1-(1/N)},\ X^{1-N},\ X^{1/(1-N)},\ X^{N/(N-1)}$$

はすべて互いに射影同値な o-多項式となる。(ここで指数はすべて $q-1$ を法として読む。)

$q=2^{d+1}$ とする。現在知られている $GF(q)$ 係数の o-多項式のうち、単項式で与えられる無限系列は、次のいずれかと射影同値である。

(T) (Galois 群の生成元に対応するもの) $X^{2^m}$, $(1 \le m \le d+1, m$ は $d+1$ と互いに素$)$. 特に $m=1$ の場合は、同次 2 次式の解集合に対応し、最も標準的な例である。$X^2$ と一般の $X^{2^m}$ は射影同値ではない。

(S) (Segre の多項式) 偶数 $d$ に対する $X^6$.

(G) (Glynn の多項式) $d$ を偶数とする。
(G-1) $d=4m-2$ $(m \ge 1)$ のとき $X^{2^{2m}+2^m}$ 及び $X^{3\cdot 2^{2m}+4}$
(G-2) $d=4m$ $(m \ge 1)$ のとき $X^{2^{3m+1}+2^{2m+1}}$ 及び $X^{3\cdot 2^{2m+1}+4}$

単項式で表されるとは限らない o-多項式の無限系列として次が知られている。ここで単項式の指数に現れる整数は、乗法群 $(\mathbf{Z}/(q-1))^\times = \{n(\bmod q-1) \mid n \in \mathbf{Z}, (n, q-1)=1\}$ の元と見なし、それらの逆数、積はこの群の中で考えている。

(P) (Payne の多項式) 偶数 $d$ に対する $X^{1/6}+X^{1/2}+X^{5/6}$

(C) (Cherowitzo の多項式) 偶数 $d=2s$ に対する $X^{2^{s+1}}+X^{2^{s+1}+2}+X^{3\cdot 2^{s+1}+4}$

以上はすべて係数が素体 $GF(2)$ に入る o-多項式と射影同値な例であるが、次のものはそうとは限らない。

(Sub) (Subiaco [2]多項式) $d+1 \not\equiv 2 \pmod 4$ ならば $e$ は $Tr_{GF(q)/GF(2)}(e)=1$ を満たす任意の $GF(q)$ の元、$d+1 \equiv 2 \pmod 4$ ならば $e$ はこの条件に加えて $e \notin GF(4)$ を満たすとする。このとき次の多項式は o-多項式である。

$$\left(e^2(X^4+X)+e^2(1+e+e^2)(X^3+X^2)\right)(X^4+e^2X^2+1)^{-1}+X^{1/2}.$$

(Ade) (Adelaide 多項式) $F=GF(q)$ $(q=2^{d+1})$ の二次拡大体 $K=GF(q^2)$ を考え、$b$ は $b^{q+1}=1 \ne 1$ を満たす $K$ の元とする。拡大 $K/F$ に関するトレースを $tr$ と書く: $tr(x)=x^q+x$.

$d$ が偶数の時は $m$ は任意の整数 $d$ が奇数の時は $m=\pm(q-1)/3$ とする。このとき次の多項式は o-多項式である。

$$(tr(b))^{-1}tr(b^m)(X+1)+(tr(b))^{-1}tr((bX+b^q)^m)(X+tr(b)X^{1/2}+1)^{1-m}+X^{1/2}.$$

小さい $d$ の値においては、これらの族に属する o-多項式には重なるものがある。また $d=4$ の時にはこれらのどれにも属さない散在的な例が存在する。更に $d=2,3,4$ では分類表が出来ており、単項の場合には $d \le 27$ までは分類されているという。

[2]オーストラリア、パースの近郊で University of Western Australia に近い土地の名らしい

Flock と呼ばれる幾何学的概念（射影空間 $PG(3,q)$ 中の二次錘の頂点以外の点のなす集合を、互いに交わらない平面での切り口に分割したもの）があるが、o-多項式のまとまりと関連することが知られており、上の表の例 (Sub), (Ade) は、この観点から幾何学的に発見された無限系列である。これらの幾何学的概念はまた、ある種の translation planes や一般化された四角形の一部とも関連することが知られており、o-多項式は、様々な幾何学的概念の介在役といえる存在である。

具体的に与えられた多項式が o-多項式であるための判定条件が Glynn により得られているが、これは計算機を用いて確認するのに適した形である。その説明のため、区間 $[1,q-1] := \{i \in \mathbf{Z} \mid 1 \le i \le q-1\}$ 上に次の半順序関係 $\preceq$ を用意する。

**定義 7** 区間 $[1,q-1]$ $(q=2^{d+1})$ 中の整数 $a$ と $b$ に対して、それらの 2 進展開をとる:

$$a=\sum_{i=0}^{d} a_i 2^i,\ b=\sum_{i=0}^{d} b_i 2^i,\ a_i,b_i \in \{0,1\}\ (i=0,\ldots,d).$$

このとき、すべての $i=0,\ldots,d$ に対して $a_i \le b_i$ であるとき、そのときに限って $a \preceq b$ と定義する。

$a,b \in [1,q-1]$ に対して、標数 2 の体を係数として多項式 $(X+1)^b$ を展開したとき、そこに項 $X^a$ が現れるための必要かつ十分な条件が $a \preceq b$ であることに注意しよう。

**定理 8** *(Glynn の判定条件 [6][3])* $GF(q)$ 係数の多項式 $f(X)$ が *o*-多項式であるためには、次の条件がともに満たされることが必要かつ十分である。

*(1)* $\sum_{\alpha \in GF(q)} f(\alpha)^{q-1} = 1$.

*(2)* $a,b \in [1,q-1]$, $b \ne q-1$, $a \preceq b$ を満たすすべての整数の組 $(a,b)$ に対して $f(X)^b \bmod X^q - X$ *($f(X)^b$ を $X^q-X$ で割った余りである次数高々 $q-1$ の多項式)* における $X^a$ の係数は 0.

特に $f(X)$ が単項式 $X^N$ の場合、$X^N$ が o-多項式であるための必要かつ十分な条件は

(i) $(N,q-1)=1$ かつ

(ii) $1 \le b \le q-2$ を満たすすべての整数 $b$ に対して $b \not\preceq (bN \bmod q-1)$

が成立することである。(ここで $bN \bmod q-1$ とは、整数 $bN$ を $q-1$ で割った余りのこと。(i) と $1 \le b \le q-2$ から $bN$ は $q-1$ で割り切れないことに注意。) これは [5, Theorem A] の主結果である。

[3]先日のオランダ Oisterwijk での集会 (Aug.14–19,2005) における Betten 氏の公演中に述べられた修正形を述べる。原論文では、条件 (1) が抜けている。

## 2 高次元化の試み

### 2.1 高次元の双対弧

前章に述べた射影平面中の弧という概念を高次元化するのが目的である。様々な方向があろうが、ここでは、射影平面 $PG(2,q)$ を一般の射影空間 $PG(n,q)$ に、射影点の集合を $PG(n,q)$ の一般の次元の部分空間に拡張したい。そのような対象をうまく（二次曲面の部分空間化などを標準例に含み、かつ面白い例外があるような豊かな体系として）定義して、これらの部分空間族の研究を、低次元での研究方向をモデルにして進めるだけでなく、逆に、射影平面での古典論で展開される（かなり無統制に見える）o-多項式の中からより標準的なものを選び出すといった形の、高次元化の効用も期待したい。更に大きく夢を描けば、前章の最後に述べたような、様々な幾何学的概念との関連の仲介役となる概念となる可能性を検討したい。

射影平面での弧を、その双対弧に置き換えてみると高次元化しやすいので（特にマシュー群に $M_{22}$ に関連する例を考えたとき、そのようにした方が見やすいという理由で）まず、射影平面での弧の定義 (1) において射影点と射影直線を入れ替えて得られる双対弧の公理を書いてみる。すると、

> 射影平面 $PG(2,q)$ 中の射影直線 $^*\mathcal{A}$ の集合が双対弧であるとは、
> 任意の射影点 $P$ に対して $P$ を通る $^*\mathcal{A}$ の元の個数が高々 2 本であること：

となるが、これを言い換えれば、次の性質となる。

$$^*\mathcal{A} \text{ の相異なる 3 メンバー } l,m,n \text{ に対して} \qquad l\cap m\cap n=\{0\}. \tag{2}$$

更に、射影平面中では $^*\mathcal{A}$ の任意の相異なる直線は一点で交わる。つまり、

$$^*\mathcal{A} \text{ の相異なる 2 メンバー } l,m \text{ に対して} \qquad l\cap m \text{ は射影点である.} \tag{3}$$

ここで、射影平面中の射影直線のかわりに、ある射影空間中の固定した次元の部分空間を考え、二つのメンバーの交わりが射影点という性質を保存して定義される概念を考える。以下の公理 (DA1) は上の性質 (3) に、公理 (DA2) は上の性質 (2)（性質 (1) の双対化）に相当する。

**定義 9** $n$ と $d$ は $1\le d\le n$ を満たす整数とし、$q$ はある素数のべき乗とする。また、$U$ を有限体 $GF(q)$ 上の $n+1$ 次元ベクトル空間とする。$U$ の幾つかの $d+1$ 次元部分空間のなす集合 $\mathcal{A}$ が次の 2 条件 *(DA1)* と *(DA2)* を満たすとき、$\mathcal{A}$ を $d$（射影）次元双対弧 *(d-dimensional dual arc)* と呼ぶ。

*(1)* $\mathcal{A}$ の任意の相異なる二つのメンバー $X$ と $Y$ に対して、それらの共通部分 $X\cap Y$ は $U$ の 1 次元の部分空間である。

*(2)* $\mathcal{A}$ の任意の相異なる 3 つのメンバー $X, Y, Z$ に対して、それらの共通部分は零空間である: $X\cap Y\cap Z=\{0\}$.

また $\mathcal{A}$ のメンバー全体により生成される $U$ の部分空間のことを $\mathcal{A}$ の生成空間 *(ambient space)* といい $\mathbf{A}(\mathcal{A})$ と記す。

$$\mathbf{A}(\mathcal{A}) := \langle X \mid X\in\mathcal{A}\rangle.$$

$\mathcal{A}$ が $d$ 次元双対弧で $U$ がその生成空間 $\mathcal{A}(\mathcal{A})$ に一致することを、「$\mathcal{A}$ は $U$ 中の双対弧」ないしは 「$\mathcal{A}$ は $PG(U) \cong PG(n,q)$ 中の双対弧」とも表現する。また次元 $d$ を明示しないときには、高次元の双対弧ともいう。

**注意**　従来の定義では上の公理に加えて「生成空間が $U$ に一致している」ことを条件に加えていた。しかし、大きなベクトル空間 $V$ の中で構成される実例が多く、生成空間が $V$ と一致するわけではないので、従来の定義に合わせようとすると、生成空間とその射影次元を、それぞれ $A, n$ などと記号で置き直して、$PG(A,q) \cong PG(n,q)$ 中の $d$ 次元双対弧と呼んでいた。これは、煩瑣であり、生成空間がはっきりしない場合には曖昧さも感じられる。そこで、今回の定義ではこの条件をはずすことにした。そのようにしても実質上全く問題はない。

**$d=1$ の場合**　$d=1$ としたときに、1 次元の双対弧 $\mathcal{A}$ という概念は、古典的な射影平面中の双対弧という概念と一致していることを見よう。

生成空間 $\mathrm{A}(\mathcal{A})$ が 3 次元ベクトル空間であることを確かめれば、$PG((\mathcal{A})) \cong PG(2,q)$ は射影平面で $\mathcal{A}$ はその射影直線の集合であり、上の公理 (DA1) は自動的に満たされ、公理 (DA2) は射影平面中の双対弧の定義に他ならない。そこで、$\dim(\mathrm{A}(\mathcal{A})) = 3$ を見ればよい。

$\mathcal{A}$ の相異なるメンバー $l, m$ を取れば、$d=1$ から $\dim(l) = \dim(m) = 2$ で、公理 (DA1) より $\dim(l \cap m) = 1$ なので、$l$ と $m$ が生成する $\mathrm{A}(\mathcal{A})$ の部分空間 $\langle l, m\rangle$ は $2+2-1=3$ 次元である。$\mathcal{A}$ の $l, m$ 以外のメンバー $n$ を取ると、公理 (DA1) から $\dim(n \cap l) = 1 = \dim(n \cap m)$ であり、公理 (DA2) から $\dim(n \cap l \cap m) = 0$ なので $2 = \dim(n) = \dim(n \cap l) + \dim(n \cap m)$ 従って $n = \langle n \cap l, n \cap m\rangle$ となり、$n$ は $\langle l, m\rangle$ に含まれる。$n$ は $\mathcal{A} \setminus \{l, m\}$ の任意のメンバーだったから　$\mathrm{A}(\mathcal{A}) = \langle n \mid n \in \mathcal{A}\rangle \subseteq \langle l, m\rangle \subseteq \mathrm{A}(\mathcal{A})$ となり、$\mathrm{A}(\mathcal{A}) = \langle l, m\rangle$ の次元は 3 である。

**補題 10** $\mathcal{A}$ を生成空間 $U$ 中の $d$ 次元双対弧とする。このとき、双対弧 $\mathcal{A}$ に含まれる部分空間の個数 $|\mathcal{A}|$ について次が成り立つ。

$$|\mathcal{A}| \leq \frac{q^{d+1}-1}{q-1} + 1. \tag{4}$$

**証明**　$\mathcal{A}$ の一つのメンバー $A$ を取る。$A$ 以外の $\mathcal{A}$ のメンバー $X$ に対して共通部分 $A \cap X$ を考えれば、公理 (DA1) により、$A \cap X$ はベクトル空間 $A$ の与える射影空間 $PG(A) \cong PG(d,q)$ の射影点である。そこで、$\binom{A}{1}$ により射影空間 $PG(A)$ の射影点全体の集合を表すことにすると、写像

$$\mathcal{A} \setminus \{A\} \ni X \mapsto X \in \binom{A}{1}$$

が定義された。公理 (DA2) は、この写像が単射であることを示す。従って、

$$|\mathcal{A}| - 1 \leq |\binom{A}{1}| = \frac{(q^{d+1}-1)}{(q-1)}$$

であり、不等式 (4) を得る。　**補題の証明終わり**

この結果は、まさしく射影平面の場合 ($d=1$) の結果（命題 1 の前半）の拡張である。そこで、射影平面の例にならって、次の命名を行う。

**定義 11** $\mathcal{A}$ を $d$ 次元の双対弧とする。$|\mathcal{A}| = ((q^{d+1}-1)/(q-1))+1$ のとき $\mathcal{A}$ を**双対超卵形**、$|\mathcal{A}| = (q^{d+1}-1)/(q-1)$ のとき $\mathcal{A}$ を**双対卵形**という。

非常に不思議なことであるが、命題の後半の拡張にあたる結果「$PG(n,q)$ の部分空間からなる $d$ 次元の双対超卵形が存在すれば $q$ は偶数である」は、未だ一般に証明されていない。($d$ が奇数のとき、$d=2$ または生成空間の射影次元が $2d$ に等しいときには、この事実が成立することが知られている。)

## 2.2 高次元の双対卵形・超卵形の生成空間と例

**生成空間の次元** $d$ 次元双対（超）卵形 $\mathcal{H}$ の生成空間 $U$ のベクトル次元に関しては次の結果が知られている [15]。

**命題 12** $U$ を有限体 $GF(q)$ 上のベクトル空間、$\mathcal{H}$ は $U$ を生成空間とする $d$ 次元双対超卵形または卵形であるとする。このとき

*(1)* $q \neq 2$ ならば $\dim(U) \leq (d+1)(d+2)/2$.

*(2)* $q = 2$ ならば $\dim(U) \leq 2 + ((d+1)(d+2)/2)$.

2 以外のすべての素数べき $q$ に対して、上の命題の不等式で等号が成立するような $d$ 次元双対卵形の例が構成できる。(後述の例 (V) を見よ。) $q=2$ の時でも $q \neq 2$ の時と同じ不等式が成立すると予想されているが、未解決である。

**高次元双対超卵形の例–概観** 一般の自然数 $d$ に対する $d$ 次元の双対卵形（超卵形）の例として、現時点で知られている例をすべて挙げる。ここでは数学的に正確な描写は与えない。構成 (V), (T) についてのみ、次に詳しく記述する。

(M) **自己同型群として 22 次マシュー (Mathieu) 群が現れる構成:**
古くから知られており、高次元の双対超卵形の概念が作られるきっかけを与えた例である。これは四元体 $GF(4)$ 上の 6 次元ベクトル空間 $U$ を生成空間とする 2 次元双対超卵形 $\mathcal{M}$ である。しかも、$\mathcal{M}$ は $U$ 上のユニタリ形式 $f$ に関して極型 ($\mathcal{M}$ のすべてのメンバーは $f$ に関して極大全等方部分空間) であることが知られている。また、$\mathcal{M}$ の自己同型群（つまり $U$ 上の射影変換で $\mathcal{M}$ のメンバーの入れ替えを引き起こすもの全体のなす群）は 22 次のマシュー群 $M_{22}$ を指数 2 で含むことも知られている。

(V) **ヴェロネーズ (Veronese) 写像を用いた構成:** (J.Thas と H.van Maldeghem [11] 及び、彼らとは別個に Yoshiara [15, Subsection 3.2] による。)
任意の素数べき $q$ 及び任意の自然数 $d$ に対して双対卵形 $\mathcal{V}$ が構成され、その生成空間 $U$ のベクトル次元は $(d+1)(d+2)/2$ である。$q$ が偶数の時、そのときに限って、この双対弧 $\mathcal{V}$ に一つの $d+1$ 次元部分空間 $N$ を付け加えて、$\mathcal{HV}_q^d := \mathcal{V} \cup \{N\}$ を生成空間 $U$ 中の $d$ 次元双対超卵形とすることが出来る。

二次曲面の超平面化を与えるヴェロネーズ写像の与える部分空間族が、高次元の双対弧という概念に取り込めたことになり、この概念の豊かさを示す事実である。

論文 [11] はこの高次元双対卵形を幾何学的条件から特徴付けようとした試みであり、Segre の定理の偶標数・高次元版と考えられる。ここで課されている条件がどれだけ緩和できるか検討するのは重要であろう。

(C) **ブロックデザインと関連した構成:** (M. Buratti と A. Del Fra [1] による。) 任意の自然数 $d$ に対して $GF(2^{d+1})$ 上の $(d+1)(d+2)/2$ 次元ベクトル空間を生成空間とする双対超卵形で、そのメンバーの集合上にある種のブロックデザインの構造が入るようなものが構成できる。この構成から本質的に異なる二種類の超卵形が得られることがわかる [4, Theorem 3] が、このうち一方は C.Huybrechts がはじめて構成したもの [9] と同一である。

この構成は、ある意味で $q=2$ の特殊性を示す。この例の位置付けについては、更に考察すべきことが多々ある。

(Y) **$GF(2^{d+1})$ 上のある多項式を用いた構成 $S^{d+1}_{\sigma,\phi}$:** (S.Yoshiara [13, Section 2] による。) 二つの $GF(2^{d+1})$ の直和 $U := GF(2^{d+1}) \oplus GF(2^{d+1})$ を $GF(2)$ 上の $2(d+1)$ 次元ベクトル空間と見なす。$GF(2^{d+1})$ の元を係数とする二つの多項式 $\sigma(X)$, $\phi(X)$ を選んで、($GF(2^{d+1})$ の元でパラメータ付けられた) $U$ の $d+1$ 次元部分空間の族 $X(t)$ $(t \in GF(2^{d+1}))$ を構成する。これらの集合 $\{X(t) \mid t \in GF(2^{d+1})\}$ が双対超卵形になるための必要十分条件は、(適当な変換により) 多項式 $\sigma(X)$ の定める $GF(2^{d+1})$ 上の写像 $\sigma$ が拡大 $GF(2^{d+1})/GF(2)$ のガロア群 $Gal(GF(2^{d+1})/GF(2))$ の生成元であり、かつ多項式 $\phi(X)$ が o-多項式であることが示される [12, Section 5]。

この事実は、谷口氏により初めて明白に示されたものである。多項式が自然に o-多項式とならざる得ない (一つは更に強くガロア群の生成元にならざる得ない) という点は、「高次元の超卵形の研究が射影平面と深く結びつきながらも、o-多項式の中からより標準的なものと関係してくる」という期待されるべき方向を示している。

$S^{d+1}_{\sigma,\phi}$ の生成空間は合成写像 $\sigma\phi$ が $GF(q)$ 上の恒等写像でないかあるかに従って $U$ ないしはその超平面 $\{(x,y) \in V \mid Tr_{GF(q)/GF(2)}(y) = 0\}$ に一致する。

(T) **$GF(q)$ 上のある多項式を用いた構成:** (H.Taniguchi [10] による。) この構成は、構成 (Y) の変形のように見えるものであるが、任意の素数べき $q$ に対して定義出来る。$q=2$ で、ある条件を満たす場合には $S^{d+1}_{\sigma,\phi}$ $(\phi(X) = X^{q-2})$ と一致することがわかる。構成された双対超卵形の生成空間の次元が、様々に動きうることがこの構成の利点であるが、後述するように、この構成による双対超卵形は構成 (V) による双対超卵形から原理的に得られる (商構造になっている)。

このほかに、生成空間の次元が $2d+1$ であるような $d$ 次元双対超卵形の一般形を定めた B. Cooperstein と J. Thas の結果 [2] 及び A. Del Fra による 2 次元の双対超卵形の分類 [3] において、当時知られていなかった例が構成されている。

# 3 谷口の双対卵形と Veronese 双対卵形

この章では、谷口氏の双対超卵形の構成を拡張して、任意の素数べき $q$ に対して、一般には生成空間の小さい双対卵形を構成し、それが Veronese 構成で得られる高次元の卵形（最も生成空間の次元が高い）ものから（半）線形写像によって、商構造として得られるという観察結果を述べる。この結果から、論文 [15] に述べられた問題がほぼ解決されるが、最終的な解決には、ある有限体上の算術問題を解く必要がある。

## 3.1 谷口の双対卵形と Veronese 双対卵形

谷口氏が論文 [10] で与えた構成をそのまま拡張して、次のような対象を考える。$q$ を任意の素数べきとし、直和 $U := GF(q^n) \otimes GF(q^n)$ を $GF(q)$ 上 $2n$ 次元のベクトル空間と見なし、$K$ を $U$ の $d+1$ 次元の任意の部分空間とする。ガロア群 $Gal(GF(q^n)/GF(q))$ の生成元 $\sigma$ を取り固定する。$PG(K) \cong PG(d,q)$ の射影点 $P$ に対して（$K$ の 1 次元部分空間と見た）$P$ 中の任意の非零ベクトル $t$ を取り

$$T(P) := \{(xt, x^\sigma t + xt^\sigma) \mid x \in K\}$$

とおく。$T(P)$ は $t$ の取り方によらずに決まる $U$ の $d+1$ 次元部分空間である。$P$ が $PG(K)$ の射影点を動くときの $T(P)$ を集めて $\mathcal{T}_\sigma(K) := \{T(P) \mid P \in \binom{K}{1}\}$ とする。このとき次が示せる。

**命題 13** *[19, Subsection 2.2]* $\mathcal{T}_\sigma(K)$ は $d$ 次元双対卵形であり、その生成空間は $K$ の $GF(q)$ 上の基底を $e_i$ $(i = 0, \ldots, d)$ とするとき $0 \le i \le j \le d$ を満たす対 $(i,j)$ に対する $U$ のベクトル $e_{(i,j)} := (e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma)$ の全体で生成される $U$ の部分空間に一致する。

$q$ が偶数であれば $T(\infty) := \{(x^2, 0) \mid x \in K\}$ も $U$ の $d+1$ 次元部分空間であり $\tilde{\mathcal{T}}_\sigma(K) := \mathcal{T}_\sigma(K) \cup \{T(\infty)\}$ は $d$ 次元双対超卵形である。その生成空間は $\mathcal{T}_\sigma(K)$ の生成空間に等しい。

命題 13 から見られるように、一般に生成空間 $\mathbf{A}(\mathcal{T}_\sigma(K))$ の次元ははっきり決まらない。しかし、この構成は非常にコンパクトであるので、例えば包絡数 (wrapping number) というような重要な数を計算するのに適している。その計算アルゴリズムと計算値は [19, Subsection 3.3] を参照されたい。

前章で紹介した $d$ 次元双対卵形 $\mathcal{A}_d(q)$ は任意の素数べき $q$ に対して Veronese 写像を用いて次のように定義される [15, Subsection 3.1]。

一般に $V$ と $W$ を $GF(q)$ 上それぞれ $d+1$ 次元と $(d+1)(d+2)/2$ 次元のベクトル空間とする。ここで

$$I := \{0, 1, \ldots, d\}, \quad J := \{(i,j) \mid i, j \in I, i \le j\}$$

とおくとき、$V$ の基底 $\mathcal{E}$ を $\{\mathbf{e}_i \mid i \in I\}$, $W$ の基底 $\mathcal{F}$ を $\{\mathbf{e}_{(i,j)} \mid (i,j) \in J\}$ と添数付けることが出来る。Veronese 写像とは、次の式で定義される $V$ から $W$ への写像 $\zeta$ のことである：

$$\zeta(\sum_{i \in I} x_i \mathbf{e}_i) := \sum_{(i,j) \in J} x_i x_j \mathbf{e}_{(i,j)}.$$

さて、$d$ 次元射影空間 $PG(V) \cong PG(d,q)$ の各点 $P = [\sum_{i\in I} t_i \mathrm{e}_i]$ (基底 $\mathcal{E}$ に関する同次座標) に対してその $V$ における双対空間

$$P^{\perp} := \{\sum_{i\in I} y_i \mathrm{e}_i \mid \sum_{i\in I} t_i y_i = 0\}$$

をとれば、$P^{\perp}$ は $V$ の超平面である。$P^{\perp}$ の Veronese 写像 $\zeta$ による像 $\zeta(P^{\perp})$ を考えると、これはベクトル空間 $W$ 中の単なる部分集合であるが、その $W$ における双対

$$A(P) := (\zeta(P^{\perp})^{\perp} := \{\sum_{(i,j)\in J} x_{(i,j)}\mathrm{e}_{(i,j)} \mid \sum_{(i,j)\in J} x_{(i,j)}y_{(i,j)} = 0(\forall \sum_{(i,j)\in J} y_{(i,j)}\mathrm{e}_{(i,j)} \in \zeta(P^{\perp}))\}$$

を考えると、これは $W$ の $d+1$ 次元部分空間になる。この部分空間を集めて得られる族

$$\mathcal{V}_d(q) := \{A(P) \mid P \in \binom{V}{1}\}$$

は $d$ 次元双対卵形で、その生成空間は $W$ に一致する。更に $q$ が偶数であるとき、かつそのときに限り $\mathcal{V}_d(q)$ は超卵形 $\tilde{\mathcal{V}}_d(q)$ に拡張される。

## 3.2 ある観察とその帰結・関連問題

Veroense 双対卵形 $\mathcal{V}_d(q)$ のメンバーである $W$ の部分空間 $A(P)$ は、Veronese 写像を使わず、$W$ の基底のみを用いて直接表示することが出来る。

**補題 14** *([15, Lemma 6, Proposition 7])* $P = [\sum_{i\in I} t_i \mathrm{e}_i]$ に対して、$W$ の部分空間 $A(P)$ は次の基底を持つ：

$$\sum_{i\in I} t_i \mathrm{e}_{i0}, \sum_{i\in I} t_i \mathrm{e}_{i1}, \ldots, \sum_{i\in I} t_i \mathrm{e}_{id}, \quad \text{ここで}$$

$(i,j) \in J$ か $(i,j) \notin J$ *(このとき* $(j,i) \in J$*)* に応じて $\mathrm{e}_{ij} := \mathrm{e}_{(i,j)}$ または $\mathrm{e}_{(j,i)}$ と定める。

補題 14 と命題 13 を見比べると、これらの節における記号のもとで次が得られる。

**命題 15** ベクトル空間 $W$ からベクトル空間 $U$ への $GF(q)$-線形写像写像 $\rho$ を $\rho(\mathrm{e}_{(i,j)}) := e_{(i,j)}$ *(*$(i,j) \in J$*)* により定めると、$\rho$ は $W$ から $\mathrm{A}(\mathcal{T}_\sigma(K))$ の上への写像であって、$PG(V) \cong PG(d,q)$ のそれぞれの射影点 $P = [\sum_{i\in I} t_i \mathrm{e}_i]$ に対し、$d+1$ 次元ベクトル空間 $A(P)$ から $d+1$ 次元ベクトル空間 $T(\sum_{i\in I} t_i e_i)$ 上への線形同型写像を与える。

また $q$ が偶数のときには、$\tilde{\mathcal{V}}_d(q) \setminus \mathcal{V}_d(q)$ の唯一のメンバー $\{\sum_{i\in I} x_i^2 \mathrm{e}_{(i,i)} \mid x_i \in GF(q)\}$ は写像 $\rho$ により $\tilde{\mathcal{T}_\sigma(K)} \setminus \mathcal{T}_\sigma(K)$ の唯一のメンバー $T(\infty)$ に移される。

つまり、以下の意味で双対卵形 $\mathcal{T}_\sigma(K)$ は双対卵形 $\mathcal{V}_d(q)$ の商になっている。

**定義 16** $\mathcal{A}$ と $\overline{\mathcal{A}}$ は同一の係数体 $GF(q)$ 上の $d$ 次元の双対弧で、同一個数のメンバーから構成される *(*$|\mathcal{A}| = |\overline{\mathcal{A}}|$*)* ものとする。このとき、生成空間 $\mathrm{A}(\mathcal{A})$ から生成空間 $\mathrm{A}(\overline{\mathcal{A}})$ への $GF(q)$ 上の半線形写像 $\rho$ が存在して、$\rho$ は全射であり、$\mathcal{A}$ のそれぞれのメンバー $X$ に対して $\overline{\mathcal{A}}$ のメンバー $X'$ がただ一つ存在して $\rho$ の $X$ への制限は $X$ と $X'$ の間の射影空間としての同型を与えるとき、$\mathcal{A}$ は $\overline{\mathcal{A}}$ の被覆である、または $\overline{\mathcal{A}}$ は $\mathcal{A}$ の商であるという。

論文 [15, Proposition 13] で示されたように次の言い換えが出来る。$d$ 次元双対弧 $\mathcal{A}$ の生成空間 $\mathbf{A}(\mathcal{A})$ の部分空間 $N$ で条件

$$N \cap \langle X, Y \rangle = \{0\} \quad (\forall X \neq Y \in \mathcal{A})$$

を満たすものがあれば、自然な全射線形写像 $\rho : \mathbf{A}(\mathcal{A}) \to \mathbf{A}(\mathcal{A})/N$ に関して $\overline{\mathcal{A}} := \{X^\rho \mid X \in \mathcal{A}\}$ は $d$ 次元双対弧で $\mathcal{A}$ の商となり、その生成空間は $\mathbf{A}(\mathcal{A})/N$ である。逆に、任意の $\mathcal{A}$ の商 $\overline{\mathcal{A}}$ に対して上の条件を満たす $\mathbf{A}(\mathcal{A})$ の部分空間 $N$ が存在して $\overline{\mathcal{A}}$ はこの形に書ける。すなわち、与えられた高次元双対弧の商をすべて求めるには、上の条件を満たすような生成空間中の部分空間 $N$ を求めればよい。

$U = GF(q^{d+1}) \oplus GF(q^{d+1}) = K$ に対する谷口の卵形 $\mathcal{T}_\sigma(K)$ の生成空間の次元は $2(d+1)$ であり、これは生成空間の次元が $(d+1)(d+2)/2$ の Veronesean 卵形 $\mathcal{V}_d(q)$ により被覆されている。そこで、[15, Proposition 13] により、次がいえる。

**命題 17** $2(d+1) \leq l \leq (d+1)(d+2)/2$ を満たす任意の整数 $l$ に対して生成空間の次元が $l$ であるような $d$ 次元双対卵形で、$\mathcal{V}_d(q)$ の商でありかつ $\mathcal{T}_\sigma(U)$ の被覆であるものが存在する。

この結果は、論文 [15] における問い「$\mathcal{V}_d(q)$ の商構造の可能な生成次元をすべて決めよ」に殆ど完全な解答を与えている。ただ一つ解決されていないのは、$\mathcal{V}_d(q)$ が生成次元 $2d+1$ の商を持つか否かである。それに関連して $\mathcal{T}_\sigma(U)$ が生成次元 $2d+1$ の商を持つか否かが問題になる。先に注意したように、この問題は、$\mathcal{T}_\sigma(U)$ の生成空間中のある 1 次元部分空間 $N$ を見いだすことと同値であり、それは次のように完全な有限体上の算術問題の形に定式化できる。

**問題 1** $q$ を 2 のべき乗とする。$GF(q^{d+1})$ の任意の元 $\gamma, \delta$ の対 $(\gamma, \delta)$ に対して、次の関係を満たすような $x, \alpha, \beta \in GF(q^{d+1})$ で、条件「$\alpha \neq 0, \beta \neq 0$ で $\alpha/\beta \notin GF(q)$」を満たすものが存在するか？

$$\delta - (\beta^{1-\sigma}\gamma^\sigma + \beta^{\sigma-1}\gamma) \;=\; \left(\frac{x^\sigma}{\beta} - \frac{x}{\beta}\right)(\alpha\beta^\sigma - \alpha^\sigma\beta)$$

最後に、より一般的な問題を一つ提出して終わりとする。

**問題 2** $2d+1 \leq l \leq (d+1)(d+2)/2$ を満たす任意の整数 $l$ に対して生成空間が $GF(q)$ 上 $l$ 次元となるような $d$ 次元双対卵形ないしは超卵形で、単連結なもの（すなわち、自分自身以外の被覆を持たない）が存在するか？

# References


[1] M. Buratti and A. Del Fra, Semi-Boolean Steiner quadruple systems and dimensional dual hyperovals, Advances in Geometry 3 (2003), Special Volume, S245–S253.

[2] B. Cooperstein and J. Thas, On generalized $k$-arcs in $PG(2n,q)$, Ann. Combin. 5 (2001), 141–152.

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

[4] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals assosiated with Steiner systems, Europ. J. Combin. 26 (2005), 173–194.

[5] D. G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, Combinatorial Mathematics X, Springer Lecture Notes in Mathematics 1063 (1983), 217–229.

[6] D. G. Glynn, A condition for the existence of oval in PG(2,q), q even, Geom. Dedicata 32 (1989), 247–252.

[7] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Second Edition, Oxford Math. Monographs, Clarendon Press, Oxford, 1998.

[8] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40 (1999), 503–532.

[9] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AG^*$ geometries, Discrete Math. 255 (2002), 503–532.

[10] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with $q$ even, Europ. J. Combin. 26 (2005), 195–199.

[11] J. Thas and H. van Maldeghem, Characterizations of the finite quadric and Hermitian Veroneseans over finite fields, J. Geom. 76 (2003), 282–293.

[12] H. Taniguchi and S. Yoshiara, On the dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$, Innovations in Incidence Geometry, 1 (2005), 197–219.

[13] S. Yoshiara, A family of $d$-dimensional dual hyperovals in $PG(2d+1,2)$, Europ. J. Combin. 20 (1999), 589–603.

[14] S.Yoshiara, Segre の定理, 2003 年秋学期講義用ノート（4 年、修士向け）

[15] S. Yoshiara, Ambient spaces of dimensional dual arcs, J. Alg. Combin. 19 (2004), 5–23.

[16] S. Yoshiara, Some remarks on dimensional dual hyperovals of polar type, to appear in Simon Steven. (The proceeding of La Roche Conference on Incidence Geometry, May, 2004.)

[17] S. Yoshiara, 極空間中の双対弧 (Dimensional dual arcs of polar type), 第 2 1 回代数的組合せ論シンポジウム報告集 (June 28–30, 2004, Shinhu Univ., Matsumoto), p.57–68, October, 2004.

[18] S. Yoshiara, Dimensional dual arcs–a survey, to appear in the proceeding of the Pingree Park conference on Groups, Geometries and Computations, September, 2004.

[19] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals, submitted for publication, 2005.

# Examples of dimensional dual hyperovals of polar type

南部 奈緒
東京女子大学大学院
理学研究科 博士前期課程 2 年
naonambu@rf7.so-net.ne.jp

October 9, 2005

## 1 polar type の dual hyperovals

**Definition 1** $n$ と $d$ は $1 \leq d \leq n$ を満たす整数とし、$q$ はある素数のべき乗とする。また、$U$ を有限体 $GF(q)$ 上の $n+1$ 次元ベクトル空間とする。$U$ の幾つかの $d+1$ 次元部分空間のなす集合 $\mathcal{A}$ が次の 3 条件 *(DA1), (DA2), (DA3)* をすべて満たすとき、$\mathcal{A}$ を **$d$-dimensional dual arc)** （*$d$-(射影)次元双対弧*）と呼び、$U$ を $\mathcal{A}$ の **ambient space** *(生成空間)* という。

*(1)* $\mathcal{A}$ の任意の相異なる二つのメンバー $X$ と $Y$ に対して、それらの共通部分 $X \cap Y$ は $U$ の 1 次元の部分空間である。

*(2)* $\mathcal{A}$ の任意の相異なる 3 つのメンバー $X, Y, Z$ に対して、それらの共通部分は零空間である: $X \cap Y \cap Z = \{0\}$.

*(3)* $\mathcal{A}$ のメンバーの全体が生成する $U$ の部分空間は $U$ に一致する: $\langle X \mid X \in \mathcal{A} \rangle = U$.

$\mathcal{A}$ が $d$ 次元双対弧で $U$ がその生成空間であることを、「$\mathcal{A}$ は生成空間 $U$ 中の双対弧」とも表現する。また次元 $d$ を明示しないときには、高次元の双対弧ともいう。

$\mathcal{A}$ を生成空間 $U$ 中の $d$ 次元の双対弧とする。このとき、双対弧 $\mathcal{A}$ に含まれるメンバーの数は高々 $((q^{d+1}-1)/(q-1))+1$ であることが示される:

$$|\mathcal{A}| \leq \frac{q^{d+1}-1}{q-1} + 1. \tag{1}$$

**Definition 2** 不等式 *(1)* において等号が成立する場合に、双対弧 $\mathcal{A}$ のことを **dual hyperoval** *(双対超卵形)* と呼ぶ。

**Definition 3** $\mathcal{A}$ を生成空間 $U$ 中の $d$ 次元双対弧とする。ベクトル空間 $U$ 上の非特異な計量 $f$ (*symplectic form*、*unitary form*、*orthogonal form* のいずれか) が存在し、$\mathcal{A}$ のそれぞれのメンバーが $f$ に関して極大全等方部分空間 *(maximal totally isotropic subspace)* になるとき、$\mathcal{A}$ を計量 $f$ に関して polar type であるという。

**Remark 4** $\mathcal{A}$ の *ambient space* の次元 $n+1$ とそのメンバーの次元 $d+1$ の関係について次のいずれかが成立する。

*(1)* $f$ が *symplefic form* $\Rightarrow$ $n+1 = even$ かつ $(n+1)/2 = d+1$

*(2)* $f$ が *unitary form* $\Rightarrow$ $\lfloor (n+1)/2 \rfloor = d+1$ かつ $q$ は平方数

*(3)* $f$ が *orthogonal form* $\Rightarrow$

| | | | | | | |
|---|---|---|---|---|---|---|
| $f$: *neutral type* のとき | $n+1$: | *odd* | かつ | $d$ | $=$ | $\frac{n}{2}$ |
| $f$: *plus type* のとき | $n+1$: | *even* | かつ | $d+1$ | $=$ | $\frac{n+1}{2}$ |
| $f$: *minus type* のとき | $n+1$: | *odd* | かつ | $d+1$ | $=$ | $\frac{n+1}{2}-1$ |

**Examples 5** *Dual hyperoval* として次の 4 つの無限系列が知られている。$n+1$ は生成空間の次元を示す。詳細は本報告集中の解説 *[6]* を参照せよ。

*(1) Veronese* 写像を使った構成例：*(H. Van Maldeghem and J. Thas, 2003 [2])*
$n+1 = (d+1)(d+2)/2$ $(q = 2$ のべき$)$

*(2)* 特性関数を使った構成例：*(M. Buratti and A. Del Fra [1])*
$n+1 = (d+1)(d+2)/2$ $(q = 2)$

*(3)* $GF(2^{d+1})$ 上のある多項式を用いた構成例 $\mathcal{S}^{d+1}_{\sigma,\phi}$：*(Yoshiara 1999 [4])*
$n+1 = 2(d+1)$ $(q{=}2)$

*(4)* $GF(q)$ 上ある多項式を用いた構成例 $\tilde{T}_\sigma(K)$：*(H. Taniguchi 2005 [3])*
$n$ と $d$ は様々な関係 $(q{=}2$ のべき$)$

**Remark 6** 先の *Remark 4* より無限系列 *(1)* と *(2)* は、*ambient space* の次元が大きすぎるので *polar type* になりえない。よって *polar type* になる可能性があるものは、無限系列 *(3)* と *(4)* のみである。

無限系列 (4) に関しては次が知られている。

**Proposition 7** $\tilde{T}_\sigma(K)$ は、*polar type* になりえない。*(Yoshiara 2004 [5])*

従って polar type になり得る無限系列は (4) のみであり、次が問題となる。

**Problem 8** $\mathcal{S}^{d+1}_{\sigma,\phi}$ は、いつ *polar type* になるか？

ここで、$S^{d+1}_{\sigma,\phi}$ の正確な定義を与えよう。

**Definition 9** $GF(q)$ 係数の多項式 $\phi(X)$ は、次の写像（代入写像）が $GF(q)$ 上の全単射であるときに、**置換多項式**と呼ばれる。

$$\phi : GF(q) \ni x \mapsto \phi(x) \in GF(q).$$

$GF(q)$ 係数の多項式 $\phi(X)$ が **o-多項式**であるとは、次の条件がすべて満たされることである。

*(0)* $\phi(0) = 0, \phi(1) = 1.$

*(1)* $\phi(X)$ は置換多項式である。

*(2)* $GF(q)$ の元 $s$ に対して、$GF(q)$ 係数の多項式 $\phi_s(X)$ を次の式で定義する。このとき、すべての $s \in GF(q)$ に対して $\phi_s(X)$ は置換多項式である。

$$\phi_s(X) := \frac{\phi(X+s) - \phi(s)}{X}$$

**Examples 10** *o*-多項式 $\phi$ が単項式で与えられているとき、$\phi$ を **monomial** とよぶ。知られている *monomial o-polynomial* の無限系列は、次のいずれかの多項式と射影同値である。*($q = 2^{d+1}$)* (*[6]* の解説参照)

*(1)* ガロア群に入るもの
$\phi(X) = X^{2^m}$, $1 \le m \le d$, $(m, d+1) = 1$
特に、逆関数に対応するもの $\phi(X) = X^{q-2}$ は $X^2$ と射影同値である。

*(2)* *Segre* 多項式
偶数 $d$ に対する $\phi(X) = X^6$

*(3)* *Glynn* の *o-polynomial* ($d$ が *even* のときのみ定義される)

*(i)* $d = 4m - 2$ $(m \ge 1)$ のとき
$\phi(X) = X^{2^{2m}+2^m}, X^{3\cdot 2^{2m}+4}$

*(ii)* $d = 4m$ $(m \ge 1)$ のとき
$\phi(X) = X^{2^{3m+1}+2^{2m+1}}, X^{3\cdot 2^{2m+1}+4}$

**Remark 11** 一般に *dual hyperoval* $S, S'$ が同型であるとき、$S$ が *polar type* であれば $S'$ も *polar type* である。しかし $S^{d+1}_{\sigma,\phi}$ と $S^{d+1}_{\sigma',\phi'}$ が同型であるのは $(\sigma, \phi) = (\sigma', \phi')$ または $\sigma\sigma' = id_{GF(q)} = \phi\phi'$ のときしかないので、この注意を用いる機会はあまりない。

一方、$S^{d+1}_{\sigma,\phi}$ が *polar type* であったとしても、$\phi(X)$ と射影同値な *o-polynomial* $\phi'(X)$ に対する $S^{d+1}_{\sigma,\phi'}$ が *polar type* であるとはいえない。従って、与えられた $S^{d+1}_{\sigma,\phi}$ が *polar type* であるかどうかの判定は、*o*-多項式 $\phi(X)$ の形に非常に大きく依存する。

例えば、$\phi(X) = X^2$ に対する $S^{d+1}_{\sigma,\phi}$ が *polar type* であったとしても、$\phi'(X) = X^{q-2}$ に対する $S^{d+1}_{\sigma,\phi'}$ が *polar type* であるとは限らない。

**Definition 12** $\mathcal{S}^{d+1}_{\sigma,\phi}$
$d$ を 2 以上の整数とし、$q=2^{d+1}$ とする。また $\sigma$ をガロア群 $Gal(GF(q)/GF(2))$ の生成元とし、$\phi$ を $GF(q)$ 係数の $o$-多項式とする。

$$V := GF(q) \oplus GF(q) = \{(x,y) \mid x,y \in GF(q)\}$$

とおき、$V$ を $GF(q)$ 上の $2(d+1)$ 次元ベクトル空間とみる。
$\forall t \in GF(q)$ に対し、$V$ の $(d+1)$ 次元部分空間 $X(t)$ を

$$X(t) := \{(x, x^\sigma t + xt^\phi) \mid x \in GF(q)\}$$

により定義する。これらの部分空間を集めて

$$\mathcal{S}^{d+1}_{\sigma,\phi} := \{X(t) \mid t \in GF(q)\}$$

とおく。

**Proposition 13** $\sigma \cdot \phi \neq id_{GF(q)}$ ならば $\mathcal{S}^{d+1}_{\sigma,\phi}$ は $GF(2)$ 上 $d$ 次元 *dual hyperoval* で、その *ambient space* は $V$ に一致する。

$\mathcal{S}^{d+1}_{\sigma,\phi}$ の ambient space $V$ は $GF(2)$ 上のベクトル空間である。従って、もし $V$ 上の形式 $f$ に関して $\mathcal{S}^{d+1}_{\sigma,\phi}$ が polar type であれば、$f$ は unitary form ではない。また $f$ が orthogonal form であれば plus type であり、それに関連した symplectic form $s$ $(s(x,y) = f(x+y) + f(x) + f(y), x,y \in V)$ に関して $\mathcal{S}^{d+1}_{\sigma,\phi}$ のメンバーはすべて totally isotropic である。従って次がいえる。

**Remark 14** $\mathcal{S}^{d+1}_{\sigma,\phi}$ が $f$ に関して *polar type* ならば、$f$ は *symplectic form* としてよい。

また $\phi$ がガロア群 $Gal(GF(q)/GF(2))$ の元であるときは、吉荒が研究しており、任意の偶数 $d$ に対し、$d$ 次元の dual hyperovals で polar type のものが存在することが示されている。より詳しくいうと

**Proposition 15** $\phi \in Gal(GF(q)/GF(2))$ ならば、$\mathcal{S}^{d+1}_{\sigma,\phi}$ が *polar type* $\Leftrightarrow \sigma = \phi^{-2}$
また $\sigma = \phi^{-2}$ のとき $f((x,y),(u,v)) = Tr(xv^\phi + uy^\phi)$ とすれば、$f$ は *symplectic form* で、$\mathcal{S}^{d+1}_{\sigma,\phi}$ は $f$ に関して *polar type* である。

従って、次が問題として残されている。

**Problem 16** $\mathcal{S}^{d+1}_{\sigma,\phi}$, $\sigma \notin Gal(GF(q)/GF(2))$ が、*symplectic form* $f$ に関して *polar type* となるのは、どんなときか？

## 2 主結果とその証明の概要

この論文の主結果は、次の通りである。

**Theorem 17** $\sigma \in Gal(GF(q)/GF(2)))$, $\phi$ は *o-polynomial* とする。

*(i)* $\phi(X) = X^{q-2}$ のとき
$S^{d+1}_{\sigma,\phi}$ は *polar type* になりえない。

*(ii)* *d: even* で $\phi(X) = X^6$ のとき
$S^{d+1}_{\sigma,\phi}$ は *polar type* になりえない。

愛媛での講演時においては、$d = 2, 4, 6$ のときに対する (ii) の場合が未確認であったが、その後これらはすべて polar type になりえないことが示された。従って、主定理は上の形に述べられる。

**Proposition 18** $S^{d+1}_{\sigma,\phi}$ が *symplectic form* $f$ に関して *polar type* であり、$\sigma(x) = x^{2^m}$, $\phi(x) = x^N$ $(\forall x \in GF(q))$ とする。このとき $\gamma := (1-\phi\sigma)\cdot(\phi-1)^{-1}$ とおくと、
$\exists c \in \mathbf{Z}, \quad 0 \le c \le d$ s.t. $\gamma(x) = x^{2^c}$ $(\forall x \in GF(q))$

**Cororally 19** $1 - 2^m N \equiv 2^c(N-1)$ *(mod* $2^{d+1}-1$ *)*

これに $N = q-2$ を適用すると Theorem 17(1) が得られる。しかし $N = 6$ を適用しても、以下の解が得られ、矛盾がえられない。

**Fact 20** $S^{d+1}_{\sigma,\phi}$, $\phi(x) = x^6$ が *polar type* のとき、*Cororally 19* の合同式の唯一の解は、$m = d-3$, $c = d-2$ つまり $\sigma(x) = x^{2^{d-3}}$, $\gamma(x) = x^{2^{d-2}}$. よって $\sigma^{-1}(x) = x^{16}$, $\gamma^{-1}(x) = x^8$ $(\forall x \in GF(q))$

**Proposition 21** $S^{d+1}_{\sigma,\phi}$ が *symplectic form* $f$ に関して *polar type*, $\gamma := (1-\phi\sigma)\cdot(\phi-1)^{-1}$ とする。また $\phi$ は *monomial* とする。
$\forall t \in GF(q)\backslash GF(2)$ に対し

$$\phi_t(u) := \frac{\phi(u+t)+\phi(t)}{u} \quad = \quad 1 \tag{2}$$

を満たす $u \in GF(q)^\times$ をとる。
このとき

$$\left(\frac{t}{u}\right)^{\sigma^{-1}} + \left(\frac{t^\phi}{u}\right) = \left(t^\phi + t\right)^{\gamma^{-1}} \tag{3}$$

Fact 20 の $\sigma^{-1}(x)=x^{16}, \gamma^{-1}(x)=x^8$ $(\forall x \in GF(q))$ を Proposition の (2), (3) に代入すると

$$\phi_t(u)=\frac{(u+t)^6+(t)^6}{u} = 1$$
$$\left(\frac{t}{u}\right)^{16}+\left(\frac{t^6}{u}\right) = \left(t^6+t\right)^8$$

これから $t$ を消去すると、かなり大変な計算により次を得る:

$$u^{68}+u^{25}+u^{15}+u^{10}+u^8+1=0.$$

つまり

$$\mathcal{U} := \{u \in GF(q) \mid \exists t \in GF(q)\backslash GF(2) \ \ s.t. \ \ \phi_t(u)=1\}$$

とおくと $\mathcal{U}$ は 68 次の $GF(2)$ 上の多項式の解に対応するので

$$|\mathcal{U}| \leq 68.$$

一方 $|\mathcal{U}| \geq q/2-5$ であることが、次のステップを踏んで示せる。

**Step 1**

$$\mathcal{Y} := \{u^{-5} \mid u \in \mathcal{U}\}$$

とおくと $|\mathcal{U}|=|\mathcal{Y}|$

**Step 2** $\mathcal{Y}$ は次の集合に一致する:

$$\{y \in GF(q)^\times \mid Tr(y)=1\}\backslash\{u^{-5} \mid u \in GF(q),\ u^5+u^3+u+1=0\}$$

ここで $Tr=Tr_{GF(q)/GF(2)}$.

**Final Step** $Tr$ は、$GF(q)$ から $GF(2)$ への全射 $GF(2)$-線形写像なので $\{y \in GF(q) \mid Tr(y)=1\}=GF(q)\backslash Ker(Tr)$ は $q/2$ 個の元からなる。また集合 $\{u^{-5} \mid u \in GF(q), u^5+u^3+u+1=0\}$ の元は高々 5 個の元からなる。従って $|\mathcal{U}|=|\mathcal{Y}| \leq (q/2)-5$.

以上より

$$q/2-5 \leq |\mathcal{U}| \leq 68.$$

$q=2^{d+1}$ なので $d \leq 6$ が得られる。そこで $\mathcal{S}^{d+1}_{\sigma,X^6}$ が polar type になるのは $d \leq 6$ に限る。$d=2,4,6$ に対しては特別の考察を行うことにより、$\mathcal{S}^{d+1}_{\sigma,X^6}$ が polar type にならないことが示せる。

# References


[1] M. Buratti and A. Del Fra, Semi-Booln Steiner quadruple systems and dimensional dual hyperovals, Advances in Geometry 3 (2003), Special Volume, S245–S253.

[2] J. Thas and H. van Maldeghem, Characterizations of the finite quadric and Hermitian Veroneseans over finite fields, J. Geom. 76 (2003), 282-293.

[3] H. Taniguchi, A family of dual hyperovals over GF(q) with q even, Europ. J. Combin 26 (2005), 195–199.

[4] S. Yoshiara, A family of d-dimensional dual hyperovals in PG(2d+1,2), Europ. J. Combin. 20 (1999), 589–603.

[5] S. Yoshiara, Some remarks on dimensional dual hyperovals of polar type, to appear in Simon Steven (the proceeding of La Roche Conference on Incidence Geometry, May, 2004)

[6] 吉荒 聡, 高次元の双対弧–平面上の二次曲線の高次元化, 本報告集

# On dimensional dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$

詫間電波高専
Hiroaki Taniguchi(谷口浩朗)

## 1 はじめに

monomial o-polynomial から構成された 2d+1 次元射影空間内における 2 元体上の d 次元 dual hyperoval について報告する。詳しい証明等は [1] を見てほしい.

高次元の dual hyperoval の定義は最初に Hyubrechts と Pasini によって与えられた.

**定義 1 (Hyubrechts and Pasini, 1999).** $q$ 元体 $GF(q)$ 上の $N$ 次元射影空間 $PG(N,q)$ 内における $d$-次元双対超卵形 *(dimensional dual hyperoval)* $S$ は，以下の性質をみたす $d$-次元部分空間の集合として定義される.

1. $S$ は $q^d+q^{d-1}+\cdots+q+2$ 個の $d$-次元部分空間よりなる集合であり,
2. $S$ の要素であるどの 2 つの $d$-次元部分空間も 1 点で交わり,
3. $S$ のどの 3 つの $d$-次元部分空間も共有点を持たず,
4. $S$ の $d$-次元部分空間全体は, $PG(N,q)$ を生成する.

また，o-polynomial は以下のように定義される.

**定義 2 (o-polynomial).** $\phi(x)\in GF(q)[x]$ が *a permutation polynomial* とは, $GF(q)\ni x\mapsto\phi(x)\in GF(q)$ が $GF(q)$ の *permutation* であることとする.
また, *permutation polynomial* $\phi(x)$ が *o-polynomial* であるとは,

1. $\phi(0)=0$ かつ $\phi(1)=1$ であり,
2. $\phi_s(x):=(\phi(s+x)-\phi(s))/x$ ($\phi_s(0)=0$ とする) が すべての $s\in GF(q)$ にたいして成り立つこととする.

$o$-polynomial の研究は，以下の事実 1 によって，古典的な（射影平面上の）hyperoval の研究と深く関わりがある．1950 年代から今まで種々の $o$-polynomial が発見されている．

**事実 1 (Segre).** 射影平面 $PG(2,q)$ の，どのような *hyperoval* も，適当な射影変換および適当な *o-polynomial* $\phi(x)$ によって

$$\{(1,x,\phi(x)) \mid x \in GF(q)\} \cup \{(0,1,0),(0,0,1)\}$$

と表せる．

高次元の dual hyperoval においても，$o$-polynomial を用いた構成が以下のように可能であることが，[2] において発見された．この $o$-polynomial を用いた dual hyperoval のうち，$o$-polynomial が単項式の場合についての研究が，この小論の主題である．

**事実 2 (Yoshiara).** $\phi(x)$ を $GF(q)[x]$ 上の *o-polynomial* とし $\sigma$ を $Gal(GF(2^{d+1}))$ の生成元とする．

$t \in GF(q)$ に対して，$GF(q) \times GF(q)$ 内で

$$X(t) = \{\ (x, x^\sigma t + x\phi(t)) \mid x \in GF(q)\ \}$$

と定義する．このとき，

$$\mathcal{S} := \{\ X(t) - \{(0,0)\} \mid t \in GF(q)\ \}$$

は 射影空間 $PG(2d+1,2) = PG(GF(q) \times GF(q))$ における $d$ 次元 *dual hyperoval* である．

この dual hyperoval $S$ を dimensional dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\phi}$ ということにする．

この小論の中心的な結果は定理 1 と定理 2 であるが，ambient space の次元については，以下のように，特別な場合をのぞいて $2d+1$ になることがわかる．

**命題 1.** *$\sigma\phi = id$ の場合に限り，ambient space の次元は $2d$．それ以外は ambient space の次元は $2d+1$ である．*

*Proof.* 以下が成り立つことに注意する．

$$X(0) \cap X(t) = (t^{(\phi-1)/(\sigma-1)}, 0) = (\phi_0(t)^{1/(\sigma-1)}, 0). \quad (1)$$

$$X(s) \cap X(t) = \left( (\frac{s^\phi + t^\phi}{s+t})^{1/(\sigma-1)}, (\frac{s^\phi + t^\phi}{s+t})^{1/(\sigma-1)} (\frac{s^\phi t + t^\phi s}{s+t}) \right). \quad (2)$$

さて ambient space $U = \langle X(t) \mid t \in GF(q)\rangle$ を決定したい．$t \in GF(q)^\times$ にたいし，$A(t) := \{x^\sigma t + xt^\phi | x \in GF(q)\}$ とおく．このとき $A(t) = \{x \in GF(q) \mid Tr(t^{(1-\phi\sigma)/(\sigma-1)}x) = 0\}$ が，すべての $t \in GF(q)^\times$ にたいして成り立つことがわかる．さて $A := \langle A(t) \mid t \in GF(q)^\times\rangle$ とおいて，すべての $A(t)$ を含む $GF(q)$ の部分空間 $A$ を考える．$\langle X(0), X(t)\rangle = \{(x,y) \mid x \in GF(q), y \in A(t)\}$ なので，$U = \{(x,y) \mid x \in GF(q), y \in A\}$ である．

また，$A(1) = \{x \in GF(q) \mid Tr(x) = 0\}$ は $GF(q)$ の超平面なので，$A = GF(q)$ かまたは $A = A(1)$ のどちらかが成り立つ．つまり $U = GF(q)\times GF(q)$ または $U = \{(x,y) \mid Tr(y) = 0\}$ のどちらかである．

$U = \{(x,y) \mid Tr(y) = 0\}$ と仮定すると $A = A(1) = A(t)$ がすべての $t \in GF(q)^\times$ に対して成り立つことになる．$GF(q)$ の超平面は，(ある $a \in GF(q)^\times$ に対して，) $GF(2)$-線形写像 $x \mapsto Tr(ax)$ の Kernel として表せることに注意すると，$t^{(1-\phi\sigma)/(\sigma-1)} = 1$, つまり $t^{\phi\sigma} = t$ がすべての $t \in GF(q)^\times$ に対して成り立つことになる．つまり $\phi\sigma = id$ となる．

逆にもし $\phi = \sigma^{-1}$ が成り立つとすると，$A(t) = A(1)$ が すべての $t \in GF(q)^\times$ に対して成り立つので，$A = A(1)$ つまり $U = \{(x,y) \mid Tr(y) = 0\}$ であることになる． □

## 2 $S^{d+1}_{\sigma,\phi}$ の同型性

この節では，o-polynomial が単項式である場合を考える．つまり $\phi(t) = t^M$, $\phi'(t) = t^{M'}$ と仮定する．また，$\sigma$, $\sigma'$ を $Gal(GF(2^{d+1})/GF(2))$ の生成元とする．

**定理 1.** *o-polynomial が単項式である場合，dual hyperoval $S^{d+1}_{\sigma,\phi}$ と $S^{d+1}_{\sigma',\phi'}$ が同型であるための必要十分条件は*

1. $\sigma = \sigma'$, $\phi = \phi'$ または
2. $\sigma\sigma' = id$, $\phi\phi' = id$

である．

**Remark 1.** *o-polynomial $\phi(x) = x^N$ を用いて*

$$\{(1, x, \phi(x)) \mid x \in GF(q)\} \cup \{(0,1,0), (0,0,1)\}$$

*と表される (射影平面上の古典的な)hyperoval と同型な (射影平面上の古典的な)hyperoval を定める o-多項式は*

$$x^N, x^{1/N}, x^{1-N}, x^{1/1-N}, x^{N/N-1}, x^{(N-1)/N}$$

の6個 (同じものがあるかもしれない!)であるが，定理 1. によると，*dimensional dual hyperoval* $S^{d+1}_{\sigma',\phi'}$ が *dimensional dual hyperoval* $S^{d+1}_{\sigma,\phi}$ と同型である場合は

$$(\sigma',\phi') = (\sigma, t^N) \text{ または } \quad (\sigma',\phi') = (\sigma^{-1}, t^{1/N})$$

の場合だけであり，古典的な *hyperoval* の場合と比べて，分類が細かくなっていると考えられる

[定理 1. の証明の概略] (If part の証明)
1. の場合は明らか．2. の場合　$\tau : (x,y) \mapsto (x, y^{\sigma'})$ により $S^{d+1}_{\sigma,\phi}$ は $S^{d+1}_{\sigma',\phi'}$ と同型になることが確かめられる．
(以下 Only if part の証明を行う)

**Remark 2.** $S^{d+1}_{\sigma,\phi}$ は，$b \in GF(q)^\times$ に対して

$$m_b : (x,y) \mapsto (bx, b^{(\sigma\phi-1)/(\phi-1)}y)$$

で定められる，$X(t)$ を $X(b^{(\sigma-1)/(\phi-1)}t)$ に移す同型写像を持つ．
$M := \{m_b | b \in GF(q)^\times\}$ とおくと，$M$ は $Aut(S^{d+1}_{\sigma,\phi})$ の部分群であり，$S^{d+1}_{\sigma,\phi} - \{X(0)\}$ に可移に作用する．

以下　$S^{d+1}_{\sigma,\phi}$ から $S^{d+1}_{\sigma',\phi'}$ への同型写像 $\tau$ があると仮定する．このとき次節の定理 2. の結果を援用すると $\tau(X(0)) = X(0)$ と仮定することが出来る．(Remark 4 参照.) ここに $X(0) := \{(x,0) | x \in GF(q)\}$ である．(定理 2 を援用しない初等的な方法もあります.)
さらにまた，$X(\infty) := \{(0,y) | y \in GF(q)\}$ とするとき，次の補題 1 の系を用いて，$\tau(X(\infty)) = X(\infty)$ と仮定することが出来る
つまり $\tau$ を行列 $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ で表すことが出来る．
以下の補題 1 等の証明は省略します．

**補題 1.** $V$ を $M$ の作用で不変な $d+1$-次元部分ベクトル空間とし，すべての $X(t)$ にたいし，$V \cap X(t) = \emptyset$ と仮定する．このとき $V = \{(0,y) | y \in GF(q)\}$ または $V = \{(x, cx^{(\sigma\phi-1)/(\phi-1)}) \mid x \in GF(q)\}$.

**定義 3 (Glynn).** $\ll$ を整数 $0 \le b, c \le q-1$ において次の規則によって定められた *partial ordering* とする．
$b = \sum_{i=0}^{d} b_i 2^i$, $c = \sum_{i=0}^{d} c_i 2^i$, ここに $0 \le b_i, c_i \le 1$, $i = 0, \ldots, d$ のとき，$b \ll c$ とは 「すべての $i$ について $b_i \le c_i$ がなり立つ」ことをいう．

**事実 3 (Theorem A of Glynn).** $x^m$ が *o-polyn* である必要十分条件は，$k \in \{1, \ldots, q-1\}$ に対して $k \not\equiv mk$ がなり立つことである． （ここに $mk$ は *modulo* $q-1$ で考える.）

**系 1.** 上記補題の条件においては，
$V = \{(0, y) | y \in GF(q)\}$ の場合しかあり得ない.

**補題 2.** $X(0)$ を $X(0)$ に移す，$S^{d+1}_{\sigma,\phi}$ から $S^{d+1}_{\sigma',\phi'}$ への同型写像が存在するとする． このとき，同型 $\tau$ で $M \subset Aut(S^{d+1}_{\sigma,\phi})$ を $M \subset Aut(S^{d+1}_{\sigma',\phi'})$ に移すものが存在する.

この補題 2 は Kantor の idea によるもので，証明は [2] をご覧ください.

巡回群 $M \subset Aut(S^{d+1}_{\sigma,\phi})$ の生成元を $\begin{pmatrix} X & 0 \\ 0 & X^{(\sigma\phi-1)/(\phi-1)} \end{pmatrix}$，また $M \subset Aut(S^{d+1}_{\sigma',\phi'})$ の生成元を $\begin{pmatrix} X & 0 \\ 0 & X^{(\sigma'\phi'-1)/(\phi'-1)} \end{pmatrix}$ と表すと，補題 2 によって以下の 1 と 2 が成り立つことがわかる.

1. $A = I$ (identity matrix) と仮定して良い.
2. $B^{-1} X^{(\sigma\phi-1)/(\phi-1)} B = X^{(\sigma'\phi'-1)/(\phi'-1)}$ がなり立つ.

このとき，まず次のことが成り立つ.

**系 2.** 2. により $\mu \in Aut(GF(q))$ および，ある $s$ に対して $D \in GL_{(d+1)/s}(2^s)$ が存在して，

$$B = D\mu$$

と表せることが分かる.

この系の証明も省略します.

さて，$D$ は $GF(2)$-線形写像なので，[3] により，まず

$$Dy \equiv b_0 y + b_1 y^{2^s} + b_2 y^{2^{2s}} + \cdots + b_{r-1} y^{2^{(r-1)s}} \tag{3}$$

と表しておく.

1 . と系 2 により $\tau(x, x^{2^h} t + x t^m) = (x, D(x^{2^h} t + x t^m)^{2^a})$ と表せるので，$t = 1$ とすることにより

$$D(x^{2^h} + x)^{2^a} = x^{2^k} + x \tag{4}$$

とできる.

ここで，先ほどの 1. 2. および (3) より

$$b_0(x^{2^h}+x)^{2^a}+\cdots+b_{r-1}(x^{2^h}+x)^{2^{((r-1)a+a)}} \equiv x^{2^k}+x.$$

が成り立つ.

よって，ある $i$ に対して

$$D((x^{2^h}+x)^{2^a}) \equiv (x^{2^h}+x)^{2^{(a+is)}} \pmod{x^q-x}$$

がなり立つことが分かる.

結局 $x^{2^{h+a+is}}+x^{2^{a+is}} \equiv x^{2^k}+x$ となり，(a) $x^{2^{h+a+is}} \equiv x^{2^k}$ かつ $x^{2^{a+is}} \equiv x$, または (b) $x^{2^{h+a+is}} \equiv x$ かつ $x^{2^{a+is}} \equiv x^{2^k}$ が結論される.

(a) より $a+is \equiv 0 \pmod{d+1}$ かつ $h=k$. (b) より $h+k=d+1$ かつ $a+is \equiv k$ がわかる.

さて，先ほどの 2. より

$$(X^{(2^hm-1)/(m-1)})^{2^{(a+is)}} = X^{(2^kn-1)/(n-1)}$$

なので

$$(2^hm-1)2^{a+is}(n-1) \equiv (2^kn-1)(m-1)$$

となる.

(a) より $(m-n)(2^k-1) \equiv 0 \pmod{2^{d+1}-1}$ であり，$m=n$ となりさらに $k=h$ となる. この場合が $\sigma=\sigma'$ かつ $\phi=\phi'$ である.

(b) の場合 $(mn-1)(2^k-1) \equiv 0 \pmod{2^{d+1}-1}$ となり $mn \equiv 1 \pmod{2^{d+1}-1}$ さらに $h+k=d+1$ となる. この場合 $\sigma\sigma'=id$ かつ $\phi\phi'=id$ である.

## 3 $S^{d+1}_{\sigma,\phi}$ の自己同型群 $G$

この節では，$\phi(x)$ が単項式の場合の $S^{d+1}_{\sigma,\phi}$ の自己同型群 $G$ についての結果を示す.

**定理 2.** *1.* $\phi \in Gal(GF(q)/GF(2))$ であるとき

*(a)* $q=2^3$ の場合 $G \cong Z_q : GL_3(2)$

*(b)* 上記以外 $G \cong Z_q : (Z_{q-1} : Z_{d+1})$.

*2.* $\phi \notin Gal(GF(q)/GF(2))$ のとき

(a) $q=2^3$ の場合 $G \cong GL_3(2)$

(b) 上記以外　$G \cong Z_{q-1} : Z_{d+1}$

**Remark 3.** $\mathcal{S}^{d+1}_{\sigma,\phi}$ は以下の自己同型群 $M$, $F$ を含んでいる．ここで，$M := \{m_b \mid b \in GF(q)^\times\}$，　ここで $m_b$ とは，$b \in GF(q)^\times$ に対して定まる写像

$$m_b : (x,y) \mapsto (bx, b^{(\sigma\phi-1)/(\phi-1)}y)$$

のことである．$X(t)^{m_b} = X(b^{(\sigma-1)/(\phi-1)}t)$ となることに注意する．

また，$F := \{f_\theta \mid \theta \in Gal(GF(q)/GF(2))\}$，ここで $f_\theta$ とは $\theta \in Gal(GF(q)/GF(2))$ に対して定まる写像

$$f_\theta : (x,y) \mapsto (x^\theta, y^\theta)$$

のことである．$X(t)^{f_\theta} = X(t^\theta)$ となることに注意する．

さて $|M| = q-1$, $|F| = d+1$ でありさらに $MF \cong Z_{q-1} : Z_{d+1}$ となっていることに注意する．結局，$\phi \notin Gal(GF(q)/GF(2))$ かつ $q \neq 2^3$ のときは，自己同型群 $G$ は $MF$ に他ならない．しかしこの証明は (この稿では省略するが，) 決してやさしくはない．

また，$\phi \in Gal(GF(q)/GF(2))$ であれば，自己同型群 $G$ はさらに，$a \in GF(q)$ に対して，

$$t_a : (x,y) \mapsto (x, x^\sigma a + xa^\phi + y)$$

$X(t)^{t_a} = X(t+a)$ となる *Translation* をふくむ．ここに $|T| = |\{t_a \mid a \in GF(a)\}| = q$ である．結局，$\phi \in Gal(GF(q)/GF(2))$ かつ $q \neq 2^3$ であるときは，自己同型群 $G$ は $T : M : F$ に他ならない．

$q = 2^3$ の場合は，$(1,0)^v = (1,0)$, $(\eta,0)^v = (\eta^2,0)$, $(\eta^2,0)^v = (\eta,0)$ $(0,1)^v = (0,1)$, $(0,\eta)^v = (\eta+\eta^2,\eta)$, $(0,\eta^2)^v = (\eta^2,\eta+\eta^2)$, (ただし $\eta^3 = \eta+1$)，で定義される $GF(q)$ の *involutive* な *GF(2)*-線形写像 $v$ によって

$X(\eta^2)^v = X(\eta^4)$, $X(\eta^4)^v = X(\eta^2)$ $X(\eta^3)^v = X(\eta^6)$, $X(\eta^6)^v = X(\eta^3)$ $X(0)^v = X(0)$, $X(1)^v = X(1)$,$X(\eta)^v = X(\eta)$, $X(\eta^5)^v = X(\eta^5)$, として，*dual hyperoval* の *involution* が定まる．

$\phi \notin Gal(GF(q)/GF(2))$ の場合は $G$ は $MF$ および *involution* $v$ を含むので $G \cong GL_3(2)$ となる．同様，$\phi \in Gal(GF(q)/GF(2))$ の場合には，自己同型群 $G$ はさらに，$G \cong T : GL_3(2)$ となるのである．

**Remark 4.** $\phi \notin Gal(GF(q)/GF(2))$ の場合，自己同型群 $G$ によって $X(0)$ は固定される．

## 4 $S^{d+1}_{\sigma,\phi}$ と同型になる dual hyperoval について

**命題 2.** $a(x)$ および $b(x)$ を $GF(q)[x]$ の多項式とする．2元体上の射影空間 $PG(GF(q)\times GF(q))$ において，

$$X(t) := \{(x, a(x)t + xb(t)) \mid x \in GF(q)\}$$

と定義する．このとき，

$$S := \{X(t) - \{(0,0)\} \mid t \in GF(q)\}$$

が $GF(2)$ 上の $d$-次元 *dual hyperoval* であるならば，$S$ は (適当な $\sigma$ と $\phi$ に対して) *dual hyperoval* $S^{d+1}_{\sigma,\phi}$ と同型である。

次の補題を用いるが補題の証明は省略する．(証明は難しくない.)

**補題 3.** $c(X)$ を $GF(q)[X]$ の多項式で

$$(c(t_1) + c(t_2))/(t_1 + t_2) \neq (c(t_1) + c(t_3))/(t_1 + t_3)$$

が $GF(q)$ の異なる元 $t_1, t_2, t_3$ に対して成り立っているとする．このとき $\lambda \in GF(q)$ および *o-polynomial* $f(X)$ が存在して，$t \in GF(q)$ に対して $c(t) = (c(0) + c(1) + \lambda)f(t) + \lambda t + c(0)$ がなりたつ．ここに $\lambda$ は $GF(q)$ の元で どのような $t_1 \neq t_2 \in GF(q)$ に対しても $(c(t_1) + c(t_2))/(t_1 + t_2)$ と表せない唯一の元である．

**命題の証明.** $X(t) = \{(x, a(x)t + xb(t)) \mid x \in GF(q)\}$ は $GF(2)$ ベクトル空間であるので，$a(X)$ は加法的である:つまり $a(x_1 + a_2) = a(x_1) + a(x_2)$ が $x_1, x_2 \in GF(q)$ に対して成り立つ．さて，$S$ は dual hyperoval であるので，互いに異なる $GF(q)$ の元 $t_i$ $(i = 1,2,3)$ に対して $X(t_1) \cap X(t_2)$ はただ一つの非零ベクトルを含み，またt $X(t_1) \cap X(t_2) \cap X(t_3) = \{(0,0)\}$ である．つまり $a(x)/x = (b(t_1) + b(t_2))/(t_1 + t_2)$ は $GF(q)^\times$ にただ一つの解 $x$ をもつが，$(b(t_1) + b(t_2))/(t_1 + t_2) \neq (b(t_1) + b(t_3))/(t_1 + t_3)$ である．よって $b(X)$ は補題 3 の仮定を満たしているので，$t \mapsto (b(t_1) + b(t))/(t_1 + t)$ は $GF(q) \setminus \{t_1\}$ から $GF(q) \setminus \{\lambda\}$ への全単射を与える．つまり $x \mapsto a(x)/x$ によって $GF(q)^\times$ と $GF(q) \setminus \{\lambda\}$ の全単射が得られる．よって $GF(q)$ の元 $x_i$ $(i = 1,2,3)$ に対して

$$\frac{a(x_1) + a(x_2)}{x_1 + x_2} = \frac{a(x_1 + x_2)}{x_1 + x_2} \neq \frac{a(x_1 + x_3)}{x_1 + x_3} = \frac{a(x_1) + a(x_3)}{x_1 + x_3}$$

が成り立つ.

よって $a(X)$ もまた, 補題 3 の仮定を満たす. よって 補題 3 より, $\lambda, \lambda' \in GF(q)$ と o-polynomials $\pi$ と $\phi$ が存在して $a(t) = (a(0)+a(1)+\lambda)\pi(t)+\lambda t+a(0)$ および $b(t) = (b(0)+b(1)+\lambda')\phi(t)+\lambda' t+b(0)$ が すべての $t \in GF(q)$ に対して成り立つ.

ここで $\lambda = \lambda'$ である. なぜなら $x_1 \neq x_2 \in GF(q)$ に対して $\{(a(x_1)+a(x_2))/(x_1+x_2)\} = GF(q)\backslash\{\lambda\}$ であるからである. ここで $\alpha := a(0)+a(1)+\lambda$ と $\beta := b(0)+b(1)+\lambda$ とおく.

$a(X)$ は加法的なので, $a(0) = 0$ かつ $\pi(X)$ は加法的な o-polynomial である. よって [3, Theorem 8.41] から $\pi(X) = X^{2^\sigma}$ と表せる. よって $a(x) = \alpha x^\sigma + \lambda x$ が $x \in GF(q)$ に対して成り立つ. ところで $a(x)t+xb(t) = (\alpha x^\sigma+\lambda x)t+x(\beta t^\phi+\lambda t+b(0)) = \alpha x^\sigma t+x(\beta t^\phi+b(0))$ なので $a(x)t+xb(t) = a'(x)t+xb'(t)$, (ここに $a'(t) := \alpha x^\sigma$ かつ $b'(t) := \beta t^\phi+\gamma$ ここに $\gamma := b(0)$) と表せる. .

$GF(2)$-線形写像 $G$, $H$, $I$ を $G : (x,y) \mapsto (x, \gamma x+y)$, $H : (x,y) \mapsto (\delta x, \delta^\sigma y)$( ここに $\delta \in GF(q)^\times$ であって $\delta^{\sigma-1} = \alpha/\beta$ とする. ) さらに $I : (x,y) \mapsto (x, \alpha^{-1}y)$ と定める. $X(t) = \{(x, \alpha x^\sigma t+x(\beta t^\phi+\gamma)) \mid x \in GF(q)\}$ なので, $X(t)^{GHI} = \{(x, x^\sigma t+xt^\phi \mid x \in GF(q)\}$ がわかる. よって $S^{GHI} = S^{d+1}_{\sigma,\phi}$. がなりたつ. □

# References


[1] H. taniguchi and S. Yoshiara, On dimensional dual hyperovals $S^{d+1}_{\sigma,\phi}$ Innovations in Incidence Geometry, Vol. 1(2005), 197–219.

[2] S. Yoshiara, A family of $d$-dimensional dual hyperovals in $PG(2d+1,2)$, Europ. J. Combinatorics. 20 (1999), 589–603.

[3] J. W. P. Hirschfeld: *Projective Geometries over Finite Fields*,

# Arrangements of hyperplanes constructed from Latin hypercubes

川原　行人 (Yukihito Kawahara)

Department of Mathematics, Tokyo Metropolitan University

ykawa@comp.metro-u.ac.jp

## 1　動機

複素射影空間 $\mathbb{P}^n$ (もしくは複素アファイン空間 $\mathbb{C}^n$) の中の超平面の有限集合 $\mathcal{A} = \{H_1, \ldots, H_N\}$ を超平面配置という．その補集合を $M = M(\mathcal{A}) = \mathbb{P}^n \setminus \cup_{i=1}^N H_i$ (もしくは $\mathbb{C}^n \setminus \cup_{i=1}^N H_i$) とかくことにする．本稿では射影空間内で考えることの方が多いので注意されたい．各超平面に複素数の重み $\lambda = (\lambda_1, \ldots, \lambda_N)$ $(\lambda_i \in \mathbb{C})$ を与える．ただし、射影空間内の配置を考える際には $\sum_{i=1}^N \lambda_i = 0$ を仮定する．ここで $H_i$ のまわりを反時計回りに一周するループを $\gamma_i$ とすると、モノドロミー表現 $\rho : \pi_1(M) \to \mathbb{C}^*$ を $\rho(\gamma_i) = \exp(-2\pi\sqrt{-1}\lambda_i) \in \mathbb{C}^*$ で定めることができ、$M$ 上の階数 1 の複素局所系 $\mathcal{L}_\lambda$ が得られる．その局所系を係数とする (コ) ホモロジー $H^p(M, \mathcal{L}_\lambda)$, $H_p(M, \mathcal{L}_\lambda)$ が考えられる．一方、超平面 $H_i$ の定義方程式を $\alpha_i = 0$ とすると、重み $\lambda$ に対して、対数微分形式

$$\omega_\lambda = \sum_{i=1}^N \lambda_i d\log \alpha_i$$

を考える．$M$ 上の正則微分形式の芽の層を $\Omega_M$ とし、平坦接続 $\nabla_\lambda = d + \omega_\lambda : \mathcal{O}_M \to \Omega_M^1$ を与えると、その核は $\mathcal{L}_\lambda$ になっている．そして $(\Omega_M, \nabla_\lambda)$ は複体をなす．$M$ が Stein であることから

$$H^p(M, \mathcal{L}_\lambda) \simeq H^p(\Gamma(M, \Omega_M), \nabla_\lambda)$$

が成立する．ここで $\Gamma$ は大局切断を表す．$\mathcal{L}_\lambda$ の双対な局所系 $\mathcal{L}_\lambda^\vee$ をとるとペアリング

$$H^p(M, \mathcal{L}_\lambda) \times H_p(M, \mathcal{L}_\lambda^\vee) \to \mathbb{C}$$

が得られる．これは超幾何ペアリングと呼ばれ、一般化された超幾何関数論において中心的な役割を果たす [2, 11]．また、一般に $p > n$ のときは $H^p(M, \mathcal{L}_\lambda) = 0$ となる．そして、重み $\lambda$ がある一般的な条件を満たすとき、消滅定理

$$H^p(M, \mathcal{L}_\lambda) = 0, \qquad p \neq n$$

が成立する [2, 4, 14, 15, 11].

最近、$n$ 次より低いところで非消滅となる場合について盛んに研究されるようになった ([1, 3, 5, 8, 9]). 最も簡単なものは、重み $\lambda$ がすべて整数で与えられる場合で、このとき $\mathcal{L}_\lambda$ は自明となり、局所系コホモロジーは通常のコホモロジーとなる: $H^p(M, \mathcal{L}_\lambda) = H^p(M, \mathbb{C})$. よって、非消滅である. また、重み $\lambda$ が非自明ならば $H^0(M, \mathcal{L}_\lambda) = 0$ となる. さらに Lefschetz の超平面切断定理から $n-1$ 次の非消滅が本質的となる.

**問題** $\mathbb{P}^n$ (もしくは $\mathbb{C}^n$) 内の超平面配置で $H^{n-1}(M, \mathcal{L}_\lambda) \neq 0$ となる非自明な重み $\lambda$ をもつものを構成せよ.

次の例は基本的となる.

**例 1 (中心的超平面配置)** すべての超平面の共通部分が空でない超平面配置を中心的 (central) という. ここでは $\mathbb{C}^n$ 内の配置を考える. $\mathcal{A}$ を中心的とし重み $\lambda$ が非自明で $\sum_{i=1}^N \lambda_i = 0$ を満たすとき $H^n(M, \mathcal{L}_\lambda) = H^{n-1}(M, \mathcal{L}_\lambda) \neq 0$ となる. 正確には特別な場合を除く必要があるが、それを記述するには少々の準備が必要であるので割愛する.

中心的でない例として次のものが知られている:

- Ceva の定理に現れる射影空間内の直線配置
- Pappus の定理に現れる射影空間内の直線配置
- $B_3$-配置: $xyz(x-y)(x+y)(y-z)(y+z)(z-x)(z+x)$ で定義される $B_3$ 型の鏡映群に付随する配置である. 本来、$\mathbb{C}^3$ 内の配置であるが、本稿では射影化して $\mathbb{P}^2$ 内の直線配置で考える.
- Monomial 配置: $(x^m - y^m)(y^m - z^m)(z^m - x^m)$ で定義される配置で、Monomial 群に付随する配置である. これも同様、$\mathbf{P}^2$ 内の直線配置で考える.
- The Hessian configuration : $xyz\prod_{k=0}^{2}(x^3+y^3+z^3-3\exp(2k\pi/3)xyz)$ で定義される配置で、非特異な 3 次曲線の 9 個の変曲点を通る 12 本の直線配置である.

これらはすべて $n=2$ 次元で $H^2(M, \mathcal{L}_\lambda) \neq 0$, $H^1(M, \mathcal{L}_\lambda) \neq 0$, $H^0(M, \mathcal{L}_\lambda) = 0$ となる重み $\lambda$ を持っている. これら以外にも幾つか知られているが、非消滅をもつ超平面配置は思いのほか少ない. 3 次元以上では具体的な例も知られていない (?). そこで、これら以外の例があるのかないのか、これらがなぜ非消滅をもつのか、高次元の例は構成できるか、などが問題となる. 実は、上の例は組合せ的に、ラテン方陣により構成される直線配置であり [9, 7]、さらに、高次元ではラテンハイパーキューブから構成される超平面配置が非消滅をもつ [7]. 本稿では、その構成法とそれに関連する事柄や問題を紹介する.

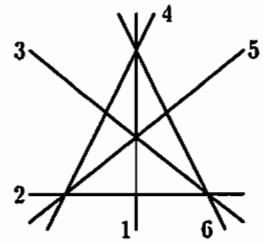
## 2 ラテン方陣から構成される直線配置

2 次元の場合、$H^1(M,\mathcal{L}_\lambda)\neq 0$ となる直線配置を構成することが主題となる. まず、その構成法を述べる:

**定理 2 (Libgober-Yuzvinsky [9])** $m>1$ とする.

1. $m$ 次ラテン方陣 $K$ (Latin square of order $m$) を用意する.
   ラテン方陣とは, すべての行および列にもすべての文字 (記号) が 1 個ずつ現れるような正方行列である. すなわち、すべての行および列は $m$ 個の文字 (記号) の並べ替えとなっている. たとえば、 $m=2,3$ では
   $$K=\begin{pmatrix}\bigcirc & \triangle\\ \triangle & \bigcirc\end{pmatrix},\quad \begin{pmatrix}\bigcirc & \triangle & \square\\ \square & \bigcirc & \triangle\\ \triangle & \square & \bigcirc\end{pmatrix}.$$

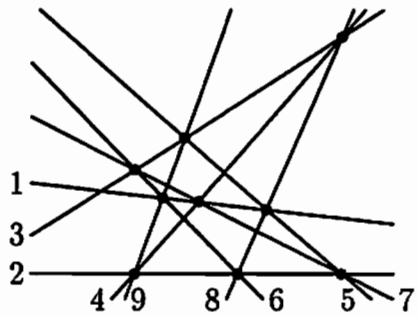
2. 次のようにして、パズル $\mathcal{C}[K]$ を作る. 行に $1,2,\ldots,m$、続けて列に $m+1,m+2,\ldots,2m$、成分の文字に $2m+1,2m+2,\ldots,3m$ と番号を付けて、各成分ごとに対応する行番号、列番号、成分番号の組をかく. たとえば、 $m=2$ では
   $$\begin{pmatrix}\bigcirc & \triangle\\ \triangle & \bigcirc\end{pmatrix}\to\begin{array}{c|cc} & 3 & 4\\ \hline 1 & 5 & 6\\ 2 & 6 & 5\end{array}\to\mathcal{C}[K]=\begin{bmatrix}(1,3,5) & (1,4,6)\\ (2,3,6) & (2,4,5)\end{bmatrix}.$$
   そして、たとえば $(1,3,5)$ は 3 本の直線 1, 3, 5 は 1 点で交わるパズルのピースだと考える. こうして $\mathcal{C}[K]$ を $m^2$ 個のピースを持ったパズルとする.

3. パズル $\mathcal{C}[K]$ のピースをつなぎ合わせて、$3m$ 本の直線の配置 $\mathcal{A}$ を見つける. たとえば $m=2$ の場合 Ceva の配置が得られる:
   $$\mathcal{C}[K]=\begin{bmatrix}(1,3,5) & (1,4,6)\\ (2,3,6) & (2,4,5)\end{bmatrix}\quad\to$$
   
   

この配置 $\mathcal{A}$ を $\mathbb{P}^2$ 内で考える. $\lambda$ を
$$\lambda=(\underbrace{\lambda_1,\ldots\lambda_1}_{m},\underbrace{\lambda_2,\ldots\lambda_2}_{m},\underbrace{\lambda_3,\ldots\lambda_3}_{m});\qquad \lambda_1+\lambda_2+\lambda_3=0$$
となる非自明な重みとすると
$$H^2(M,\mathcal{L}_\lambda)\neq 0,\quad H^1(M,\mathcal{L}_\lambda)\neq 0,\quad H^0(M,\mathcal{L}_\lambda)=0.$$

この事実は本質的に Libgober-Yuzvinsky [9] によって得られていたものであるが、結果を部分的に抽出して構成法を具体的にしたものである．また、$m=1$ の場合が 3 本の直線が 1 点を共有している配置に対応することになる．この構成で $m=2$ の場合が Ceva の配置であり、$m=3$ の場合には Pappus の定理に現れる直線配置が得られる:

$$K=\begin{pmatrix}1&2&3\\3&1&2\\2&3&1\end{pmatrix}\to C[K]=\begin{bmatrix}(1,4,7)&(1,5,8)&(1,6,9)\\(2,4,9)&(2,5,7)&(2,6,8)\\(3,4,8)&(3,5,9)&(3,6,7)\end{bmatrix}\to$$




## 3 Geometric Net と 直交性

定理 2 で得られる直線配置は 3-ネットというものになる．

**定義 3** $\mathbb{P}^2$ 内の直線配置 $\mathcal{A}$ が $\mathcal{A}=\bigcup_{i=1}^{k}\mathcal{A}_i$ と分割されていて、$\mathbb{P}^2$ の点の集合 $\mathcal{X}$ とのペア $(\mathcal{A},\mathcal{X})$ が次の条件を満たすとき、$k$-ネット ($k$-net in $\mathbb{P}^2$) という:

(i) $i\neq j, l\in\mathcal{A}_i, l'\in\mathcal{A}_j \Rightarrow l\cap l'\in\mathcal{X}$.

(ii) すべての $X\in\mathcal{X}$ と $1\leq i\leq k$ に対して $X\in l$ となる $l\in\mathcal{A}_i$ が唯一存在する．

定義から、すべての $i$ と $l\in\mathcal{A}$ に対して $|\mathcal{A}_i|=|l\cap\mathcal{X}|=m$ が一定となり $m$ を order といい、order $m$ の $k$-ネットを $(k,m)$-ネットということもある．また、$|\mathcal{X}|=m^2$ であることもすぐにわかる．そして

$$m\text{ 次ラテン方陣}\quad\longleftrightarrow\quad(3,m)\text{-ネット}$$

という対応がつく．一般には

$$k-2\text{ 個の互いに直交するラテン方陣}\quad\longleftrightarrow\quad k\text{-ネット}$$

という対応がある．これは組み合わせ的な興味から Dénes, J. and Keedwell, A.D., Latin Squares and their Applications, 1974. の本の中で述べられている．

直交性の定義を述べる: 同じ次数の2つのラテン方陣 $K=(k_{i,j})$, $K'=(k'_{i,j})$ が各成分ごとのペア $(k_{i,j},k'_{i,j})$ がすべて異なるとき、$K$ と $K'$ は直交する (orthogonal) といい、同じ次数の幾つかのラテン方陣の任意の2つが直交しているとき、それらを互いに直交する (mutually orthogonal) という. とくに直交する2つのラテン方陣の組はオイラー方陣と呼ばれている.

例 4 (Hessian configuration) $L_1=\begin{pmatrix}1&2&3\\3&1&2\\2&3&1\end{pmatrix}$ と $L_2=\begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix}$ の各成分の組は $\begin{pmatrix}(1,1)&(2,2)&(3,3)\\(3,2)&(1,3)&(2,1)\\(2,3)&(3,1)&(1,2)\end{pmatrix}$ ですべて異なるので $L_1$ と $L_2$ は直交している. 定理2を拡張して直線配置を得ることができる. 上の例で構成してみると $C[L_1]$ は定理2と同じ構成をし、$C[L_2]$ は成分番号を $3m+1,3m+2,\dots,4m$ と番号が続くようにする:

$$C[L_1]=\begin{bmatrix}(1,4,7)&(1,5,8)&(1,6,9)\\(2,4,9)&(2,5,7)&(2,6,8)\\(3,4,8)&(3,5,9)&(3,6,7)\end{bmatrix},$$

$$C[L_2]=\begin{bmatrix}(1,4,10)&(1,5,11)&(1,6,12)\\(2,4,11)&(2,5,12)&(2,6,10)\\(3,4,12)&(3,5,10)&(3,6,11)\end{bmatrix}.$$

さらに2つを合わせて

$$C[L_1,L_2]=\begin{bmatrix}(1,4,7,10)&(1,5,8,11)&(1,6,9,12)\\(2,4,9,11)&(2,5,7,12)&(2,6,8,10)\\(3,4,8,12)&(3,5,9,10)&(3,6,7,11)\end{bmatrix}$$

とし、今度はたとえば $(1,4,7,10)$ は4本の直線 $1,4,7,10$ が1点で交わるとし、このような $3^2$ 個の4重点がある配置を探す. このパズルは解けて、Hessian configuration がその答えになる. Hessian configuration は 4-ネットであり、また、非特異な3次曲線の9個の変曲点を通る12本の直線配置であるが、上の9つの4重点がその変曲点に対応している. そして $H^1(M,\mathcal{L}_\lambda)=\mathbb{C}^2$ となる重み $\lambda$ がある.

同様の構成の仕方で、次が得られる:

系 5 $k-2$ 個の互いに直交するラテン方陣から構成される配置 (すなわち $k$-ネット) $\mathcal{A}$ と重み

$$\lambda=(\underbrace{\lambda_1,\dots\lambda_1}_{m},\dots,\underbrace{\lambda_k,\dots\lambda_k}_{m});\quad \lambda_1+\cdots+\lambda_k=0$$

に対して $\dim H^1(M,\mathcal{L}_\lambda)\geqq k-2$ となる.

ただし $k \geq 4$ である $k$-ネットは Hessian configuration 以外は知られていない．また、$m-1$ 個の $m$ 次ラテン方陣が互いに直交しているとき完全直交系と呼ばれ、$m$ 次有限射影平面と同等になっている．よって Hessian configuration は組合せ的には 3 次有限射影平面の構造を持っている．

## 4 Quasi-group（準群）

さて、ラテン方陣を作るのに最も手っ取り早い方法は位数 $m$ の有限群を用意し、その乗積表をかけば、それが $m$ 次ラテン方陣となる．たとえば 加法群 $\mathbb{Z}_2 = \{0,1\}$ では乗積表は $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ となりラテン方陣 $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ が得られる．
ラテン方陣は、この意味で有限群より広いものになっている．実際には、群の拡張のひとつである準群とラテン方陣は同等なものになっている．

定義 6 2 項演算 $*$ をもつ集合 $Q$ において、$a,b \in Q$ に対して $a * x = b$, $y * a = b$ となる $x,y \in Q$ が一意に存在するとき、$Q$ を quasi-group（準群）という．

例 7 位数 $m = 4$ の有限群は 2 つあるが、加法群でかいて $\mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ である．また、準群またはラテン方陣としても 2 つしかない．

$$K_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{pmatrix} \to C[K_1] = \begin{bmatrix} (1,5,9) & (1,6,10) & (1,7,11) & (1,8,12) \\ (2,5,12) & (2,6,9) & (2,7,10) & (2,8,11) \\ (3,5,11) & (3,6,12) & (3,7,9) & (3,8,10) \\ (4,5,10) & (4,6,11) & (4,7,12) & (4,8,9) \end{bmatrix}$$

$$K_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \to C[K_2] = \begin{bmatrix} (1,5,9) & (1,6,10) & (1,7,11) & (1,8,12) \\ (2,5,10) & (2,6,9) & (2,7,12) & (2,8,11) \\ (3,5,11) & (3,6,12) & (3,7,9) & (3,8,10) \\ (4,5,12) & (4,6,11) & (4,7,10) & (4,8,9) \end{bmatrix}$$

これらのパズルは両方とも解けて、それぞれ Kirkman の定理, Steiner の定理に現れる直線配置となる．この 2 つの定理は classical な射影幾何学の定理で有名であるが、解説した文献もさほど多くないようなので、ここで述べておく．まずは超有名な Pascal の定理を思い出す．1 つの 2 次曲線上に異なる 6 個の点 $A,B,C,D,E,F$ をとる．

**Pascal の定理** 直線 $AB$ と $DE$, $BC$ と $EF$, $CD$ と $AF$ の 3 つの交点は 1 直線上にある．

この直線を $ABCDEF$ の Pascal 直線という．$ABCDEF$ は必ずしも六角形でなくてもよく、Pascal 直線は 6 点の順序を換えることによって 60 本引ける．このとき、次の定理が知られている．

**Steiner の定理** $ABCDEF$, $ADEBCF$, $ADCFEB$ の 3 つの Pascal 直線は 1 点で交わる．

**Kirkman の定理** $ABCDEF$, $ADEBCF$, $ADCFEB$ の 3 つの Pascal 直線は 1 点で交わる.

$ABCDEF$ を六角形と見れば、両定理ともに、6 つの辺と 3 つの対角線と 3 つの Pascal 直線で計 12 本の直線を引いている. この Kirkman, Steiner の定理の直線配置がそれぞれ $\mathcal{C}[K_1]$, $\mathcal{C}[K_2]$ に対する実現になる. ちなみに 2 つの定理および配置の違いは、六角形の 3 つの対角線の引き方から確認できる (実際の絵を見たい方は [7] を参照のこと).

## 5 退化

定理 2 での $\mathcal{C}[K]$ は、局所系コホモロジー $H^1(M, \mathcal{L}_\lambda)$ の非消滅をもつ直線配置の最低限の直線の退化の情報である. よって、$\mathcal{C}[K]$ よりも多く退化している配置、すなわちネットが退化した配置も非消滅をもつ. ただし、退化が多すぎると中心的配置 (すべての直線が 1 点を共有する) となってしまう. 退化し中心的でないものを構成するのにいくつかのタイプが考えられる.

**Type I :** 定理 2 において、ラテン方陣 $K$ の各行、各列、各成分に対応して直線を考えた. したがって、直線配置は行、列、成分に対応して 3 つのクラスに分けられる (3 つのクラスに分けるので 3-ネットといった). 定理 2 では各クラスは一般の位置にある (退化がない) 配置である. そこで、"各クラスの中で退化している配置は非消滅をもつ" ことになる. この中で最も退化しているのは、各クラスが中心的となる場合であり、Monomial 配置がその例となる. ちなみに、Monomial 配置は加法群 $\mathbb{Z}_m$ から得られるラテン方陣から来ている.

**Type II :** 定理 2 で得られる配置 (3-ネット) で幾つかの直線を重ね合わせる事によって、非消滅をもつ配置を構成することができる. たとえば、前章の $\mathcal{C}[K_2]$ から得られる Steiner の定理の直線配置において、2 つの直線 1 と 2 を 1 つの直線とし, 同様に 5 と 6, 11 と 12 をそれぞれ 1 つの直線とすると計 9 本の直線の配置となり、$B_3$ 配置となる.

**Type III :** ラテン方陣の中に小さいラテン方陣がある場合があり、それを部分ラテン方陣という. 部分ラテン方陣に対応する直線たちが 1 点で交わるように退化させることが可能になる. たとえば、前章の $K_2$ において

$$J = \begin{pmatrix} 2 & 4 \\ 4 & 2 \end{pmatrix}$$

は部分ラテン方陣となり $K_2$ から得られる Kirkman の定理の配置で、直線 $1,3,6,8,10,12$ が1点で交わるようにすることができる (実際の絵を見たい方は [7] を参照のこと).

これらまたはこれらの組合せ以外の退化は今のところ例はないが、組合せ的なマトロイドのレベルでも確定できていない.

## 6 一般次元への拡張

定理 2 は一般次元へ拡張することができる. まず、ラテンハイパーキューブ (日本語ではラテン超方格と呼ばれることもあるようである. ) の定義を与えておく. 位数 $m$ の有限集合を今は $[m] := \{1,2,\ldots,m\}$ としておく. $\ell$ 次元のラテンハイパーキューブ (Latin hypercube of dimension $\ell$ and order $m$) とは $m^\ell = m \times \cdots \times m$ のハイパーキューブで任意の $\ell-1$ 個の座標を固定したとき、残り1つの座標上には $[m]$ の置換が配列されている. $\ell = 2$ のときはラテン方陣に他ならない.

**定理 8 (K [7])** $m > 1$ とする.

1. $\ell$ 次元のラテンハイパーキューブ $K$ を用意する.
2. 定理 2 同様に、パズル $C[K]$ を作る. ここで $C[K]$ は $m^\ell$ 個のピースを持つ.
3. パズル $C[K]$ のピースをつなぎ合わせて、$\mathbb{P}^\ell$ 内で $(\ell+1)m$ 枚の超平面の配置 $\mathcal{A}$ を見つける.

この $\mathcal{A}$ が存在すれば

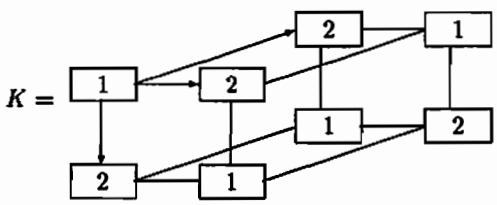
$$\lambda = (\underbrace{\lambda_1,\ldots\lambda_1}_{m},\ldots,\underbrace{\lambda_{\ell+1},\ldots\lambda_{\ell+1}}_{m}); \qquad \lambda_1+\cdots+\lambda_{\ell+1} = 0$$

となる重み $\lambda$ に対して

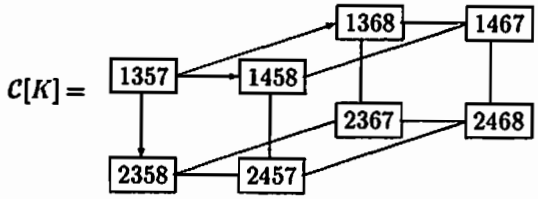
$$H^{\ell-1}(M,\mathcal{L}_\lambda) \neq 0$$

となる.

**例 9** $[m=2]$ 上の $\ell = 3$ 次元のラテンハイパーキューブ $K$ をとる.




そして、上 $\to 1$, 下 $\to 2$, 左 $\to 3$, 右 $\to 4$, 前 $\to 5$, 後 $\to 6$ とし、成分には $1 \to 7$, $2 \to 8$ を割り振り、$C[K]$ を作成する.




そして、たとえば $(1,2,5,7)$ に対して 4 つの (超) 平面 $1,2,5,7$ は 1 点を共有し、その他では退化していない中心的配置 (各平面を $x=0, y=0, z=0, x+y+z=0$ で与えることができる) をパズルのピースとする. このようにしてできる $2^3=8$ 個のピースをつなぎ合わせた平面配置を探す. この答えは見つかり、たとえば

$$x_1x_2x_3x_4(x_1+x_2+x_3+x_4)(x_1-2x_2+2x_3-x_4)(x_1-x_2+x_3-x_4)(x_1+2x_2+2x_3+x_4)$$

で定義される平面配置である. この配置は退化した直線を持たず退化している点は $C[K]$ の各成分に対応する $2^3=8$ 個の点だけである. よって

$$H^3(M,\mathcal{L}_\lambda)\neq 0,\ H^2(M,\mathcal{L}_\lambda)\neq 0,\ H^1(M,\mathcal{L}_\lambda)=H^0(M,\mathcal{L}_\lambda)=0$$

となる重み $\lambda$ を持つ.

## 7 問題

定理 2 や定理 8 のように構成される超平面配置の存在・非存在が問題である. マトロイドではすべて存在している [7] ので、このような構成で得られるマトロイドが実現可能か、という問題となる. 2 次元の場合 (ラテン方陣の場合) には Yuzvinsky [16] の結果があるが、一般には未解決である. また、[16] で述べられているように、アーベル群でない群 (または準群) から構成される直線配置は存在するか? $k\geq 4$ のとき Hessian configuration 以外の $k$-ネットは存在するか? などの問題がある.

## References

[1] D. Arapura, *Geometry of cohomology support loci for local systems* I, J. Alg. Geom. **6** (1997), 563–597.

[2] K. Aomoto and M. Kita, *Hypergeometric functions* (in Japanese), Tokyo Springer, 1994.

[3] D. Cohen and A. Suciu, *Characteristic varieties of arrangements*, Math. Proc. Cambridge Philos. Soc. 127 (1999), 33–54.

[4] H. Esnault, V. Schechtman and E. Viehweg, *Cohomology of local systems on the complement of hyperplanes*, Invent. Math. **109** (1992), 557–561; Erratum **112** (1993), 447.

[5] M. Falk, *Arrangements and Cohomology*, Annals of Comb. 1 (1997), 135–157.

[6] Y. Kawahara, *On matroids and Orlik-Solomon algebras*, Annals of Combinatorics, 8 (2004) 63-80.

[7] Y. Kawahara, *The non-vanishing cohomology of Orlik-Solomon algebras*, math.CO/0506421.

[8] A. Libgober, *Characteristic varieties of algebraic curves*, Applications of algebraic geometry to coding theory, physics and computation (Eilat, 2001), 215–254, NATO Sci. Ser. II Math. Phys. Chem., 36, Kluwer Acad. Publ., Dordrecht, 2001.

[9] A. Libgober and S. Yuzvinsky, *Cohomology of the Orlik-Solomon algebras and local systems*, Compositio Math. 121 (2000), no. 3, 337–361.

[10] P. Orlik and H. Terao, *Arrangements of Hyperplanes*, Grundlehren der mathematischen Wissenschaften 300, Springer-Verlag, 1992.

[11] P. Orlik and H. Terao, *Arrangements and Hypergeometric integrals*, MSJ, Mem. vol.9, Math. Soc. Japan, 2001.

[12] J. Oxley, *Matroid Theory*, Cambridge Univ. Press. Cambridge, 1993.

[13] V. V. Prasolov, *Essays on numbers and figures*, Translated from the 1997 Russian original by A. B. Sossinski. Mathematical World, 16. American Mathematical Society, Providence, RI, 2000.

[14] V. Schechtman, H. Terao and A. Varchenko, *Local systems over complements of hyperplanes and the Kac-Kazhdan conditions for singular vectors*, J. Pure Appl. Algebra 100 (1995), 93–102.

[15] S. Yuzvinsky, *Cohomology of the Brieskorn-Orlik-Solomon algebras*, Comm. Algebra 23 (1995), 5339–5354.

[16] S. Yuzvinsky, *Realization of finite abelian groups by nets in* $\mathbb{P}^2$, Compos. Math. 140 (2004), no. 6, 1614–1624.

# Coxeter群の同型問題、直既約性と自己同型群について

東京大学大学院数理科学研究科　博士課程3年　縫田　光司 (Koji Nuida)
日本学術振興会特別研究員 DC2 (No. 16-10825)

**概要**

Coxeter群 $W$ とその標準生成系 $S$ の組 $(W,S)$ を Coxeter 系という。Coxeter 系の構造は、Coxeter グラフと呼ばれる図形によって完全に特定され、Coxeter 系の同型類と Coxeter グラフの同型類の間の対応が一対一であることも古くから知られている。その一方で、一つの Coxeter 群に対してその標準生成系の取り方は一般に複数存在し、それぞれに対応する Coxeter グラフが互いに同型でなくなる例も知られている。本稿の基となる講演では、この Coxeter 群と Coxeter グラフの対応に関する話者の結果を含む最近の研究状況、及び関連する話題に関する解説を行った。

## 1　導入

本稿では、Coxeter 群の群構造に関するいくつかの問題を扱う。まず定義を述べよう。群 $W$ が *Coxeter*群であるとは、$W$ のある生成系 $S$ について $W$ が以下のような群表示

$$W = \langle S \mid s,t \in S \text{ で } m(s,t) < \infty \text{ ならば } (st)^{m(s,t)} = 1 \rangle$$

を持つことをいう。この定義において、$m$ は両成分に関して対称的なある写像 $m : S \times S \to \{1,2,3,\ldots\} \sqcup \{\infty\}$ であって「$m(s,t) = 1 \Leftrightarrow s = t$」なるものである（後者の条件から全ての $s \in S$ について $s^2 = 1$ が従う）。$S$ を $W$ の *Coxeter*生成系と呼び[1]、対 $(W,S)$ のことを *Coxeter*系と呼ぶ。なお、本稿では断りのない限り生成系 $S$ の有限性は仮定しない。

さて、上の定義を見直してみると、$W$ と $S$ に対する写像 $m$ の選び方に多様性があるようにも思われるが、実際には以下のような著しい事実が成り立つ。この事実の証明を含め、Coxeter 群の理論の基本的な部分は [6] に纏められている。

**定理 1.1** 上の定義において、写像 $m$ は（存在すれば）$W$ と $S$ のみから一意的に定まる。詳しくは、$m(s,t)$ の値（$\infty$ の場合も含めて）は $W$ の元 $st$ の位数に一致する。

この事実に基づき、以下のようなグラフを用いて Coxeter 群を表示することが多い[2]。頂点集合 $S$ を持つ無向単純グラフ $\Gamma$ で、各辺が3以上の整数もしくは $\infty$ でラベル付けされているものを *Coxeter* グラフと呼ぶ[3]。（ただし、3というラベルは頻出するため、図示の際には省かれることが多い。）すると、$m(s,t)$ を辺 $s$ — $t$ のラベル（$s = t$ なら1、辺が無ければ2）と定めれば上の群表示を持つ群 $W$ は $S$ を生成系として Coxeter 群をなし、また $W$ から逆算して対応する Coxeter グラフを構成することもできる。（図1は $B_n$ 型の有

[1]本稿では Coxeter 生成系ばかり登場するので、以下では単に生成系とも書く。
[2]ただし、生成系 $S$ が有限濃度でない場合にこのグラフを図示できるかどうかはまた別の話である。
[3]Weyl 群の Dynkin 図形から矢印を取り除き、多重辺を適切なラベル付きの辺で置き換えたもの、と言ってもよい。ただし、全ての Coxeter 群が Weyl 群として現れるわけではない。

限 Coxeter 群に対応する Coxeter グラフである。）定理 1.1 によれば、この対応は Coxeter 系 $(W,S)$ と Coxeter グラフ $\Gamma=\Gamma(W,S)$ の間の（同型を除いた）一対一対応である[4]。

一方で、Coxeter グラフを Coxeter 群の表示と見るとき、実はこれは必ずしも一意的な

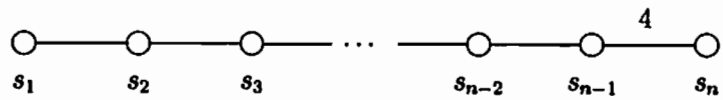



図 1: $B_n$ 型の Coxeter グラフ

表示ではない — 同型でない二つのグラフが同型な Coxeter 群を定め得る — ことが知られている。例えば図 1 のグラフが定める Coxeter 群は、$n$ が 3 以上の奇数の場合には $A_1\times D_n$ 型のグラフが定める Coxeter 群と同型である。ここで後者の Coxeter グラフは、1 点からなるグラフ（$A_1$ 型）と図 2 のグラフ（$D_n$ 型）の二つの連結成分からなる。

二つの Coxeter 群が同型かどうか判定する問題を、*Coxeter* 群の同型問題[5](*isomorphism*

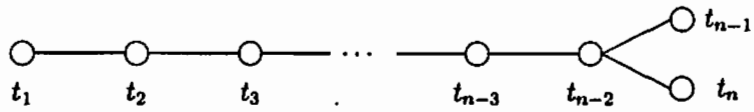



図 2: $D_n$ 型の Coxeter グラフ

*problem*) と呼ぶ。これには大別すると以下の二通りの問題設定の仕方があるが、これらは本質的には同値な設定なので、状況に応じて二通りの設定を使い分けて議論を進める。

1. 与えられた二つの Coxeter 群 $W$ と $W'$ の間に群同型写像 $W\xrightarrow{\sim}W'$ が存在するかどうか、存在すればそれはどのような性質を持つか考察する。

2. 与えられた Coxeter 群 $W$ がどのくらい多様な生成系を持つか、またそれらの生成系が互いにどのような関係にあるかを考察する。

なお、一つの Coxeter 生成系 $S$ の共役 $wSw^{-1}$ はまた全て Coxeter 生成系であるから、本質的に最も生成系の種類の「少ない」Coxeter 群とは、その生成系が全て互いに共役である（*strongly rigid* と呼ばれる）ものである。一方、$(W,S)$ に対応する Coxeter グラフ $\Gamma(W,S)$ が $S$ に依らずに常に同型となる $W$ は *rigid* な Coxeter 群と呼ばれる。(strongly) rigid な Coxeter 群の決定は、同型問題における大きな目標の一つである。

次に、本稿で扱う第二の問題を述べる。Coxeter グラフ $\Gamma=\Gamma(W,S)$ について、その連結成分 $\Gamma_I$ の頂点集合 $I\subset S$ を $S$ の既約成分と呼び、また $I$ が生成する $W$ の部分群 $W_I$ を $(W,S)$ の既約成分と呼ぶ。（一般に、$I\subset S$ の生成する部分群 $W_I$ を $W$ の放物型部分群(*parabolic subgroup*) と呼ぶ。）生成系 $S$ が文脈から明らかな場合は、$W_I$ を単に $W$ の既約成分とも呼ぶ。このとき、Coxeter 群 $W$ はその既約成分 $W_I$ たちの直積[6]に（生成系 $S$

[4]ここで、Coxeter 群の間の群同型写像で生成系を保つものを *Coxeter* 系の同型写像と呼ぶ。
[5]以下、単に同型問題と書く。
[6]本稿では通常、群の直積と書いたら完全直積ではなく制限直積を指す。

を指定すれば）一意的に分解される（$W$ の既約分解）。これは $W$ の放物型部分群による分解の中では最も細かいものであるが、前述の $B_n$ 型の例が示す通り、抽象群としての最も細かい分解（直既約分解）であるとは限らない。第二の問題は、$W$ の既約分解を基に直既約分解を得ることであるが、これには筆者が最近次のような結果を与えた[7]。

**定理 1.2** （縫田 [11]）$W$ が無限群でありかつ $\Gamma(W,S)$ が連結（このような Coxeter 系 $(W,S)$ は既約と言われる）であれば、$W$ は抽象群として直既約である。

従って、$W$ の直既約分解を得るには、$W$ の既約分解において有限群である成分を全て直既約分解すればよいが、有限既約 Coxeter 群の分類定理を用いればこれはそう難しくはない。具体的には、$B_n$ 型（$n$ は 3 以上の奇数）、$E_7$ 型、$H_3$ 型、$I_2(m)$ 型（$m$ は 3 以上の奇数の 2 倍）の有限既約 Coxeter 群はその中心（位数 2）とある直既約群の直積に分解され、他の有限既約 Coxeter 群は全て直既約である。

本稿の基となった講演では、定理 1.2 と関連する結果、及び同型問題に関する（筆者の結果を含む）最近の結果について紹介した。この場を借りて、講演の場を与えて下さったシンポジウム世話人の皆様に深い感謝の意を表したい。

## 2 定理 1.2 の証明の概略

講演では時間の関係で割愛せざるを得なかったが、ここでは定理 1.2 の証明の概略を紹介したい。この証明では Coxeter 群における中心化群や正規化群が重要な役割を果たし、群論的な観点からも興味深いものと思われる。

定理 1.2 は次の命題の簡単な帰結として得られる。

**命題 2.1** ([11]) $W$ を Coxeter 群、$H$ をその正規部分群であって、位数 2 の元たちで生成されているものとする。このとき $H$ の $W$ における中心化群 $Z_W(H)$ の構造は完全に記述される。特に、もし $Z_W(H)$ が $W$ の中心 $Z(W)$ とも $W$ 自身とも異なれば、$H$ と $Z_W(H)$ は $W$ のある共通の真部分群に含まれる。

この命題から定理 1.2 を導こう。実際、既約な無限 Coxeter 群 $W$ が二つの真部分群 $H_1$ と $H_2$ の直積に分解したならば、このような $W$ の中心が単位群であるという事実から、$H_1$ と $H_2$ は $W$ 自身とも $Z(W)$ とも異なる。また、$W$ が位数 2 の元で生成されているので、$H_1$ と $H_2$ も位数 2 の元で生成される $W$ の正規部分群である。すると命題 2.1 より、$H_1$ と $Z_W(H_1)$ は共に $W$ のある真部分群に含まれるが、一方で $H_2$ は $Z_W(H_1)$ に含まれるので、これは $W = H_1 \times H_2$ という仮定に反する。よって確かに $W$ は直既約である。

命題 2.1 の証明には、群論における以下の結果を用いる。

**補題 2.2** $X$ を群 $G$ の部分集合、$H$ を $G$ の正規部分群で $X$ を含む最小のものとすると、$Z_G(H)$ は全ての $x \in X$ に対する $\mathrm{Core}_G(Z_G(x))$ の共通部分と一致する。ここで $\mathrm{Core}_G(H')$ は $G$ の正規部分群で $H'$ に含まれる最大の部分群を表す。

[7] これは $S$ が有限集合の場合には L. Paris 氏のプレプリント [12] で示されているが、氏の証明は $S$ の有限性の仮定を必要とする。一方、筆者の証明は $S$ の濃度によらず全ての場合に適用可能である。

R. W. Richardson 氏の定理 ([13]、定理 A) より、Coxeter 群 $W$ における位数 2 の元の共役類の代表系として、有限放物型部分群 $W_I$ の最長元 $w_0(I)$ で $w_0(I) \in Z(W_I)$ となるもの全体がとれる。このとき、$w_0(I)$ の中心化群が $W_I$ の正規化群 $N_W(W_I)$ と等しいことを示すことができる。すると、定理 2.1 のような $H$ は、$H$ に含まれる上記の代表元 $w_0(I)$ の全てを含む最小の正規部分群であり、補題 2.2 と直前の文より $H$ はいくつかの $\mathrm{Core}_W(N_W(W_I))$ たちの共通部分として表される。さらに、Coxeter 群特有の議論により $\mathrm{Core}_W(N_W(W_I))$ の構造を特定でき、そこから目的の命題が証明される。詳細は [11] を参照されたい。

## 3 同型問題に関する筆者の結果 1 — 既約な場合への帰着

定理 1.2 を用いると、一般の Coxeter 群の同型問題を、以下の意味で既約 Coxeter 群の同型問題に帰着させることができる。まず定義を一つ準備する。Coxeter 群 $W$ の (ある生成系に応じた) 既約分解において、有限群である既約成分全ての積を $W$ の有限成分 (*finite part*) と呼び、$W_{\mathrm{fin}}$ で表す[8]。この定義の下で、筆者は以下の結果を得た。

**定理 3.1** ([11]) $(W,S)$ と $(W',S')$ を Coxeter 系とする。このとき、$W$ と $W'$ が抽象群として同型となる必要充分条件は以下の二つである。

1. 各々の有限成分 $W_{\mathrm{fin}}$ と $W'_{\mathrm{fin}}$ が互いに同型である。
2. $W$ の既約成分で無限群であるもの全体の集合と、$W'$ のそのような集合の間の一対一対応で、対応する既約成分同士が互いに同型となるものが存在する。

なお、定理の条件 1 を確認するためには、各々の有限成分の既約成分全てを (定理 1.2 の直後の注意に基づき) 直既約因子の積に分解し、各直既約因子の同型類の重複度を $W_{\mathrm{fin}}$ と $W'_{\mathrm{fin}}$ において比較すればよい。その重複度の全てが $W_{\mathrm{fin}}$ と $W'_{\mathrm{fin}}$ で一致するときに限り、$W_{\mathrm{fin}}$ と $W'_{\mathrm{fin}}$ は同型となることが示される。

実際の証明では、より詳しく、$W$ と $W'$ の間の同型写像の性質についても言及している。その結果を $W = W'$ の場合に適用することで、$W$ の有限成分 $W_{\mathrm{fin}}$ は (群構造のみならず集合として) 生成系 $S$ に依らず一意に定まることが示される。また、更に $S = S'$ も仮定することで、この結果から $W$ の自己同型群 $\mathrm{Aut}(W)$ の記述が得られる。その紹介の前に更に記号を導入する。$W_{\mathrm{fin}}$ と同様に、$W$ の既約成分で無限群であるもの全体の積を $W_{\mathrm{inf}}$ で表す[9]。すると、各準同型写像 $f : W_{\mathrm{inf}} \to Z(W)$ は自然に準同型 $W \to Z(W)$ まで延長されるが、このとき以下の写像

$$f^\flat : W \to W, \quad f^\flat(w) = wf(w)^{-1} \quad (w \in W)$$

は $W$ の自己同型であることが示される。このような $f^\flat$ 全体の集合を $H_1$ とおく。また、$H_2 = \mathrm{Aut}(W_{\mathrm{fin}})$、$H_3$ を $W_{\mathrm{inf}}$ の自己同型でその制限写像が各既約成分の自己同型を定め

[8] $W_{\mathrm{fin}}$ の各既約成分は有限群であるが、それらが無限個存在する場合もあるので、$W_{\mathrm{fin}}$ 自体は必ずしも有限群とは限らないことに注意されたい。

[9] 有限成分とは違い、この $W_{\mathrm{inf}}$ は一般には生成系の選び方に依存する。

るもの全体、$H_4$ を $W_{\mathrm{inf}}$ の互いに同型な既約成分の入れ替えのなす $\mathrm{Aut}(W)$ の部分群とおく。この記号の下で、次のような $\mathrm{Aut}(W)$ の分解が得られる。

**定理 3.2** ([11]) $\mathrm{Aut}\, W = (H_1 \rtimes (H_2 \times H_3)) \rtimes H_4$.

定理 3.1 や定理 3.2 の証明は、定理 1.2 を基に、群の直既約分解に関する Krull-Remak-Schmidt の定理と同様の方針で得られる[10]。また、煩雑になるので詳細は割愛するが、$H_2 = \mathrm{Aut}(W_{\mathrm{fin}})$ の構造も、やはり K-R-S 定理の類似品として、$W_{\mathrm{fin}}$ の既約成分の自己同型群を用いて記述することができる。なお、各（有限）既約成分の自己同型群の構造に関しては坂内英一先生の論文 [1] を参照されたい。

更に、自己同型群 $\mathrm{Aut}(W)$ は以下の性質も持つ。定義の準備であるが、$W$ の自己同型で各既約成分をある既約成分の上に写すものをここでは $W$ の**自然な自己同型**と呼ぶ。また、Coxeter グラフ $\Gamma = \Gamma(W, S)$ から、ラベルが奇数でない辺を全て取り除いたグラフ $\Gamma^{\mathrm{odd}}$ を、$(W, S)$ に対応する *odd Coxeter* グラフと呼ぶ。

**命題 3.3** ([11]) 一般の Coxeter 系 $(W, S)$ に対して以下は同値である：

1. $\mathrm{Aut}(W)$ の中で、$W$ の自然な自己同型が生成する部分群は指数有限である。
2. $Z(W) = 1$ であるか、もしくは $(W, S)$ に対応する odd Coxeter グラフが連結成分を有限個しか持たない。

特に、$W$ が有限生成ならば $\Gamma$ 自体が連結成分を有限個しか持たないので、条件 2 は常に満たされ、従って $W$ は性質 1 も常に持つことがわかる。なお、$\Gamma^{\mathrm{odd}}$ の連結成分の個数は生成系 $S$ に依らないことが示せるので、上の条件 2 も $S$ の選び方とは独立である。

# 4 同型問題の歴史と最近の進展

## 同型問題の歴史

3 節とは順番が前後するが、ここで同型問題の歴史について簡単に触れておく。有限既約 Coxeter 群については、H. S. M. Coxeter 氏によって 1930 年代半ばには既に分類が完了しており、その後も有限単純群論との絡み[11]もあって詳しく調べられている。しかし、一般の同型問題に関しては、A. M. Cohen 氏の比較的新しい論文 [3]（1991 年）において「既約な無限 Coxeter 群は常に rigid か」との問い (Problem 6.5) が提示されていることからも、近年まで殆ど研究がなされていなかったことが伺い知れる。

この状況を打破する大きなきっかけとなったのが、B. Mühlherr 氏による 2000 年の論文 [7] である[12]。その論文の内容は、図 3 に示された互いに同型でない二つの連結な Coxeter

[10]ただし、この場合に K-R-S 定理自体を適用できるとは限らない。また、証明も全く同じに進むわけではなく、多少の工夫が必要である。

[11]例えば、$E_7$ 型と $H_3$ 型の有限 Coxeter 群の直既約因子のうち位数 2 でない方は、それぞれ単純群 $S_6(2)$ と $A_5$ である。

[12]本稿の参考文献表のページ数の記載は誤植ではなく、実際にこの論文は 1 ページで完結している。

グラフが同型な Coxeter 群を定めるというもので、上記の Cohen 氏の問いに対する否定的な答えを与えたものである。Mühlherr 氏の与えた同型写像の構成法は、2年後の同氏らの論文 [2] において「diagram twisting」という一般的手法に昇華され、同型問題の研究における重要な役割を担うことになった。

その頃を皮切りに同型問題に関する多くの結果が世に出始め、Mühlherr 氏の最新のプ

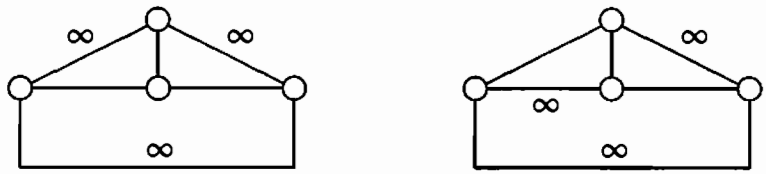



図 3: Mühlherr 氏が与えた、Cohen 氏の問いに対する解答

レプリント [8] によると、後に紹介するように、現在では有限生成な Coxeter 群の場合には完全解決の一歩手前まで到達しているとのことである。

## diagram twisting

diagram twisting の定義を述べる前に、有限放物型部分群 $W_I$ の最長元 $w_0(I)$ は「$I$ の元の $w_0(I)$ による共役はまた $I$ の元」という性質を常に持つことを注意しておく。さて、diagram twisting の定義は以下の通りである。

**定義 4.1** (Mühlherr 等 [2]) $(W,S)$ を Coxeter 系、$\Gamma=\Gamma(W,S)$ とする。$S$ の互いに交わらない部分集合 $I,J$ が、

1. $W_J$ は有限群
2. $s$ を $I$、$J$ に含まれない $S$ の任意の元とすると、$s$ は $I$ の全ての元と（$\Gamma$ において）$\infty$ をラベルに持つ辺で結ばれているか、もしくは $J$ のどの元とも（$\Gamma$ において）辺で結ばれていない

を満たすとする。このとき「$I$ の任意の元 $s$ と $J$ の任意の元 $t$ を結ぶ $\Gamma$ の辺を、$t$ の代わりに $w_0(J)tw_0(J)^{-1}\in J$ へ繋ぎ直す」という操作を、対 $(I,J)$ に対応する *diagram twisting* と呼ぶ。

つまり $(I,J)$ に対応する diagram twisting とは、$I$ から $J$ へ向かう $\Gamma$ の辺を一旦 $J$ から引き抜き、$w_0(J)$ の作用でその辺たちを捻ってまた $J$ へ差し込む操作である。例えば図3において、左端の1点を $I$、中間の縦に並んだ2点を $J$ とおくと、$(I,J)$ に対応する diagram twisting を左側のグラフに施すと右側のグラフが得られ、逆も成り立つ。

diagram twisting に対応する同型写像の構成法は以下の通りである。

**定理4.2** ([2]) 定義4.1のdiagram twistingで得られたCoxeterグラフ$\Gamma'$は$W$と同型なCoxeter群を定める。より詳しくは、$W$の部分集合$S'$を

$$S' = \{w_0(J)sw_0(J) \mid s \in I\} \cup (S \setminus I)$$

で定めると、$(W, S')$はCoxeterグラフ$\Gamma'$に対応するCoxeter系である。

ここで注目すべきことは、$W$の新しい生成系$S'$はもとの生成系$S$に関する鏡映からなるという点である。なお、$W$において$S$のある元と共役な元を$W$の（$S$に関する）鏡映(*reflection*)と呼び、その全体をここでは$R_S(W)$と書く。すると上記の性質は$S' \subset R_S(W)$と言い換えられるが、[2]によればこのことから関係$R_{S'}(W) = R_S(W)$が導かれる。つまりdiagram twistingは、対応するCoxeter群のみならずその鏡映集合をも保つ操作である。

更に、上記の事実の「逆」とも言える予想が同じ論文[2]において提示されている。

**予想4.3** ([2]) もしCoxeter群$W$の二つの生成系$S$、$S'$が共に有限集合であり[13]、それらの定める鏡映集合が等しければ、$\Gamma(W, S)$と$\Gamma(W, S')$はdiagram twistingの繰り返しによって互いに移り合える。

## 最近の進展 — 有限生成の場合

詳細は複雑になるので割愛するが、上述のdiagram twisting以外にも、対応するCoxeter群を保つようなCoxeterグラフの局所的な変形が[8]においていくつか与えられている。ここではそれらをCoxeterグラフの基本変形と呼ぶことにする。最も簡単な例の一つは、Coxeter群の自由積[14]の間の同型$W * W(B_n) \simeq W * W(A_1 \times D_n)$（$n$は3以上の奇数）に対応する変形であり、これは左辺に対応するCoxeterグラフのうち因子$W(B_n)$に相当する部分を$A_1 \times D_n$型のグラフに置き換える操作である。(実際には、もう少し弱い前提の下でもこれと同種の基本変形が定義される。)

Mühlherr氏らによる最近の研究により、有限生成なCoxeter群の同型問題に関しては、次のような著しい結果が得られている。

**定理4.4** ([8]) Coxeter群$W$の二つの生成系$S$、$S'$が共に有限集合であると仮定する。このとき、$W$の生成系$S''$で、$\Gamma(W, S'')$は$\Gamma(W, S)$に対する基本変形の繰り返しで得られ、更に$R_{S''}(W) = R_{S'}(W)$であるものが存在する。

従って、もし予想4.3が正しいとすると、定理4.4の系として次が得られる。

**予想4.5** 二つの有限なCoxeterグラフが同型なCoxeter群を定める必要充分条件は、それらが基本変形とdiagram twistingの繰り返しで互いに移り合えることである。

---

[13]原論文[2]ではこの仮定については触れられていないが、この仮定抜きだと反例が存在する。

[14]直積の場合と同様に、Coxeter群の自由積もまた自然にCoxeter群となる。

予想 4.3 や 4.5 は、Coxeter 群のいくつかのクラス（例えば後述の"2-spherical" な Coxeter 群）においては成立する[15]ことが確かめられており、その手法を応用して一般の（有限生成の）場合にも証明できると信じられている。この意味で、有限生成 Coxeter 群の同型問題は解決まであと一歩と言えよう。

## 5 筆者の結果 2 — 有限生成でない場合

4 節では同型問題に関する最新の研究状況について紹介したが、それらは有限生成な Coxeter 群に限ったものであった[16]。そのような仮定の下では予想 4.3 のような有力な予想や定理 4.4 のような強力な結果が与えられているのであるが、この有限生成性の仮定を外すと状況はもっと複雑になる。実際、定理 4.4 の証明においては Coxeter 群の極大な有限部分群が重要な役割を果たすのであるが、有限生成でない場合には極大な有限部分群が存在しない可能性もあるので、その証明はそのままでは一般の場合に拡張できない。また、有限生成という仮定を外すと、後述のように予想 4.3 の簡単な反例が存在する。

同型問題に関する既存の研究の対象は殆ど全てが有限生成な Coxeter 群であるが、筆者は有限生成とは限らない一般の場合を研究しているので、ここでは一般の同型問題に関する結果の例として筆者の最新の結果を紹介する。その結果は大まかに言えば、Coxeter 群の間の同型写像 $f : W \xrightarrow{\sim} W'$ による $W$ の生成元 $s \in S$ の像 $f(s) \in W'$ が、$W'$ においてどのような形をしているかを調べる手法である。特にこの結果は、このような $f(s)$ が $(W', S')$ や $f$ の選び方に依らずに常に $W'$ の鏡映となるための $(W, S)$ や $s$ に関する充分条件を与えている。

まず準備であるが、Coxeter 系 $(W, S)$ と $I \subset S$ について、$Z_W(W_I) \setminus I$ に属する $W$ の（$S$ に関する）鏡映全体が生成する $W$ の部分群を $W^{\perp I}$ と記す。V. V. Deodhar 氏 [4] や M. Dyer 氏 [5] の定理により、この $W^{\perp I}$ はある canonical な生成系に関して Coxeter 群をなす。その $W^{\perp I}$ の有限成分を $W^{\perp I}{}_{\mathrm{fin}}$ で表す。一方、同型写像 $f : W \xrightarrow{\sim} W'$ と $s \in S$ に関して、$f(s)$ は $W'$ の位数 2 の元なので、2 節で用いた Richardson 氏の定理より、部分集合 $I' \subset S'$ で

- $W'_{I'}$ は有限群、かつ $W'_{I'}$ の最長元 $w_0(I')$ は $W'_{I'}$ の中心 $Z(W'_{I'})$ に含まれる
- $f(s)$ は $w_0(I')$ と $W'$ で共役

となるものが存在する。「鏡映である」というのは共役で保たれる性質なので、以下では初めから $f(s) = w_0(I')$ であるとして話を進めることにする。

このとき、以下が筆者の件の結果である。

**定理 5.1** （縫田 [10]）このような状況の下で、$W'_{I'}$ の $W'$ における正規化群 $N_{W'}(W'_{I'})$ のある有限部分群 $G$ が存在して、$f$ の制限が同型写像

$$f : \langle s \rangle \times W^{\perp s}{}_{\mathrm{fin}} \xrightarrow{\sim} (W'_{I'} \times W'^{\perp I'}{}_{\mathrm{fin}}) \rtimes G$$

[15] より強く、無限、既約、2-spherical な Coxeter 群は strongly rigid であることが示されている。
[16] ただし、diagram twisting の定義自体は有限生成でなくとも通用する。

となる。

より詳しく、Coxeter系 $(W', S')$ と部分集合 $I' \subset S'$ からこの部分群 $G$ を具体的に特定することができる。なお、筆者は大抵の場合には $G$ は単位群であると予想している。この結果の系として直ちに以下が得られる。

**系 5.2** もし $W^{\perp_s}$ の有限成分 $W^{\perp_s}_{\mathrm{fin}}$ が単位群であれば、$(W', S')$ や $f$ の選び方に依らず、($|I'| = 1$ であるから) 像 $f(s)$ は $W'$ の鏡映である。

さらに、筆者の別のプレプリント [9] において、$W^{\perp_s}$ の有限成分の構造が完全に特定されている。その結果を観察することで以下の充分条件が得られる。

**定理 5.3** (縫田 [9]) もし、$W$ が無限群である既約 Coxeter系 $(W, S)$ が以下のいずれか

- $\Gamma(W, S)$ のどの辺もラベル $\infty$ を持たない (*2-spherical* と呼ばれる)
- $(W, S)$ に対応する odd Coxeter グラフが連結である[17]

を満たすならば、$W$ の生成系 $S'$ は全て $S$ に関する鏡映集合 $R_S(W)$ の部分集合である。特に、このような $W$ の鏡映集合は生成系の選び方に依らずに一意に定まる (このような $W$ は *reflection independent* と呼ばれる)。

なお、定理5.3の証明には系5.2を用いるが、定理5.3の状況で系5.2が常に適用できるわけではないことを注意しておく。実際には、系5.2を適応できない例外的な場合が少々存在するので、それらについては個別に議論することでこの定理を証明している。

## 付録1：有限既約Coxeter群の諸性質の表

Coxeter群 $W$ の (strong) rigid性の定義に現れる生成系を、ある与えられた生成系 $S$ に関する鏡映集合 $R_S(W)$ の部分集合に制限することで、より弱い性質である *(strong) reflection rigid* 性が定義される。下表は有限既約 Coxeter群のこれらの性質をまとめたものである。なお、有限既約 Coxeter群は全て reflection rigid であることが知られている ([2]) ため、その性質は表には記載していない。

## 付録2：有限既約Coxeter群のある極限に関して

有限既約 Coxeter群の無限系列としては $A, B, D$ の3系列が存在する。ここで、自然な埋め込みによって得られる昇鎖 $W(A_1) \subset W(A_2) \subset W(A_3) \subset \cdots$ の極限として得られる無限既約 Coxeter群を $W(A_\infty)$ と書き、同様に $B$ 型、$D$ 型の系列から極限 $W(B_\infty), W(D_\infty)$ を定める。一方、$A$ 型の極限を取る際に Coxeter グラフを片側ではなく両側に延長してい

[17] この条件は、「$S$ の各元が互いに共役」もしくは「$W$ が指数2の部分群をただ一つ含む」ことと同値である。後者の言い換えより、この条件は生成元 $S$ の選び方に依らない。

| 型 | | strongly rigid | rigid | strongly reflection rigid | reflection independent |
|---|---|---|---|---|---|
| $A_n$ | $(n \neq 5)$ | ○ | ○ | ○ | ○ |
| $A_6$ | | × | ○ | ○ | × |
| $B_2$ | | ○ | ○ | ○ | ○ |
| $B_n$ | $(n \geq 3$ odd$)$ | × | × | ○ | × |
| $B_n$ | $(n \geq 4$ even$)$ | × | ○ | ○ | × |
| $D_n$ | $(n \geq 5$ odd$)$ | ○ | ○ | ○ | ○ |
| $D_n$ | $(n \geq 4$ even$)$ | × | ○ | ○ | × |
| $E_6$, $E_7$ | | ○ | ○ | ○ | ○ |
| $E_8$ | | × | ○ | ○ | × |
| $F_4$ | | × | ○ | ○ | × |
| $H_3$ | | × | ○ | × | ○ |
| $H_4$ | | × | ○ | × | × |
| $I_2(m)$ | $(m \not\equiv 2 \pmod 4)$ | × | ○ | × | ○ |
| $I_2(6)$ | | × | × | ○ | × |
| $I_2(4k+2)$ | $(k \geq 2)$ | × | × | × | × |

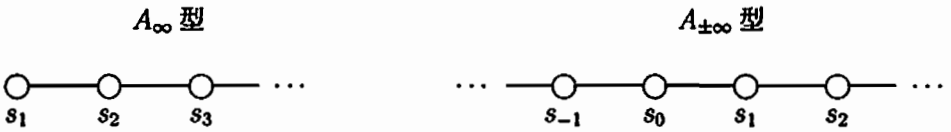



図 4: $A_\infty$ 型と $A_{\pm\infty}$ 型の Coxeter グラフ

くことで、別の極限 $W(A_{\pm\infty})$ が得られる（図 4)。このとき [11] において、これら 4 種類の Coxeter 群が、「無限群で直既約、かつ任意の有限生成部分群が有限群である」ような Coxeter 群の全てであることが示されている。この条件は生成系に依らない条件であるから、これら 4 種類の Coxeter 群の集合は同型という関係に関して閉じていることがわかる。なお、定理 5.3 よりこれらの Coxeter 群は全て reflection independent である。

すると、[9] の結果も用いることで、$W(B_\infty)$ と $W(D_\infty)$ はこれら 4 種類の中で

$B_\infty$ 型：odd Coxeter グラフが連結でない

$D_\infty$ 型：odd Coxeter グラフが連結であり、$W^{\perp s}$ $(s \in S)$ の有限成分が単位群でない

という性質で特徴付けられる。このことから $W(B_\infty)$ と $W(D_\infty)$ は共に rigid である。一方、$W(A_\infty)$ と $W(A_{\pm\infty})$ は共に対称群 $S_n$ の極限 $S_\infty = \bigcup_{n=1}^{\infty} S_n$ として実現される[18]ため、これらは rigid ではない。これが有限生成でない場合の、予想 4.3 の反例である。

[18] $W(A_\infty)$ の生成元としては隣接互換 (12), (23),...、一方 $W(A_{\pm\infty})$ の生成元としては互換 ..., (75), (53), (31), (12), (24), (46),... を取れる。

## 参考文献


[1] E. Bannai, *Automorphisms of irreducible Weyl groups*, J. Fac. Sci. Univ. Tokyo Sect. I 16 (1969) 273–286.

[2] N. Brady, J. P. McCammond, B. Mühlherr, W. D. Neumann, *Rigidity of Coxeter groups and Artin groups*, Geom. Dedicata 94 (2002) 91–109.

[3] A. M. Cohen, *Coxeter groups and three related topics*, Generators and Relations in Groups and Geometries (A. Barlotti et al.), NATO ASI Series, Kluwer Acad. Publ. (1991) pp. 235–278.

[4] V. V. Deodhar, *A note on subgroups generated by reflections in Coxeter groups*, Arch. Math. 53 (1989) 543–546.

[5] M. Dyer, *Reflection subgroups of Coxeter systems*, J. Algebra 135 (1990) 57–73.

[6] J. E. Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge Univ. Press., 1990.

[7] B. Mühlherr, *On isomorphisms between Coxeter groups*, Des. Codes Cryptogr. 21 (2000) 189–189.

[8] B. Mühlherr, *The isomorphism problem for Coxeter groups*, preprint.

[9] K. Nuida, *Centralizers of reflections and reflection independence of Coxeter groups*, preprint.

[10] K. Nuida, *On extensions of Coxeter groups by Coxeter graph automorphisms*, preprint.

[11] K. Nuida, *On the direct indecomposability of infinite irreducible Coxeter groups and the Isomorphism Problem of Coxeter groups*, arXiv:math.GR/0501276 (2005), to appear in Comm. Algebra.

[12] L. Paris, *Irreducible Coxeter groups*, arXiv:math.GR/0412214 (2004).

[13] R. W. Richardson, *Conjugacy classes of involutions in Coxeter groups*, Bull. Austral. Math. Soc. 26 (1982) 1–15.