

第18回 代数的組合せ論シンポジウム 報告集

2001年7月2日～7月4日
於 千葉大学 けやき会館

平成13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

まえがき

この報告集は、2001年7月2日（月）から7月4（水）にわたって、千葉大学けやき会館で行われた「第18回代数的組合せ論シンポジウム」の講演記録です。

梅雨明けも近い暑い日々の中、80人近い出席者を得て盛会でした。また、集会中の懇親会は、本年60才の還暦を迎えられた、原田耕一郎先生・小関道夫先生のお二人に対し、ささやかなお祝いの会として開かせていただきました。

なお、この報告集の作成は、文部科学省科学研究費補助金の

基盤研究(B)（課題番号：13440011, 研究代表者：坂内英一 九大・数理）

に依っています。また、集会に関わる講演者の旅費については、上記の他、

基盤研究(B)（課題番号：13440001, 研究代表者：吉田知行 北大・理）

基盤研究(B)（課題番号：13440002, 研究代表者：宮本雅彦 筑波大・数学）

基盤研究(B)（課題番号：12440003, 研究代表者：北詰正顕 千葉大・理）

の研究旅費を使用いたしました。

講演者を始め、集会の開催にご協力いただいた皆様に、深く感謝致します。

2001年11月

千葉大学理学部
北詰 正顕

第18回代数的組合せ論シンポジウム

標記の研究集会を下記の要領で開催しますので、ご案内申し上げます。

世話人：北詰 正顕（千葉大・理）

日程：2001年7月2日(月) - 4日(水)

場所：千葉大学 けやき会館 レセプションホール

JR「西千葉」、京成「みどり台」下車・徒歩8分

プログラム

7月2日(月)

10:00-10:50 花木 章秀（信州大・理）、平坂 貢（浦項工大）

アソシエーションスキームの指標

11:00-11:50 田中 太初（九大・数理）

The decomposition of the permutation character $1_{GL(2n,q)}$
 $1_{GL(n,q^2)}$

13:30-14:20 角 俊雄（九州芸工大）

強ギャップ条件を満たす表現について

14:30-15:00 坂内 悦子（九大・数理）

ユークリッド空間上の antipodal な s -距離集合

15:10-15:40 平峰 豊（熊本大・教育）

指数2の巡回部分群をもつ2群における半正則相対差集合の分類

15:50-16:40 関口 次郎（東京農工大）

E型ルート系と実射影平面の直線配置

7月3日(火)

10:00-10:30 小田 文仁（富山工業高専）

Parabolic Burnside rings and symmetric functions

10:40-11:10 水川 裕司（北大・理）

分解する Schur 関数

11:20-11:50 渡辺 アツミ（熊本大・理）

Morita equivalence of Isaacs correspondence for blocks of
finite groups

- 13:30-14:20 大浦 学 (札幌医大)
Some results on the graded rings coming from coding theory
- 14:30-15:20 小関 道夫 (山形大・理)
McKay's 40 dimensional even unimodular lattice as ternary code construction
- 15:30-16:20 宮本 雅彦 (筑波大・数学)
頂点作用素代数のテンソル加群とモジュラー変換
- 16:30-17:20 原田 耕一郎 (オハイオ州立大)
シロー 2 群と 3 5 年
- 17:30-19:30 懇親会 (けやき会館レストランコルザ)

7 月 4 日 (水)

- 10:00-10:50 山田 裕理 (一橋大・経済)
Highest weight vectors in lattice vertex operator algebras
- 11:00-11:50 C. Dong (Univ. of California)
Automorphism groups of vertex operator algebras
- 13:30-14:00 山内 博 (筑波大・数学)
Intertwining operators in orbifold theory
- 14:10-14:40 田辺 顕一郎 (筑波大・数学)
長さ $24n + 16$ の extremal doubly-even code のコセットと 1-デザインについて
- 14:50-15:20 原田 昌晃 (山形大・理), 北詰 正顕 (千葉大・理)
On frames of the Niemeier lattices
- 15:30-16:00 寺田 幸代 (金沢大・自然科学)
A combinatorial problem in $SL(2, q)$
- 16:10-16:40 波多野 順 (千葉大・自然科学)
有限群の指標とその複素共役との積

目次

1. 花木 章秀 (信州大・理)	
アソシエーションスキームの指標	1
2. 田中 太初 (九大・数理)	
The decomposition of the permutation character $1_{GL(n,q^2)}^{GL(2n,q)}$	7
3. 角 俊雄 (九州芸工大)	
強ギャップ条件を満たす表現について	13
4. 坂内 悦子 (九大・数理)	
ユークリッド空間上の antipodal な s -距離集合	18
5. 平峰 豊 (熊本大・教育)	
指数 2 の巡回部分群をもつ 2 群における半正則相対差集合の分類	23
6. 関口 次郎 (東京農工大)	
E 型ルート系と実射影平面の直線配置	32
7. 小田 文仁 (富山工業高専)	
Parabolic Burnside rings and symmetric functions	51
8. 水川 裕司 (北大・理)	
分解する Schur 関数	59
9. 渡辺 アツミ (熊本大・理)	
Morita equivalence of Isaacs correspondence for blocks of finite groups	68
10. 大浦 学 (札幌医大)	
Some results on the graded rings coming from coding theory	74
11. 小関 道夫 (山形大・理)	
McKay's 40 dimensional even unimodular lattice as ternary code construction	84
12. 宮本 雅彦 (筑波大・数学)	
頂点作用素代数のテンソル加群とモジュラー変換	93
13. 原田 耕一郎 (オハイオ州立大)	
シロー 2 群と 35 年	101
14. 山田 裕理 (一橋大・経済)	
Highest weight vectors in lattice vertex operator algebras	106
15. 山内 博 (筑波大・数学)	
Intertwining operators in orbifold theory	116
16. 田辺 顕一朗 (筑波大・数学)	
長さ $24n + 16$ の extremal doubly-even code のコセットと 1-デザインについて	126
17. 原田 昌晃 (山形大・理)	
On frames of the Niemeier lattices	131
18. 寺田 幸代 (金沢大・自然科学)	
A combinatorial problem in $SL(2,q)$	137
19. 波多野 順 (千葉大・自然科学)	
有限群の指標とその複素共役との積	142

アソシエーションスキームの指標

平坂 貢 (浦項工科大学), 花木 章秀 (信州大学)

アソシエーションスキームは代数的組合せ論の主要な研究対象であり、組合せ論的な性質と代数的な性質を合わせ持っている。アソシエーションスキームに関する研究は可換性を仮定して行われることが多い。特に有名な坂内 - 伊藤のテキスト [1] ではほとんどの部分で可換性を仮定している。これは応用上、可換の場合が特に重要と思われるからであろう。しかし可換を仮定したのでは、アソシエーションスキームの理論が有限群や置換群の Hecke 環の概念を含むとはいえない。ここでは可換性を仮定しないアソシエーションスキームを考える。アソシエーションスキームの研究には、先に述べたように組合せ論的な方法と代数的な方法がある。ここでは代数的な方法、特に表現論を考える。ここでいう表現とはアソシエーションスキームから自然に定義される代数、隣接代数、の線形表現である。隣接代数は有限群の群環、置換群の Hecke 環の自然な拡張となっているため、その表現論の拡張を考えるのは自然であろう。

隣接代数は群環と似ていて、標数 0 の体上では半単純、正標数ではそうとは限らない。ここでは複素数体上の表現のみを考える。したがってその表現論は、指標の理論といってもよい。アソシエーションスキームの指標の理論は、可換の場合には [1] でかなり詳しく述べられているが、一般の場合にはあまりよく分かっていない。Zieschang の本 [7] に基本的なことは書かれているが、十分とは思えない。ここでは特に一つの問題を考えるのではなく、最近得られたいくつかの結果について報告する。定義や記号は主に [7] と同じものを用いる。§4 は論文 [4], §5 は論文 [5] の内容である。

1 定義

X を有限集合とし $X \times X$ の分割

$$X \times X = \bigcup_{g \in G} g, \quad (\text{disjoint})$$

を考える。 $g \in G$ に対して隣接行列 σ_g を考える。すなわち σ_g は $X \times X$ で添字の付けられた行列で $(x, y) \in g$ のときその成分は 1 で、そうでないときには 0 である。 (X, G) がアソシエーションスキームであるとは (1) $1 = \{(x, x) \mid x \in X\} \in G$, (2) $g \in G$ ならば $g' = \{(y, x) \mid (x, y) \in g\} \in G$, (3) 任意の $f, g, h \in G$ に対して $\sigma_f \sigma_g = \sum_{h \in G} a_{fgh} \sigma_h$ となる a_{fgh} がある、の三つの条件を満たすことをいう。このとき a_{fgh} は非負整数である。 (X, G) を単に G とも書くことにする。

$x \in X, g \in G$ に対して $xg = \{y \in X \mid (x, y) \in g\}$ とする。 $H \subseteq G$ に対しても $xH = \bigcup_{h \in H} xh$ とする。 $f, g \in G$ に対して $fg = \{h \in G \mid a_{fgh} \neq 0\}$ とする。 G の部分集合などについても同様である。アソシエーションスキームの定義から $|xg|$ は $x \in X$

の取り方によらず $g \in G$ のみで定まる。これを g の valency といい n_g で表す。 $H \subseteq G$ について $n_H = \sum_{h \in H} n_h, \sigma_H = \sum_{h \in H} \sigma_h$ とする。特に $n_G = |X|$ で、これをアソシエーションスキームの位数という。

アソシエーションスキーム (X, G) に対して、定義の条件 (3) より、自然に代数が定義できる。単位元を持つ可換環 \mathcal{O} に対して

$$\mathcal{O}G = \bigoplus_{g \in G} \mathcal{O}\sigma_g$$

に行列の積で代数構造を入れたものを G の \mathcal{O} 上の隣接代数という。標数 0 の体上の隣接代数は半単純であることが知られている。特に $\mathcal{C}G$ は半単純である。

任意の $g \in G$ に対して $n_g = 1$ であるとき G は thin であるという。thin なアソシエーションスキームは本質的に有限群であり、その隣接代数は群環に同型である。

$H \subseteq G$ が closed subset であるとは $HH \subseteq H$ を満たすことをいう。また closed subset H が normal closed subset であるとは、任意の $g \in G$ に対して $gH = Hg$ となることをいう。closed subset, normal closed subset は有限群の部分群、正規部分群に相当する。それは次の命題から分かるであろう。

命題 1.1. $H \subseteq G$ が closed subset であることと $e_H = n_H^{-1}\sigma_H$ がべき等元であることは同値である。また H が normal closed subset であることと e_H が $\mathcal{C}G$ の中心的べき等元であることは同値である。

H を G の closed subset とする。 $X/H = \{xH \mid x \in X\}$ とする。 $g \in G$ に対して $g^H = \{(xH, yH) \in X/H \times X/H \mid (x_0, y_0) \in g, \text{ for some } x_0 \in xH \text{ and } y_0 \in yH\}$ とし $G/H = \{g^H \mid g \in G\}$ とおく。このとき $(X/H, G/H)$ はアソシエーションスキームになる。これを (X, G) の H による剰余スキームという。群の場合は正規部分群でない剰余群を考えることは出来ないが、アソシエーションスキームでは剰余スキームの定義に正規性は必要ない。

2 指標と直交関係

以後しばらくは複素数体 \mathbb{C} 上の表現のみを考える。 G は常にアソシエーションスキームとする。先に述べたように $\mathcal{C}G$ は半単純である [6, Problem 11.3]。したがって表現の同値類は、その指標によって決まる。 $\mathcal{C}G$ の既約指標の集合を $\text{Irr}(G)$ と表す。 $\mathcal{C}G$ はもともと行列環として定義されているので、自然な表現がある。これを標準表現、その指標を標準指標という。標準指標を γ_G と書く。標準指標の既約分解を

$$\gamma_G = \sum_{\chi \in \text{Irr}(G)} m_\chi \chi$$

とし m_χ を単に χ の重複度という。

命題 2.1. $\chi \in \text{Irr}(G)$ に対して $m_\chi \geq \chi(1)$ である。特に $m_\chi \neq 0$ である。

標準指標 γ_G について定義から明らかに $\gamma_G(\sigma_1) = n_G, \gamma_G(\sigma_g) = 0$ ($1 \neq g \in G$) が成り立つ。したがってこれは有限群の正則指標に相当すると考えられる。有限群の指標の直交関係は正則指標を用いて証明できる。それと同様にアソシエーションスキームについても標準指標を用いて直交関係が示される。

定理 2.2 (指標の直交関係 [7, Theorem 4.1.5 (ii)]). $\chi, \varphi \in \text{Irr}(G)$ について

$$\frac{1}{n_G} \sum_{g \in G} \frac{1}{n_g} \chi(\sigma_{g \cdot}) \varphi(\sigma_g) = \delta_{\chi\varphi} \frac{\chi(1)}{m_\chi}$$

この直交関係を有限群の場合と比較してみる。有限群では n_G は群の位数、 $n_g = 1$, $g \cdot$ は g の逆元、また $m_\chi = \chi(1)$ である。したがってこれは有限群の指標の直交関係の拡張となっている。ここで $\chi(\sigma_{g \cdot}) = \overline{\chi(\sigma_g)}$ が成り立つかという疑問が生じる。有限群の場合や可換なアソシエーションスキームの場合には σ_g が正規行列であることからこの関係が直ちに得られるが、一般には σ_g は正規行列ではない。すなわち $\sigma_g \sigma_{g \cdot} \neq \sigma_{g \cdot} \sigma_g$ となる場合がある。更に対角化可能でない場合もある。しかしこの関係が正しいことが直交関係から証明される。

定理 2.3. G の指標 χ と $g \in G$ に対して $\chi(\sigma_{g \cdot}) = \overline{\chi(\sigma_g)}$

Proof. χ は既約としてよい。 χ を与える表現を Φ とする。 $\overline{\Phi}(\sigma_g) = \overline{\Phi(\sigma_g)}$, $\Phi^*(\sigma_g) = \Phi(\sigma_{g \cdot})$ とすれば $\overline{\Phi}, \Phi^*$ も既約表現である。その指標を $\overline{\chi}, \chi^*$ とし直交関係を用いれば $\overline{\chi} = \chi^*$ となる。 \square

3 剰余スキームの表現

H を G の closed subset とする。剰余スキーム G/H の表現と G の表現の関係を調べる。これについては Hecke 環の表現の理論がほとんどそのまま適用できる。Hecke 環の表現については例えば Curtis - Reiner [2] を見て頂きたい。命題 1.1 より $e_H = n_H^{-1} \sigma_H$ はべき等元である。したがって e_H を単位元とする代数 $e_H CGe_H$ が考えられる。

命題 3.1. 代数として $e_H CGe_H \cong \mathbb{C}[G/H]$ が成り立つ。

この二つの代数を断り無しに同一視する。 CG は半単純であるから

$$CG \cong M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_s}(\mathbb{C})$$

と直和分解できる。 e_H をこれに対応して分解する。

$$e_H = f_1 + \cdots + f_s, \quad f_i \in M_{d_i}(\mathbb{C})$$

f_i はべき等元であるから $f_i \mapsto \text{diag}(1, \dots, 1, 0, \dots, 0)$ であるとして構わない。 $r_i = \text{rank } f_i$ とする。このとき明らかに

$$e_H CGe_H \cong M_{r_1}(\mathbb{C}) \oplus \cdots \oplus M_{r_s}(\mathbb{C})$$

である。ただし $r_i = 0$ のものも含まれている。以上より直ちに次が得られる。

定理 3.2. $\{\chi \in \text{Irr}(G) \mid \chi(e_H) \neq 0\}$ と $\text{Irr}(G/H)$ の間に自然な全単射がある。

CX を標準加群 (標準表現に対応する加群は集合 X を基底とする空間と考えられる) とすると CXe_H は $e_H CGe_H \cong \mathbb{C}[G/H]$ の標準加群になる。このことから次が得られる。

定理 3.3. 定理 3.2 の対応によって指標の重複度は保存される。

なぜ Hecke 環の理論がそのままの形で適用できるのかを考えてみる。 G が置換群から定義されるアソシエーションスキームであるとする。したがってそれは有限群 A とその部分群 B で定義される。このとき closed subset は B を含む部分群 C に対応する (置換群で考えれば imprimitive block)。このとき剰余スキームは A と C で定義されるアソシエーションスキームになり、すべては Hecke 環の理論で説明できることになる。

4 Normal closed subset による剰余スキームの表現

ここでは G の normal closed subset H による剰余スキームを考える。この場合は e_H が中心的べき等元なので、埋め込み $e_H CG e_H \rightarrow CG$ が分裂する。更に基底の対応が整数を係数として与えられるので、次の定理が成り立つ。

定理 4.1. K を任意の体とする。 H を G の normal closed subset とするとき $KG \rightarrow K[G/H]$ ($\sigma_g \mapsto (n_g/n_{gH})\sigma_{gH}$) は代数の準同型である。ここで n_g/n_{gH} は常に有理整数である。

この準同型を通して任意の体上の G/H の表現は G の表現と見ることが出来る。しかし標数によっては $n_g/n_{gH} = 0$ となる場合もあるので一般にこれが全準同型になるわけではない。標数が 0 であれば常に全準同型である。特に指標については次が成り立つ。

定理 4.2. 自然な対応で $\text{Irr}(G/H) \subseteq \text{Irr}(G)$ と見ることが出来る。またこのとき重複度は保存される。

$\chi \in \text{Irr}(G)$ が $\text{Irr}(G/H)$ に入るために条件を考える。 $\chi, \varphi \in \text{Irr}(G)$ に対して $(\chi, \varphi)_G = \delta_{\chi\varphi}$ とし、これを任意の指標に線形に拡張して指標の内積を定義する。自明な指標とは $\sigma_g \mapsto n_g$ で定義されるもので、これを 1_G と書く。 $\chi \downarrow_H$ は指標の H への制限とする。 H の指標 ξ に対して、それを与える加群を M とする。 $M \otimes_{CH} CG$ は CG 加群である。その定義する指標を $\xi \uparrow^G$ と書く。また $\chi \in \text{Irr}(G)$ に対応する中心的べき等元を e_χ と書く。このとき次が成り立つ。

定理 4.3. $\chi \in \text{Irr}(G)$ に対して次は同値である。(1) $\chi \in \text{Irr}(G/H)$, (2) 任意の $h \in H$ に対して $\chi(\sigma_h) = n_h \chi(1)$, (3) $\chi \downarrow_H = \chi(1) \cdot 1_G$, (4) $(\chi \downarrow_H, 1_H)_H \neq 0$, (5) $(\chi, 1_H \uparrow^G) \neq 0$, (6) $\chi(e_H) \neq 0$, (7) $e_\chi e_H \neq 0$, (8) $e_\chi e_H = e_\chi$.

これを見ると想像できると思うが Frobenius の相互律は一般に成り立つ。Clifford 型の理論が成り立つかどうかは分かっていない。

5 指標の核の正規性

ここではアソシエーションスキームの指標表から何が読み取れるかという問題を考える。有限群の場合はすべての正規部分群が読み取れるが、アソシエーションスキーム場合はどうだろうか。 η を G の指標とする。

$$K(\eta) = \{g \in G \mid \eta(\sigma_g) = n_g \eta(1)\}$$

とおく。一般に $|\eta(\sigma_g)| \leq n_g \eta(1)$ が成り立ち、これは有限群の指標の核と類似の定義である。ただし準同型の核というわけではないので核という言葉を使うのは不適當かも知れない。

定理 5.1. $K(\eta)$ は closed subset である。

一般に $K(\eta)$ は normal であろうと思ひ、証明を試みたがうまく行かず、具体例を調べたところ反例を見付けることが出来た。したがって $K(\eta)$ は一般には normal ではない。正規性の判定条件を述べるためにもう一つの定義をする。

$$I(\eta) = \{ \chi \in \text{Irr}(G) \mid \chi(\sigma_g) = n_g \chi(1), \text{ for any } g \in K(\eta) \}$$

定理 5.2. $K(\eta)$ が normal closed subset であるための必要十分条件は

$$\sum_{\chi \in I(\eta)} m_\chi \chi(1) = \frac{n_G}{n_{K(\eta)}}$$

が成り立つことである。またこの条件は指標表から判定できる。更に任意の normal closed subset は $K(\eta)$ の形に書くことが出来る。

有限群や可換なアソシエーションスキームの場合には $K(\eta)$ は常に normal である。これを一般化した結果を述べる。アソシエーションスキーム G に次の同値関係を考える。 $g, h \in G$ に対して $g \sim h$ とは、任意の $\chi \in \text{Irr}(G)$ に対して $n_g^{-1} \chi(\sigma_g) = n_h^{-1} \chi(\sigma_h)$ となることとする。 G が thin, すなわち有限群ならば、この同値関係は共役であることである。また G が可換ならばすべての異なる元は同値ではない。このとき次が成り立つ。

定理 5.3. 上で定義した \sim 同値類の数が $|\text{Irr}(G)|$ と一致することと、 CG の中心が Hadamard 積で閉じていることとは同値である。またこの条件が成り立つとき、任意の指標 η に対して $K(\eta)$ は normal closed subset である。

6 一つの問題

最後に現在考えている問題を紹介する。問題は素数位数アソシエーションスキームは常に可換か、というものである。素数位数アソシエーションスキームの分類は一般には困難であるため、その隣接代数の分類を試みているが、この問題はそれよりも弱い問題である。状況を説明するため一つの結果を述べる。

定理 6.1 ([3, Theorem 3.4]). F を標数 $p > 0$ の体とし G を位数が p -べきのアソシエーションスキームとする。このとき FG は局所環である。

これから直ちに以下が得られる。

系 6.2. G を素数位数 p のアソシエーションスキームとし $\chi \in \text{Irr}(G)$ とする。このとき任意の $g \in G$ に対して $\chi(\sigma_g) \neq 0$ である。

この結果から有限群に関する次の結果が思い出される。

定理 6.3 (Burnside). G を有限群とし $\chi \in \text{Irr}(G)$, $\chi(1) > 1$ とする。このときある $g \in G$ があって $\chi(g) = 0$ である。

もし Burnside の定理がアソシエーションスキームに一般化されるならば、系 6.2 より任意の指標は一次となり、素数位数アソシエーションスキームは可換になる。

追記：発表時点では Burnside の定理がアソシエーションスキームに拡張できると思っていたが、その後位数 27 で反例が見つかった (2001/8/9)。したがって一般に拡張できるわけではないが、素数位数に限って考えればこの方法で可換性が証明できるかも知れない。

References

- [1] E. Bannai and T. Ito, "Algebraic Combinatorics I : Association Schemes", Benjamin-Cummings, Menlo Park CA, 1984.
- [2] C. W. Curtis and I. Reiner, "Methods of Representation Theory, Vol. 1", Wiley, New York, 1981.
- [3] A. Hanaki, Locality of a modular adjacency algebra of an association scheme of prime power order, to appear in Arch. Math.
- [4] A. Hanaki, Representations of association schemes and their factor schemes, preprint.
- [5] A. Hanaki, Characters of association schemes and normal closed subsets, preprint.
- [6] H. Nagao and Y. Tsushima, "Representations of Finite Groups", Academic Press, New York, 1989.
- [7] P.-H. Zieschang, "An Algebraic Approach to Association Schemes", Springer-Verlag, Berlin/New York, 1996.

The Decomposition of the Permutation Character $1_{GL(n,q^2)}^{GL(2n,q)}$

坂内 英一・田中 太初 (九大・数理)

1 Introduction

Inglis-Liebeck-Saxl [6] に於いて、次の4つの組 (G, H) についてその置換指標が multiplicity-free であることが述べられている。

- (i) $(G, H) = (GL(n, q^2), GL(n, q))$,
- (ii) $(G, H) = (GL(n, q^2), GU(n, q))$,
- (iii) $(G, H) = (GL(2n, q), Sp(2n, q))$,
- (iv) $(G, H) = (GL(2n, q), GL(n, q^2))$.

一般に有限群 G とその部分群 H に対して、 G の左剰余類 G/H への可移な作用から association scheme を構成することができ、その association scheme が可換であることと置換指標が multiplicity-free であることが同値であることが知られている (詳しくは Bannai [1]、Bannai-Ito [2] をご参照下さい)。従って、上に挙げた4つの組から4種類の可換な association schemes が得られることになる。有限群の可移な作用から得られる可換な association scheme については、その指標表を求めることと、全ての zonal spherical functions を求めることは同値であり、指標表 P の (j, i) -成分 $p_i(j)$ は次の公式で与えられる (Bannai-Ito [2, p.174 Corollary 11.7.]) :

$$\begin{aligned} p_i(j) &= \frac{1}{|H|} \sum_{x \in Hg_i H} \chi_j(x) \\ &= \frac{1}{|H|} \sum_k |Hg_i H \cap C_k| \chi_j(c_k) \end{aligned} \quad (1)$$

ただしここで、 $(1_H)^G = \chi_0 + \chi_1 + \dots + \chi_d$ は置換指標 $(1_H)^G$ の既約指標への分解、 $\{Hg_i H \mid 0 \leq i \leq d\}$ は G の H による両側剰余類の全体、 $\{C_k\}$ は G の共役類の集合、さらに c_k は C_k の代表元を表す。

次の表は、上述の4種類の association schemes について現在までに知られていることをまとめたものである。

	multiplicity-free	decomposition	double coset	character table
$GL(n, q^2)/GL(n, q)$	Gow	Gow	Gow	Kawanaka
$GL(n, q^2)/GU(n, q)$	Gow	Gow	Gow	Kawanaka
$GL(2n, q)/Sp(2n, q)$	Klyachko	Bannai-Kawanaka-Song	Klyachko	Bannai-Kawanaka-Song
$GL(2n, q)/GL(n, q^2)$	Inglis-Liebeck-Saxl		?	?

本稿では置換指標 $(1_{GL(n,q^2)})^{GL(2n,q)}$ の分解を完全に決定する (後述の Theorem 3)。なお、(iv) の場合の両側剰余類分解については、Inglis により近々決定されるものと期待される。

2 Preliminaries and the Main Result

まず、一般線形群 $G_n = GL(n, q)$ の既約指標のパラメータ付けについて、Macdonald [7, Chapter IV.] に従い、簡単に復習する。

\mathcal{P} を分割全体の成す集合とする。分割 $\lambda = (\lambda_1, \lambda_2, \dots) \in \mathcal{P}$ に対し、その length 及び weight をそれぞれ $l(\lambda) := \#\{i \mid \lambda_i \neq 0\}$, $|\lambda| := \sum_{i \geq 1} \lambda_i$ と定める。 λ_i ($i \geq 1$) が全て偶数 (resp. 奇数) であるとき、 λ は even (resp. odd) であるという。また、 λ の Young 図形の転置を Young 図形とするような分割を λ の conjugate と呼び、 λ' で表す。

有限体 \mathbb{F}_q 上の多項式環 $\mathbb{F}_q[t]$ に於いて t と異なるモニックな既約多項式の全体を Φ とする。このとき G_n の既約指標は Φ から \mathcal{P} への写像 $\mu: \Phi \rightarrow \mathcal{P}$ で

$$\|\mu\| := \sum_{f \in \Phi} d(f) |\mu(f)| = n$$

を満たすもの全体によりパラメータ付けされる。ここで $d(f)$ は f の次数を表す。写像 μ に対応する G_n の既約指標を χ_μ 、さらに χ_μ の次数を d_μ と書くことにする。特に単位指標 1_{G_n} は多項式 $t-1$ に分割 (1^n) を対応させる。

\mathbb{F}_q 上の次数 k の多項式 $f(t) = t^k + a_1 t^{k-1} + \dots + a_k$ で $a_k \neq 0$ を満たすものに対し

$$\bar{f}(t) := a_k^{-1} t^k f(t^{-1})$$

と定め、さらに写像 $\mu: \Phi \rightarrow \mathcal{P}$ に対しても

$$\bar{\mu}(f) := \mu(\bar{f}) \quad (f \in \Phi)$$

と定義する。次の補題は容易に確かめられる。

Lemma 1. *An irreducible character χ_μ of G_n is real-valued if and only if $\bar{\mu} = \mu$.*

K_{2n} を $GL(n, q^2)$ と同型な G_{2n} の部分群とする。このとき次の事実が知られている。

Theorem 2 (Inglis-Liebeck-Saxl [6]). *The permutation character $(1_{K_{2n}})^{G_{2n}}$ is multiplicity-free and every irreducible constituent of $(1_{K_{2n}})^{G_{2n}}$ is real-valued.*

本稿では、次の結果を紹介する。

Theorem 3. (i) *If q is odd, then we have $(1_{K_{2n}})^{G_{2n}} = \sum \chi_\mu$, summed over μ such that $\|\mu\| = 2n$, $\bar{\mu} = \mu$, and both $\mu(t-1)'$ and $\mu(t+1)$ are even.*

(ii) *If q is even, then we have $(1_{K_{2n}})^{G_{2n}} = \sum \chi_\mu$, summed over μ such that $\|\mu\| = 2n$, $\bar{\mu} = \mu$, and $\mu(t-1)'$ is even.*

(iii) *In either case, the generating function for the rank (i.e., the number of the irreducible constituents of the permutation character $(1_{K_{2n}})^{G_{2n}}$) is given by*

$$\sum_{n \geq 0} \text{rank}(G_{2n}/K_{2n}) t^{2n} = \prod_{r \geq 1} (1 - qt^{2r})^{-1} \quad (2)$$

with the understanding that $\text{rank}(G_0/K_0) = 1$. In particular we have

$$\text{rank}(G_{2n}/K_{2n}) = \sum q^{l(\lambda)}$$

summed over all partitions λ such that $|\lambda| = n$.

なお、(2) 式は Inglis により異なる方法を用いて既に得られていることを付け加えておく。

3 Sketch of the Proof of Theorem 3

次の結果は、証明に際し重要かつ基本的である。

Proposition 4. (i) *If q is odd, then we have*

$$\sum d_{\mu} = (q^{2n} - q)(q^{2n} - q^3) \dots (q^{2n} - q^{2n-1})$$

where the sum on the left is over μ such that $\|\mu\| = 2n$, $\hat{\mu} = \mu$, and both $\mu(t-1)'$ and $\mu(t+1)$ are even.

(ii) *If q is even, then we have*

$$\sum d_{\mu} = (q^{2n} - q)(q^{2n} - q^3) \dots (q^{2n} - q^{2n-1})$$

where the sum on the left is over μ such that $\|\mu\| = 2n$, $\hat{\mu} = \mu$, and $\mu(t-1)'$ is even.

要約すると Proposition 4 は、Theorem 3 の中で述べられている既約指標たちの次数の総和が、置換指標 $(1_{K_{2n}})^{G_{2n}}$ の次数に一致することを主張している。この命題は、Macdonald の本に掲載されている例 ([7, p.289, Example 5.]) の中で用いられている手法を適当に変形することにより証明される。

次に、Affine 部分群の既約表現に関する Zelevinsky [9] の結果を紹介する。まず、 H_n を G_n の Affine 部分群とする。すなわち

$$H_n := \left\{ \begin{pmatrix} 1 & y \\ 0 & x \end{pmatrix} \middle| x \in G_{n-1} \right\}.$$

また、

$$U_{n-1} := \left\{ \begin{pmatrix} 1 & y \\ 0 & 1_{n-1} \end{pmatrix} \right\} \cong \mathbb{F}_q^{n-1}$$

とし、さらに G_{n-1} を

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \middle| x \in G_{n-1} \right\}$$

と同一視して H_n の部分群とみなす。ただしここで、 1_{n-1} は $n-1$ 次の単位行列を表す。このとき U_{n-1} は H_n の可換正規部分群で、 H_n は U_{n-1} と G_{n-1} の半直積に分解される：

$$H_n = U_{n-1} \rtimes G_{n-1}.$$

H_n の既約指標は “little group method” により完全に決定される。すなわち、写像 $\nu : \Phi \rightarrow \mathcal{P}$ で $\|\nu\| < n$ を満たすもの全体によりパラメータ付けされることが示される (cf. [9, §13.]). 写像 ν に対応する H_n の既約指標を $\zeta_{\nu}^{(n)}$ と表すことにする。なお、 $\|\nu\| = n-1$ を満たす写像 ν に対応する既約指標 $\zeta_{\nu}^{(n)}$ は、 $G_{n-1} \cong H_n/U_{n-1}$ の既約指標 χ_{ν} から自然に得られる H_n の既約指標と一致することが分かる。

ここで一つ記号を導入する。 μ 及び ν を Φ から \mathcal{P} への写像とする。もし全ての $f \in \Phi$ と $i \geq 1$ に対して $\mu(f)_i - 1 \leq \nu(f)_i \leq \mu(f)_i$ が成り立つとき、 $\nu \vdash \mu$ と書くことにする。ちなみにこの条件は、 $\mu(f)_1 \geq \nu(f)_1 \geq \mu(f)_2 \geq \nu(f)_2 \geq \dots$ が全ての $f \in \Phi$ に対して成立することと同値である。

Theorem 5 ([9, §13.5.]). (i) *Let $\mu : \Phi \rightarrow \mathcal{P}$ be a partition-valued function such that $\|\mu\| = n$. Then we have*

$$\chi_{\mu} \downarrow_{H_n}^{G_n} = \sum \zeta_{\nu}^{(n)}$$

summed over ν such that $\|\nu\| < n$ and $\nu \vdash \mu$.

(ii) Let $\nu : \Phi \rightarrow \mathcal{P}$ be a partition-valued function such that $\|\nu\| < n$. Then we have

$$\zeta_\nu^{(n)} \downarrow_{G_{n-1}}^{H_{n-1}} = \sum \chi_\lambda$$

summed over λ such that $\|\lambda\| = n-1$ and $\nu \vdash \lambda$.

次の定理は Thoma [8] により証明されたものであるが、Theorem 5 から即座に導かれる。

Theorem 6 ([8]). Let $\mu : \Phi \rightarrow \mathcal{P}$ and $\lambda : \Phi \rightarrow \mathcal{P}$ be partition-valued functions such that $\|\mu\| = n$ and $\|\lambda\| = n-1$. Then the multiplicity of χ_μ in the induced character $\chi_\lambda \uparrow_{G_{n-1}}^{G_n}$ is equal to the number of $\nu : \Phi \rightarrow \mathcal{P}$ such that $\nu \vdash \mu$ and $\nu \vdash \lambda$.

次に紹介する2つの補題は、Theorem 3 を証明する際に強力な道具となる。

Lemma 7. $(1_{K_{2n}})^{G_{2n}} \downarrow_{G_{2n-1}}^{G_{2n}} = q \cdot (1_{K_{2n-2}})^{G_{2n-2}} \uparrow_{G_{2n-2}}^{G_{2n-1}}$.

Lemma 7 は、Mackey の定理より証明される。

Lemma 8. Let $(1_{K_{2n}})^{G_{2n}} = \sum_{i=1}^k \chi_{\mu_i}$, and $(1_{K_{2n-2}})^{G_{2n-2}} = \sum_{j=1}^l \chi_{\lambda_j}$. Then we have

$$\sum_{i=1}^k \sum_{\substack{\|\nu\|=2n-1 \\ \nu \vdash \mu_i}} \chi_\nu = \sum_{j=1}^l \sum_{\substack{\|\nu\|=2n-1 \\ \lambda_j \vdash \nu}} \chi_\nu. \quad (3)$$

Lemma 8 は、Theorem 5 を用いて証明される。ここで注意すべき点として、例えば (3) の左辺に於いて、 $\|\mu_i\| - \|\nu\| = 1$ である。従ってもし $\nu \vdash \mu_i$ が成り立つならば、ある1次多項式 $t - \alpha \in \Phi$ が存在して、 $\nu(t - \alpha) \subset \mu_i(t - \alpha)$ (すなわち全ての $k \geq 1$ について $\nu(t - \alpha)_k \leq \mu_i(t - \alpha)_k$)、 $|\mu_i(t - \alpha)| - |\nu(t - \alpha)| = 1$ 、さらに $t - \alpha$ と異なる全ての $f \in \Phi$ に対して $\nu(f) = \mu_i(f)$ が成立しなければならない。

以後簡単のため q を even と仮定し、Theorem 3 (ii) を帰納法を用いて証明する。まず $n = 0$ のときは自明であるから $n > 0$ とする。このとき帰納法の仮定により $n-1$ のとき主張は正しい。すなわち

$$(1_{K_{2n-2}})^{G_{2n-2}} = \sum_{j=1}^l \chi_{\lambda_j}$$

と分解され、 $\lambda_1, \dots, \lambda_l$ は、 $\|\lambda\| = 2n-2$ 、 $\tilde{\lambda} = \lambda$ 、さらに $\lambda(t-1)'$ が even となるような写像 $\lambda : \Phi \rightarrow \mathcal{P}$ の全体である。

次に、 $(1_{K_{2n}})^{G_{2n}} = \sum_{i=1}^k \chi_{\mu_i}$ と分解されたたとすると、Theorem 2 より μ_i たちは全て real-valued、つまり $\tilde{\mu}_i = \mu_i$ を満たす。また、 $\tilde{f} = f$ を満たす1次多項式 $f \in \Phi$ は $f = t-1$ に限ることから、Lemma 8 より直ちに次が得られる。

Claim 9. If $\nu : \Phi \rightarrow \mathcal{P}$ satisfies $\|\nu\| = 2n-1$ and $\nu \vdash \mu_i$ for some i , then one of the following holds:

- (a) $\nu(t-1)'$ is even and $\tilde{\nu} \neq \nu$,
- (b) $\nu(t-1)'$ has exactly one odd part and $\tilde{\nu} = \nu$.

Moreover,

$$\sum_{i=1}^k \sum_{\substack{\|\nu\|=2n-1 \\ \nu \vdash \mu_i}} \chi_\nu \quad (4)$$

is multiplicity-free.

さらに Claim 9 より、各 i に対して $\mu_i(t-1)'$ の odd parts の個数は 0 または 2 であることが分かる。今仮に、ある i について、 $\mu_i(t-1)'$ の odd parts の個数が 2 であり、さらに $l(\mu_i(t-1)') > 2$ であるとする。このとき写像 $\nu: \Phi \rightarrow \mathcal{P}$ で、 $\|\nu\| = 2n-1$ 、 $\hat{\nu} = \nu$ 、 $\nu \vdash \mu_i$ 、かつ $\nu(t-1)'$ の odd parts の個数が 3 となるものが存在してしまい、Claim 9 に矛盾する。従って次が得られる。

Claim 10. *If an irreducible character χ_μ of G_{2n} with $\bar{\mu} = \mu$ is contained in $(1_{K_{2n}})^{G_{2n}}$, then one of the following holds:*

- (a) $\mu(t-1)'$ is even,
- (b) $\mu(t-1)'$ is odd and $l(\mu(t-1)') = 2$.

Claim 10 に於いて (b) が起こり得ないことを示すために、写像 $\mu_*: \Phi \rightarrow \mathcal{P}$ で $\|\mu_*\| = 2n$ 、 $\bar{\mu}_* = \mu_*$ 、かつ $\mu_*(t-1) = (1^{2k})$ ($k \geq 0$) となるものを一つ固定し、さらに $l(\lambda') \leq 2$ 、 $|\lambda| = 2k$ を満たす分割 $\lambda \in \mathcal{P}$ に対し、写像 $\mu_\lambda: \Phi \rightarrow \mathcal{P}$ を次で定義する：

$$\mu_\lambda(f) := \begin{cases} \lambda & \text{if } f(t) = t-1 \\ \mu_*(f) & \text{otherwise} \end{cases}$$

このとき次が確かめられる。

Claim 11. *Let $\lambda \in \mathcal{P}$ be as above, and suppose that χ_{μ_*} is contained in $(1_{K_{2n}})^{G_{2n}}$. Then χ_{μ_λ} is contained in $(1_{K_{2n}})^{G_{2n}}$ if and only if λ' is even.*

Proof. $l(\rho') \leq 2$ 、 $|\rho| = 2k-1$ を満たす分割 $\rho \in \mathcal{P}$ に対し写像 $\nu_\rho: \Phi \rightarrow \mathcal{P}$ を同様に次で定義する：

$$\nu_\rho(f) := \begin{cases} \rho & \text{if } f(t) = t-1 \\ \mu_*(f) & \text{otherwise} \end{cases}$$

このとき $\|\nu_\rho\| = 2n-1$ 、 $\hat{\nu}_\rho = \nu_\rho$ となり、さらに χ_{ν_ρ} は全て(4)式に現われる。まず、(4)式は multiplicity-free であり $\nu_{(1^{2n-1})} \vdash \mu_{(1^{2n})}$ 、 $\nu_{(1^{2n-1})} \vdash \mu_{(1^{2n-2}, 2)}$ となることから、 $\chi_{\mu_{(1^{2n-2}, 2)}}$ は $(1_{K_{2n}})^{G_{2n}}$ に現れないことが分かる。次に Claim 10 より、 $(1_{K_{2n}})^{G_{2n}}$ の分解に現れ得る既約指標 χ_μ で $\nu_{(1^{2n-2}, 2)} \vdash \mu$ を満たすものは $\chi_{\mu_{(1^{2n-2}, 2)}}$ 及び $\chi_{\mu_{(1^{2n-4}, 2^2)}}$ の二つしかないことから、 $\chi_{\mu_{(1^{2n-4}, 2^2)}}$ は $(1_{K_{2n}})^{G_{2n}}$ に現われなければならない。以下同様にして（正確には帰納法により）主張が示される。□

次の主張は、Theorem 6 及び Lemma 7 を用いて、帰納法により証明される。

Claim 12. *Let $1 \leq k \leq n$ and let $\mu_*: \Phi \rightarrow \mathcal{P}$ be a partition-valued function such that $\|\mu_*\| = 2n$ 、 $\bar{\mu}_* = \mu_*$ and $\mu_*(t-1) = (1^{2k})$. Then χ_{μ_*} is contained in $(1_{K_{2n}})^{G_{2n}}$.*

今、 χ_{μ_*} を $\bar{\mu} = \mu$ を満たす G_{2n} の既約指標とする。もし $\mu(t-1)' \neq \emptyset$ かつ $l(\mu(t-1)') \leq 2$ ならば、Claim 11、Claim 12 より、 χ_{μ_*} が $(1_{K_{2n}})^{G_{2n}}$ に現われるのは $\mu(t-1)'$ が even の場合、かつその場合に限る。さらに他の場合についても、Proposition 4、Claim 10 より χ_{μ_*} は $(1_{K_{2n}})^{G_{2n}}$ に現われなければならないことが分かる。従って、Theorem 3 (ii) が示された。

参考文献

- [1] E. Bannai, Character tables of commutative association schemes, in "Finite Geometries, Buildings, and Related Topics" (W. M. Kantor et al., Eds.), pp.105-128, Clarendon Press, Oxford, 1990.

- [2] E. Bannai and T. Ito, "Algebraic Combinatorics I," Benjamin/Cummings, Menlo Park, CA, 1984.
- [3] E. Bannai, N. Kawanaka, and S. Y. Song, The character table of the Hecke algebra $\mathcal{H}(GL_{2n}(\mathbb{F}_q), Sp_{2n}(\mathbb{F}_q))$, *J. Algebra* **129** (1990), 320-366.
- [4] E. Bannai and H. Tanaka, The decomposition of the permutation character $1_{GL(n, q^2)}^{GL(2n, q)}$, submitted.
- [5] R. Gow, Two multiplicity-free permutation representations of the general linear group $GL(n, q^2)$, *Math. Z.* **188** (1984), 45-54.
- [6] N. F. J. Inglis, M. W. Liebeck and J. Saxl, Multiplicity-free permutation representations of finite linear groups, *Math. Z.* **192** (1986), 329-337.
- [7] I. G. Macdonald, "Symmetric Functions and Hall Polynomials" 2nd ed., Oxford mathematical monographs, Oxford Univ. Press, 1995.
- [8] E. Thoma, Die Einschränkung der Charaktere von $GL(n, q)$ auf $GL(n-1, q)$, *Math. Z.* **119** (1971), 321-338.
- [9] A. V. Zelevinsky, "Representations of Finite Classical Groups: A Hopf Algebra Approach," *Lecture Notes in Math.* **869**, Springer-Verlag, Berlin, 1981.

MODULES FULFILLING THE STRONG GAP CONDITION

TOSHIO SUMI

1. INTRODUCTION

A basic problem for the theory of transformation groups is to describe the fixed point sets of smooth actions of a given finite group on specific smooth manifolds. Oliver [O2] has decided completely for actions on disks or euclidean spaces. Spheres may be considered as manifolds which have the next simple structures. However we do not completely know the fixed point sets of smooth actions on spheres. Morimoto [Mo] has shown some results with respect to the fixed point set of smooth action on spheres.

A finite group G is an *Oliver group*, if G has no series of subgroups of the form $P \triangleleft H \triangleleft G$ where $|\pi(P)| \leq 1$, $|\pi(G/H)| \leq 1$ and H/K is cyclic. Here $\pi(G)$ is the set of primes dividing the order of G . Particularly, each nonsolvable group is an Oliver groups. We denote by $O^p(G)$ the minimal normal subgroup of G whose index is a power of p . Oliver [O1] has shown that a finite group G has a one fixed point free smooth action on a disk D (that is, $D^G = \emptyset$) if and only if G is an Oliver group. Laitinen and Morimoto [LM] has shown that a finite group G has a one fixed point smooth action on a sphere S (that is, $S^G = \{x\}$) if and only if G is an Oliver group. They defined the G -module

$$V(G) = (\mathbb{R}[G] - \mathbb{R}) - \bigoplus_{p \in \pi(G)} (\mathbb{R}[G] - \mathbb{R})^{O^p(G)}$$

to show this by using an equivariant surgery theory.

An equivariant surgery theory has been developed only on G -manifolds M satisfying the weak gap condition. Here, it limits to indicating the strong gap condition. If a G -space M satisfies the strong gap condition if $2 \dim M^H < \dim M^P$ for any pairs (P, H) of subgroups such that $G \geq H > P$ and $|\pi(P)| \leq 1$. Let $\mathcal{P}(G)$ be the set of subgroups P of G with $|\pi(P)| \leq 1$ and $\mathcal{L}(G)$ the set of subgroups of G containing $O^p(G)$ for some prime p . A finite group G with $|\pi(G)| > 1$ is a *gap group* if there exists a G -module V such that the following two conditions hold.

- (1) V is $\mathcal{L}(G)$ -free, that is, $\dim V^H = 0$ for $H \in \mathcal{L}(G)$.
- (2) V satisfies the strong gap condition.

Such a G -module V is called a *gap G -module*.

If G acts smoothly on a smooth manifold M , then for any fixed point $x \in M$, the tangent space $T_x(M)$ admits the structure of a real G -modules by taking the derivatives of the transformations $g: M \rightarrow M$ determined by the elements of $g \in G$. This module $T_x(M)$ is called *the tangent G -module at x* .

2000 Mathematics Subject Classification. 57S17, 20C15.

Key words and phrases. gap group, gap module, real representation, the action on spheres.

Smith Isomorphism Question ([Sm]). *If a finite group G acts smoothly on a sphere S with exactly two fixed points x and y , is it true that the tangent G -modules $T_x(S)$ and $T_y(S)$ are isomorphic?*

Atiyah, Bott [AB] and Milnor [Mi] have shown that the question is true if the action is free outside of Σ^G and Sanchez [Sa] gave an affirmative answer if a finite group G of odd order acts smoothly on a homotopy sphere Σ in such a way that $\Sigma^G = \{x, y\}$ and for $H \leq G$, the H -fixed point set Σ^H is connected or $\Sigma^H = \Sigma^G$. On the other hand, Cappell and Shaneson [CS1, CS2, CS3] gave counterexamples.

Two real G -modules U and V are *Smith equivalent* if there exists a smooth action of G on a homotopy sphere Σ such that $\Sigma^G = \{x, y\}$ and as G -modules, $U \cong T_x(\Sigma)$ and $V \cong T_y(\Sigma)$. A smooth G -action on a homotopy sphere Σ is called *2-proper* if the manifold Σ^g is connected for every element $g \in G$ whose order is a power of 2 greater than or equal to 8. Two G -modules U and V are called *2-proper Smith equivalent* if there exists a smooth 2-proper action of G on a homotopy sphere Σ such that $\Sigma^G = \{x, y\}$ and as G -modules, $U \cong T_x(\Sigma)$ and $V \cong T_y(\Sigma)$. Petrie proved that for each finite abelian group G of odd order with at least four noncyclic Sylow subgroups, there exist two Smith equivalent G -modules U and V that are not isomorphic. In 1995, Laitinen posed a conjecture related to the Smith isomorphism question in the case where G is a finite Oliver groups.

Laitinen Conjecture. *For a finite Oliver group G , there exist 2-proper Smith equivalent G -modules that are not isomorphic, that is $Sm_2(G) \neq 0$, if and only if $r_G \geq 2$.*

The notation will be appear in the next section.

In order to approach this problem, we would like to determine which group is a gap group. In this note, we give a sufficient condition to be a gap group.

2. LAITINEN CONJECTURE

It follows $\dim T_x(S)^G = \dim T_y(S)^G$ by the slice theorem and the character of the tangent G -modules at x and y agree on each element of G of odd prime power order by Smith theory.

Proposition 2.1 (Petrie). *If a finite group G acts smoothly on a homotopy sphere Σ with $\Sigma^G = \{x, y\}$ and the action is 2-proper, the character of the tangent G -modules at x and y agree on each element of G of prime power order.*

We denote by $RO(G)$ the real representation ring of G , and by $Sm(G)$ (resp. $Sm_2(G)$) the subset of $RO(G)$ formed by taking the differences $U - V$ represented by two (resp. 2-proper) Smith equivalent real G -modules U and V . Let $Sm_2^{\mathcal{L}(G)}(G)$ be the subset of $Sm_2(G)$ obtained by $U - V$ represented by two 2-proper Smith equivalent real $\mathcal{L}(G)$ -free G -modules U and V . Two elements $g, h \in G$ are called *real conjugate in G* if h is conjugate to g or g^{-1} in G . Denote by r_G the number of the real conjugacy classes of (nontrivial) elements of G that are not of prime power order. Set

$$IO(G) = \ker \left(\bigoplus_{P \in \mathcal{P}(G)} \text{Res}_P^G: RO(G) \rightarrow \bigoplus_{P \in \mathcal{P}(G)} RO(P) \right).$$

Let $LO(G)$ be the subgroup of $IO(G)$ obtained by the differences $U - V$ represented by two real $\mathcal{L}(G)$ -free G -modules U and V which are isomorphic when restricted to any $P \in \mathcal{P}(G)$. Note that $\text{rank } IO(G) = r_G$. (cf. [LP])

Theorem 2.2 ([PS]). *If G is a finite Oliver gap group, then*

$$LO(G) = Sm_2^{\mathcal{L}(G)}(G) \subseteq Sm_2(G) \subseteq Sm(G) \subseteq IO(G).$$

Proposition 2.3 ([LP]). *Let G be a finite group. If $r_G \leq 1$, then $Sm_2(G) = 0$.*

Theorem 2.4 ([PS]). *For a finite nonsolvable group G ,*

- (1) $Sm_2(G) = 0$ for $r_G \leq 1$ and
- (2) $Sm_2(G) \neq 0$ for $r_G \geq 2$, when G is a gap group with $G \not\cong P\Omega(2, 27)$.

3. GAP GROUPS

Set $\mathcal{D}(G) = \{(P, H) \mid P \in \mathcal{P}(G), P < H \leq G\}$ and $\mathcal{D}^2(G)$ as the set of $(P, H) \in \mathcal{D}(G)$ fulfilling $[H : P] = [O^q(G)H : O^q(G)P] = 2$ and $O^q(G)P = G$ for any odd primes q . For a G -module V , we define $d_V : \mathcal{D}(G) \rightarrow \mathbb{Z}$ by $d_V(P, H) = \dim V^P - 2 \dim V^H$.

Proposition 3.1 ([LM, MSY]). *The followings hold.*

- (1) $d_{V(G)}(P, H) \geq 0$ for any $(P, H) \in \mathcal{D}(G)$.
- (2) $d_{V(G)}(P, H) = 0$ if and only if either $P \in \mathcal{L}(G)$ or $(P, H) \in \mathcal{D}^2(G)$.

Examples. Suppose that $\mathcal{L}(G) \cap \mathcal{P}(G) = \emptyset$.

- (1) Any nonabelian perfect group is a gap group.
- (2) If $\{|\{p \in \pi(G) \mid p \neq 2, O^p(G) \neq G\}| \geq 2\}$, then G is a gap group. ([MSY])
- (3) The symmetric group S_5 on 5 letters is not a gap group. ([MY])
- (4) Symmetric groups S_n ($n \geq 6$) are gap groups. ([DH])
- (5) $S_n \times C_2$ ($n \geq 6$) and $A_n \times C_2$ ($n \geq 5$) are gap groups. ([MSY])
- (6) If G is a generalized quaternion group Q_{4n} of order $4n$, then G is not a gap group but $G \times C_p$ is a gap group for all odd prime p .
- (7) $G \times D_{2n}$ is a gap group if and only if G is. ([Su1])
- (8) A finite group which has a quotient gap group is a gap group. ([Su1])

Theorem 3.2. *A nonsolvable general linear group $GL(n, q)$ is a gap group. A nonsolvable projective linear group $PGL(n, q)$ is a gap group if and only if $(n, q) \neq (2, 5), (2, 7), (2, 9), (2, 17)$.*

For a subset S of $\mathcal{D}(G)$, we let D be a matrix whose rows correspond to irreducible $\mathcal{L}(G)$ -free modules and columns correspond to elements of S . This matrix is called the *dimension matrix* over S .

$$D = \begin{pmatrix} d_{V_1}(P_1, H_1) & d_{V_1}(P_1, H_1) & \cdots \\ d_{V_1}(P_2, H_2) & d_{V_1}(P_2, H_2) & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Theorem 3.3 ([Su1]). *Let D be the dimension matrix over $\mathcal{D}(G)$. A finite group G is not a gap group if and only if there is a nontrivial solution $x \geq 0, x \neq 0$ such that $xD = 0$.*

Remark 3.4. *If W is an $\mathcal{L}(G)$ -free module such that $d_W(P, H) > 0$ for any $(P, H) \in \mathcal{D}^2(G)$, then $d_{W+(\dim W+1)V(G)}(P, H) > 0$ for any $(P, H) \in \mathcal{D}(G)$.*

We define $\mathcal{GE}(G)$ as the set of elements x outside of $O^2(G)$ such that the order $|x|$ is a power of 2, and if $|x| > 2$, then $C_G(x) \notin \mathcal{P}(G)$ and if $|x| = 2$ then $O^2(C_G(x)) \notin \mathcal{P}(G)$. For a subset S of G , let $T(G, S)$ be the set of elements outside of $\cup_{g \in G} S^g \cup O^2(G)$ of order a power of 2 and set $T_+(G, S) = T(G, S) \cap \mathcal{GE}(G)$ and $T_-(G, S) = T(G, S) \setminus T_+(G, S)$. Note that these sets are closed under the conjugate action. We define $\mathcal{E}^2(G, S)$ as the set of $(P, H) \in \mathcal{D}^2(G)$ such that a Sylow 2-subgroup of H is a subset of $P \cup T_-(G, S)$.

Proposition 3.5. *There exists an $\mathcal{L}(G)$ -free G -module W such that*

- (1) $d_W(P, H) \geq 0$ for any $(P, H) \in \mathcal{D}(G)$ and
- (2) $d_W(P, H) > 0$ if and only if $(P, H) \notin \mathcal{D}^2(G)$ or $\mathcal{GE}(G) \cap H \setminus P \neq \emptyset$.

Theorem 3.6 ([Su2]). *Let G be a finite group such that $\mathcal{P}(G) \cap \mathcal{L}(G) = \emptyset$ and let K_j be gap subgroups of G . If one of the following conditions holds, then G is a gap group.*

- (1) *There exists an $\mathcal{L}(G)$ -free G -module V such that $d_V(P, H) > 0$ for any $(P, H) \in \mathcal{E}^2(G, \cup_j K_j)$.*
- (2) *$T_+(G, \emptyset)$ is not empty and there exists an element x of G such that $\langle x \rangle$ has no Sylow 2-subgroup of G (as a subgroup), $O^2(G)\langle x \rangle = G$ and $T_-(G, \cup_j K_j) \subset \cup_{g \in G} \langle x \rangle^g$.*

Let S be a sporadic group. If S is not complete, that is, $\text{Aut}(S)$ is not isomorphic to G , then the index $[\text{Aut}(S) : S]$ is two. We can apply this theorem in the special case where $K_j = \emptyset$ for the automorphism groups of sporadic groups M_{12} , HN , J_2 , J_3 , M^cL , $O'N$, Fi_{22} , Fi'_{24} and He . In the case where $S = HS$, by taking K_1 as the subgroup isomorphic to $S_8 \times C_2$, we can apply it. If G is either M_{22} or Suz , then $\text{Aut}(S)$ has a gap subgroup of odd index by ATLAS [CNPW] and thus $\text{Aut}(S)$ is a gap group. Hence we have

Theorem 3.7 ([Su2]). *The automorphism group of any sporadic group is a gap group.*

In the present, as for the automorphism groups of simple groups, which are not gap groups, only $\text{Aut}(A_5)$, $\text{Aut}(L_2(7))$, $\text{Aut}(A_6)$, and $\text{Aut}(L_2(17))$ are known. (See Theorem 3.2.)

Furthermore we can find a gap G -module under the assumption of the existence of C below.

Theorem 3.8. *Let G be a finite group such that $\mathcal{P}(G) \cap \mathcal{L}(G) = \emptyset$.*

- (1) *If there is a cyclic subgroup C such that $O^2(G)C = G$ and $O^2(G) \cap C \notin \mathcal{P}(G)$, then G is a gap group.*
- (2) *If any subgroup K of G which is a subgroup of $O^2(G)$ with $K/O^2(G)$ cyclic is a gap group, then G is a gap group.*

For example, it follows immediately from this theorem that symmetric groups S_n for $n \geq 7$ are gap groups ([DH]). Let S be a simple group listed in ATLAS and G a subgroup of the automorphism group $\text{Aut}(S)$ such that $G > S$ and its index is a power of 2. If G does not fulfill the assumption of Theorem 3.8 (1), the group S is one of the followings groups: A_5 , $L_2(7)$, A_6 , $L_2(17)$, $L_2(16)$, $L_2(25)$, $L_3(4)$, $U_3(4)$, $S_4(4)$, $U_3(8)$, $L_3(8)$, $L_3(11)$, $O_8^+(3)$, $O_8^-(3)$, $E_6(2)$.

REFERENCES

- [AB] Atiyah, M.F. and Bott, R., *A Lefschetz fixed point formula for elliptic complexes: II. Applications*, Ann. of Math. **88** (1968), 451–491.
- [CNPW] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A., Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
- [CS1] Cappell, S.E. and Shaneson, J.L., *Fixed points of periodic maps*, Proc. Nat. Acad. Sci. USA **77** (1980), 5052–5054.
- [CS2] Cappell, S.E. and Shaneson, J.L., *Fixed points of periodic differentiable maps*, Invent. Math. **68** (1982), 1–19.
- [CS3] Cappell, S.E. and Shaneson, J.L., *Representations at fixed points in Group Actions on Manifolds* (ed. R. Schultz), Contemp. Math. **36** (1985), 151–158.
- [DH] Dovermann, K. H. and Herzog, M., *Gap conditions for representations of symmetric groups*, J. Pure Appl. Algebra **119** (1997), 113–137.
- [LM] Laitinen, E. and Morimoto, M., *Finite groups with smooth one fixed point actions on spheres*, Forum Math. **10** (1998), 479–520.
- [LP] Laitinen, E. and Pawalowski, K., *Smith equivalence of representations for finite perfect groups*, Proc. Amer. Math. Soc. **127** (1999), 297–307.
- [Mi] Milnor, J.W., *Whitehead torsion*, Bull. Amer. Math. Soc. **72** (1966), 358–426.
- [Mo] Morimoto, M., *Equivariant surgery theory: Deleting–Inserting Theorem of fixed point manifolds on spheres and disks*, K-theory **15** (1998), 13–32.
- [MSY] Morimoto, M., Sumi, T. and Yanagihara, M., *Finite groups possessing gap modules in Geometry and Topology: Aarhus 1998* (ed. K. Grove, I.H. Madsen, E.K. Pedersen), Contemp. Math. **258** (2000), 329–342.
- [MY] Morimoto, M. and Yanagihara, M., *The gap condition for S_5 and GAP programs*, Jour. Fac. Env. Sci. Tech., Okayama Univ. **1** (1996), 1–13.
- [O1] Oliver, R., *Fixed point sets of group actions on finite acyclic complexes*, Comment. Math. Helv. **50** (1975), 155–177.
- [O2] Oliver, R., *Fixed point sets and tangent bundles of actions on disks and euclidean spaces*, Topology **35** (1996), 583–615.
- [Pa1] Pawalowski, K., *Group actions with inequivalent representations at fixed points*, Math. Z. **187** (1984), 29–47.
- [Pa2] Pawalowski, K., *Smith equivalence of group modules and the Laitinen conjecture. A survey in Geometry and Topology: Aarhus 1998* (ed. K. Grove, I.H. Madsen, E.K. Pedersen), Contemp. Math., **258** (2000), 343–350.
- [Pe1] Petrie, T., *The equivariant J homomorphism and Smith equivalence of representations*, in Current Trends in Algebraic Topology (ed. M. Kane, S.O. Kochman, P.S. Selick, V.P. Snaith), CMS Conference Proc. Vol. 2, Part 2 (1982), 223–233.
- [Pe2] Petrie, T., *Smith equivalence of representations*, Math. Proc. Cambridge Philos. Soc., **94** (1983), 61–99.
- [PS] Pawalowski, K. and Solomon, R., *Smith equivalence of group modules for finite Oliver groups*, preprint (2000).
- [Sa] Sanchez, C.U., *Actions of groups of odd order on compact orientable manifolds*, Proc. Amer. Math. Soc. **54** (1976), 445–448.
- [Sm] Smith, P.A., *New results and old problems in finite transformation groups*, Bull. Amer. Math. Soc. **66** (1960), 401–415.
- [Su1] Sumi, T., *Gap modules for direct product groups*, to appear in Jour. Math. Soc. Japan.
- [Su2] Sumi, T., *Gap modules for semidirect product groups*, preprint (2001).

DEPARTMENT OF ART AND INFORMATION DESIGN, FACULTY OF DESIGN, KYUSHU INSTITUTE OF DESIGN, SHIOBARU 4-9-1, FUKUOKA, 815-8540, JAPAN

E-mail address: sumi@kyushu-id.ac.jp

An upper bound for the cardinality of an antipodal s -distance set in Euclidean space

Etsuko Bannai, Yusuke Nitamizu, Teppei Sato,
坂内 悦子、二田水 祐介、佐藤 鉄兵

Graduate School of Mathematics
Kyushu University
九大・数理

Abstract

In this paper we show that if X is an antipodal s -distance set in \mathbb{R}^m and X is on p concentric spheres then $|X| \leq 2 \sum_{i=0}^{p-1} \binom{m+s-2i-2}{m-1}$.

§1. Main theorem

A subset X in a metric space (M, d) is called an s -distance set if the cardinality of the set $A = \{d(x, y) \mid x, y \in X, x \neq y\}$ is equal to s . If we have design theory on (M, d) , it is an interesting problem to ask how the cardinalities of s -distance subsets and the cardinalities of designs relate. When M is a sphere S^{m-1} in \mathbb{R}^m , this problem is studied by P. Delsarte, J. M. Goethals and J. J. Seidel ([6]).

The upper bound of the cardinality of an s -distance set in \mathbb{R}^m was first studied by Bannai-Bannai-Stanton [2] and Blokhuis [4] independently. They showed that s -distance set in \mathbb{R}^m is bounded above by $\binom{m+s}{s}$. On the other hand Euclidean design is defined in the paper by P. Delsarte and J. J. Seidel [5]. They proved that the cardinality of a Euclidean $2s$ -design on p concentric spheres in \mathbb{R}^m is bounded below by $\sum_{i=0}^{2p-1} \binom{m+s-i-1}{m-1}$. The first author of this article proved, in a joint work with K. Kawasaki ([3]), that the upper bound of the cardinality of an s -distance set in \mathbb{R}^m coincides with this lower bound obtained by Delsarte and Seidel.

In this paper we study the antipodal s -distance sets on p concentric spheres in \mathbb{R}^m and prove the following theorem.

Theorem 1 *Let X be an antipodal s -distance set on p concentric spheres in \mathbb{R}^m . Then*

$$|X| \leq 2 \sum_{i=0}^{p-1} \binom{m+s-2i-2}{m-1}.$$

Remark: This upper bound coincides with the lower bound of the cardinality of an antipodal $(2s-1)$ -design on p concentric spheres in \mathbb{R}^m . If $p = 1$, then $2 \sum_{i=0}^{p-1} \binom{m+s-2i-2}{m-1} = 2 \binom{m+s-2}{m-1}$ and the bound coincides with the bound given by Delsarte, Geothals and Seidel for the antipodal spherical case.

In §2, and §3, we give some related known facts so that the reader will find out why we consider the antipodal s -distance set. Please refer [1], [6], [5], etc., for more details.

§2. Spherical case

A set X in \mathbb{R}^m is called antipodal if $-x \in X$ holds for any $x \in X$.

Theorem 2 (see [6])

(1) Let X be an s -distance set on the unit sphere in \mathbb{R}^m . Then

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

(2) Let X be an antipodal s -distance set on the unit sphere in \mathbb{R}^m . Then

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

In [6] the following definition of spherical design was given.

Definition 3 (see [6]) Let X be a finite set on the unit sphere $S^{m-1} \subset \mathbb{R}^m$. X is a t -design if the following condition is satisfied:

$$\frac{1}{|S^{m-1}|} \int_{\xi \in S^{m-1}} f(\xi) d\xi = \frac{1}{|X|} \sum_{\eta \in X} f(\eta).$$

for any polynomial $f(x) = f(x_1, x_2, \dots, x_m)$ of degree at most t . Where $|S^{m-1}|$ is the surface area(volume) of the unit sphere S^{m-1} .

Theorem 4 (see [6]) (1) Let X be a $2s$ -design on S^{m-1} , then the following holds:

$$|X| \geq \binom{m+s-1}{m-1} + \binom{m+s-2}{m-1} \quad (1)$$

(2) Let X be a $(2s-1)$ -design on S^{m-1} , then the following holds:

$$|X| \geq 2 \binom{m+s-2}{m-1} \quad (2)$$

If the equality holds in (1) or (2), then X is called a tight $2s$ -design or a tight $(2s - 1)$ -design respectively.

Theorem 5 (see [6])

- (1) Let X be a finite set on S^{m-1} , with $|X| = \binom{m+s-1}{m-1} + \binom{m+s-2}{m-1}$. Then X is a tight $2s$ -design if and only if X is an s -distance set.
 (2) A tight $(2s - 1)$ -design is antipodal.
 (3) Let X be a finite set on S^{m-1} , with $|X| = 2\binom{m+s-2}{m-1}$, then X is a tight $(2s - 1)$ -design if and only if X is an antipodal s -distance set.

§3. Euclidean case

For Euclidean spaces Delsarte and Seidel ([5]) gave the definition of design in the following manner. Let X be a finite set in \mathbb{R}^m . Assume $0 \notin X$. Let S_1, S_2, \dots, S_p in \mathbb{R}^m be the concentric spheres center at the origin satisfying the following conditions:

- (1) $X \subset S_1 \cup S_2 \cup \dots \cup S_p$,
 (2) $X \cap S_i \neq \emptyset$ for $1 \leq i \leq p$.

Let $X_i = X \cap S_i$ for $1 \leq i \leq p$. Let ω be a weight function $X \ni x \rightarrow \omega(x) \in \mathbb{R}_{>0}$. Let $\omega(X_i) = \sum_{x \in X_i} \omega(x)$. With these notation they gave the following definition.

Definition 6 (see [5]) X is a Euclidean t -design if the following condition is satisfied:

$$\sum_{i=1}^p \frac{\omega(X_i)}{|S_i|} \int_{\xi \in S_i} f(\xi) d\xi = \sum_{\eta \in X} f(\eta) \omega(\eta),$$

for any polynomial $f(x) = f(x_1, x_2, \dots, x_m)$ of degree at most t . Where $|S_i|$ is the area(volume) of the sphere S_i .

For the Euclidean designs the following lower bounds are known.

Theorem 7 (see [5])

- (1) Let X be a $2s$ -design in \mathbb{R}^m , then the following holds:

$$|X| \geq \sum_{i=0}^{2p-1} \binom{m+s-i-1}{m-1}.$$

- (2) Let X be a $(2s - 1)$ -design in \mathbb{R}^m . Assume that X is antipodal. Then the following holds:

$$|X| \geq 2 \sum_{i=0}^{p-1} \binom{m+s-2i-1}{m-1}.$$

In [3], the first author of this paper and K. Kawasaki showed the following theorem.

Theorem 8 (see [3])

Let X be a s -distance set in \mathbb{R}^m . Assume that X is on p concentric spheres then the following holds:

$$|X| \leq \sum_{i=0}^{2p-1} \binom{m+s-i-1}{m-1}.$$

§3. Conclusion and Examples

There are some arguments about what is the best way to define the designs in Euclidean spaces. Our main theorem of this paper and the above Theorem 8 will give a conclusion to this arguments.

The lower bounds for spherical $(2s-1)$ -design in Theorem 4, (2) are proved without assuming X be antipodal. Our next aim is to prove the lower bounds for the Euclidean $(2s-1)$ -design given in Theorem 7, (2) without the antipodal condition on X .

There is an example of a 2-distance set with 45 points on 2 concentric spheres in \mathbb{R}^8 . The number 45 is the upper bound for 2-distance set in \mathbb{R}^8 given in Theorem 8. This example was found by P. Lisoněk (see [8]). Obviously this set is not antipodal. This set is proved to be a Euclidean 3-design in \mathbb{R}^8 taking a suitable weight function. However it turned out that there is no weight function which makes this set a Euclidean 4-design. This means the design theory for Euclidean space defined by Delsarte and Seidel is slightly different from that of spherical case. We conclude this paper with giving the following example of maximal antipodal 2-distance set in \mathbb{R}^2 on 2-concentric spheres which is a Euclidean tight 3-design.

Example: $X = \{A = (1, 0), B = (-1, 0), C = (0, \sqrt{3}), D = (0, -\sqrt{3})\}$

This set is a Euclidean tight 3-design with the weight function defined by $\omega(A) = \omega(B) = 3, \omega(C) = \omega(D) = 1$.

References

- [1] Ei. Bannai, Et. Bannai, *Algebraic Combinatorics on Spheres*, Springer Tokyo, 1999 (in Japanese).
- [2] Ei. Bannai, Et. Bannai and D. Stanton, *An upper bound for the cardinality of an s -distance subset in real Euclidean space II*, *Combinatorica* 3 (1983), 147-152.
- [3] Et Bannai and K. Kawasaki, *An upper bound for the cardinality of an s -distance set in Euclidean space*, preprint
- [4] A Blokhuis, *An upper bound for the cardinality of s -distance sets in E^d and H^d* , Eindhoven Univ. Techn. Memorandum, 1982 May.

- [5] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t -designs*, Lin. Algebra and its Appl. 114-115 (1989), 213-230.
- [6] P. Delsarte, J. M. Goethals and J. J. Seidel, *Spherical codes and designs*, Geom. Dedicata 6 (1977), 363-388.
- [7] A. Erdélyi et al. *Higher transcendental functions II*, (Bateman Manuscript Project), MacGraw-Hill, 1953.
- [8] P. Lisoněk, *New maximal two-distance sets*, J. Comb. Theory, Ser. A 77 (1997) 318-338.

指数2の巡回部分群をもつ2群における 半正則相対差集合の分類

熊本大学教育学部 平峰 豊

1 半正則相対差集合

U を有限群 G の自明でない部分群とする. G の k -部分集合 R が (k, λ, U) 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) R は G の U の右剰余類分解の完全代表系である: $G = \sum_{r \in R} Ur$
- (ii) $G - U$ の任意の元 g に対して, g を $g = r_1 r_2^{-1}$ ($r_1, r_2 \in R$) の形に表す方法が丁度 λ 通りある.

条件 (ii) は群環 $\mathbb{C}[G]$ の次の等式で表される.

$$RR^{-1} = k + \lambda(G - U) \quad (k = |R|)$$

上では G の部分集合 X に対して X^{-1} で X の元の逆元の集合を表している. さらに G の部分集合 Y を $\hat{Y} \in \mathbb{C}[G]$ と同一視して単に Y と表してある. また, 条件 (i)(ii) より次がわかる.

$$|G : U| = |R| = |U|\lambda, \quad |G| = |U|^2\lambda \quad (1)$$

R は U を禁止群とする半正則相対差集合とも呼ばれる. 以下ではパラメタ (k, λ, U) を明示する必要がないときはこの名称を主として用いる.

注意 1.1 上の定義において (ii) だけを仮定するとき, R は U を禁止群とする相対差集合 (*relative difference set*) と呼ばれる. (cf. [9])

例 1.2 (i) 位数4の巡回群 $\langle a \rangle$ において $\{1, a^3\}$ は $(2, 1, \langle a^2 \rangle)$ 差集合である.
(ii) 位数8のアーベル群 $\langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ において $\{1, ab, a^2b, a^3b\}$ は $(4, 2, \langle b \rangle)$ 差集合である. また, $\langle a \rangle \times \langle b \rangle \times \langle c \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ において $\{1, a, b, abc\}$ は $(4, 2, \langle c \rangle)$ 差集合である. \mathbb{Z}_8 には半正則相対差集合は存在しない.

(iii) 位数12の任意の群には半正則相対差集合は存在しない.

G が $(4n, 2n, U)$ 差集合をもち $G \supset U \simeq \mathbb{Z}_2$ であるとき G はアダマール群と呼ばれ, これから $4n$ 次のアダマール行列が得られることが知られている ([5]).

半正則相対差集合は可換な p -群 (p :素数) のときに最も詳しく研究されている. G を p -群とし $k = p^a$, $|U| = p^b$ とおく. このとき明らかに $G = p^{a+b}$ かつ $\lambda = p^{a-b}$ である. G が可換 p -群のときは次の結果が示すように半正則相対差集合をもつような可換 p -群 G の指数 $\exp(G)$ はあまり大きくはなれない.

可能な指数の大きさ (可換 p -群の場合)

定理 1.3 (A. Pott [10])

- (i) $\exp(G) \leq p^a$ または $G \simeq \mathbb{Z}_4$
- (ii) $\exp(G) \leq p^{a+b-\lfloor \frac{a}{2} \rfloor}$

定理 1.4 (S.L. Ma & A. Pott [7])

$$2 \nmid a, p > 2 \implies \exp(G) \leq p^{\frac{a+1}{2}}$$

定理 1.5 (B. Schmidt [12])

$$2 \nmid a, p = 2 \implies \exp(G) \leq 2^{\frac{a+1}{2}}$$

位数 2^n の一般四元数群 Q_{2^n} は exponent が 2^{n-1} で非可換 2-群では最大であるが任意の $n \geq 3$ について半正則相対差集合を持つことが知られている. 従って, 上に述べた結果は非可換 2-群の場合は必ずしも正しくない. 2面体群 D_{2^n} や半 2面体群 SD_{2^n} の場合は次のようになる.

定理 1.6 (Elvira-Hiramine [1]) $G \triangleright U$ の条件のもとでは $G \not\cong D_{2^n}$ であり $G \simeq SD_{2^n}$ ならば $U \simeq \mathbb{Z}_2$ である.

定理 1.7 (Elvira-Hiramine [2]) 非可換 p -群 G で指数 p の巡回部分群をもつとする. $G \triangleright U$ で G が U に関する半正則相対差集合をもてば次のいずれかが成り立つ.

- (i) $G = Q_{2^n}$ かつ $U \simeq \mathbb{Z}_2$ (すべての $n \geq 3$ で存在).
- (ii) $G = M_n(p)$ かつ $U \simeq \mathbb{Z}_p$. ($n = 3$ では常に存在, $n > 3$ では未決定)
- (iii) $G = M_4(2)$ かつ $U \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

上に述べた定理は禁止群 U が G で normal であるという条件のもとで得られている. この定理により D_{2^n} では非存在であるが, 次の例が示すように U が G で normal であるという条件をはずせば半正則相対差集合が実際に存在する.

例 1.8 (Arasu-Chen-Pott, preprint) 2面体群 $D_8 = \langle x, y \mid x^4 = y^2 = 1, y^{-1}xy = x^{-1} \rangle$ において $\{1, x, x^2, xy\}$ は $(4, 2, \langle y \rangle)$ -差集合である。

この例は U の正規性を仮定しないのであれば $D_{2^n}, M_n(2), SD_{2^n}$ のときも Q_{2^n} のときと同様に半正則相対差集合の無限系列があるのではないかと期待を持たせる。

2 D_{2^n} or Q_{2^n} における半正則相対差集合

よく知られているように、指数 2 の巡回部分群をもつ位数 2^n の非可換 2-群 G は 2面体群 D_{2^n} 、一般四元数群 Q_{2^n} 、半 2面体群 SD_{2^n} 、または モジュラー 2-群 $M_n(2)$ のいずれかである。この節では D_{2^n} または Q_{2^n} が半正則相対差集合をもつ場合について考える。

(1) 2面体群 $D_{2^{n+1}}$

2面体群 $G = \langle x, y \mid x^{2^n} = y^2 = 1, y^{-1}xy = x^{-1} \rangle$ の場合について考える。 R を G における $(2^a, 2^b, U)$ 差集合とする。 $G \triangleright U$ のときは [2] の結果が適用できるので $G \not\triangleright U$ と仮定してよいから、2面体群の性質より共役を度外視して $U = \langle x^{2^t}, y \rangle$ と仮定できる ($t \geq 0$)。ここで次の事実を用いる。

命題 2.1 R が群 G の (k, λ, U) 差集合で U の部分群 N が $G \triangleright N$ をみたすとする。このとき \bar{R} は剰余群 $\bar{G} (= G/N)$ の $(k, \lambda|N|, \bar{U})$ 差集合である。

今の場合 $N = \langle x^{2^t} \rangle$ とおけば $G \triangleright N$ かつ $N \subset U$ なので命題 2.1 の結果が適用できて \bar{R} は剰余群 $\bar{G} (= G/N \simeq D_{2^{t+1}})$ において $(2^a, 2^{b+n-t}, \langle \bar{y} \rangle)$ 差集合となる。よって、 $U = \langle y \rangle$ の場合をまず考えればよいことがわかる。

補題 2.2 $X = \langle x, y \mid x^{2s} = y^2 = 1, yxy = x^{-1} \rangle$ を位数 $4s$ の 2面体群とする。 A, B を $\langle x \rangle$ の部分集合とし $R = A + By$ とおく。このとき、 R が X における $(2s, s, \langle y \rangle)$ -差集合であるための必要十分条件は $B = \langle x \rangle - A^{-1}$ かつ A が $\langle x \rangle$ の Hadamard 差集合となることである。

巡回群における Hadamard 差集合については次の結果が知られている。

定理 2.3 (R.J. Turyn [13]) 位数 2^{a+2} のアーベル群 A が Hadamard 差集合をもてば $\exp(A) \leq 2^{a+2}$ である。

補題 2.2 で s が 2 べきの場合は定理 2.3 より $s = 2$ のときだけが起こりうる。よって最初の 2面体群 G の場合では $D_{2^{t+1}} = D_8$ のときだけが可能性がある。つまり $t = 2$ である。関係式 (1) より $2^{n+1} \geq (2^{n-t+1})^2$ であるから $n \leq 3$ がわかる。 $n = 3$ の時は非存在が確かめられるので次を得る。

補題 2.4 2面体群 $G = \langle x, y \mid x^{2^n} = y^2 = 1, y^{-1}xy = x^{-1} \rangle$ が半正則相対差集合 R をもてば $n = 2$ で R は $(4, 2, \langle y \rangle)$ 差集合 $\{1, x, x^2, xy\}$ に同値である。

注意 2.5 上の補題 2.4 のなかで述べた "同値" とは次のこととする：
群 G において U_1 を禁止群とする半正則相対差集合 R_1 と U_2 を禁止群とする半正則相対差集合 R_2 が同値であるとは G の自己同型 σ と G の元 g があって $R_2 = \sigma(R_1)g$ かつ $U_2 = \sigma(U_1)$ と表せることをいう。

(2) 一般 4 元数群 $Q_{2^{n+1}}$

一般 4 元数群 G が R を $(2^a, 2^b, U)$ 差集合としてもつと仮定する。 $G \triangleright U$ のときは [2] を適用すればよい。 $G \not\triangleright U$ とすれば一般 4 元数群の性質より $|U| > 2$ かつ $U \supset Z(G) \simeq \mathbb{Z}_2$ である。従って \bar{R} は剰余群 $\bar{G} (= G/Z(G) \simeq D_{2^n})$ において $(2^a, 2^{b+1}, \bar{U})$ 差集合となる。従ってこの場合は補題 2.4 が適用できる。よってつぎの補題を得る。

補題 2.6 位数 2^{n+1} の一般 4 元数群 $G = \langle x, y \mid x^{2^{n-1}} = y^2, y^4 = 1, y^{-1}xy = x^{-1} \rangle$ が半正則相対差集合 R をもてば次のいずれかが成り立つ。

- (i) R は $(2^n, 2^{n-1}, \langle x^{2^{n-1}} \rangle)$ 差集合である。
- (ii) $n = 3$ で R は $(4, 4, \langle y \rangle)$ 差集合 $\{1, x, x^6, xy\}$ に同値である。

3 SD_{2^n} または $M_{n+1}(2)$ における半正則相対差集合

(1) 半 2 面体群 $SD_{2^{n+1}}$

半 2 面体群 $G = \langle x, y \mid x^{2^n} = y^2 = 1, y^{-1}xy = x^{-1}z, z = x^{2^{n-1}} \rangle$ の場合について考える。 R を G における $(2^a, 2^b, U)$ 差集合とする。 $G \triangleright U$ のときは [2] の結果が適用できるので $G \not\triangleright U$ と仮定してよい。まず $|U| > 2$ の場合を考えると半 2 面体群の性質より $Z(G) \subset U$ であるから \bar{R} は剰余群 $\bar{G} (= G/Z(G) \simeq D_{2^n})$ において $(2^a, 2^{b+1}, \bar{U})$ 差集合となる。従ってこの場合は補題 2.4 が適用できて $n = 3, G = SD_{16}, U = \langle y, z \rangle$ となり非存在が確かめられる。よって、 $G \not\triangleright U \simeq \mathbb{Z}_2$ の時を考えればよいことになる。一方 $SD_{2^{n+1}}$ の central involution $x^{2^{n-1}}$ 以外の involutions はすべて共役であるから $U = \langle y \rangle$ と仮定できる。

補題 3.1 R を $G = SD_{2^{n+1}}$ における $(2^n, 2^{n-1}, \langle y \rangle)$ 差集合とし $R = A + Bx + Cy + Dxy$ とおく。ただし $A, B, C, D \subset H = \langle x^2 \rangle (\simeq \mathbb{Z}_{2^{n-1}})$ 。このとき次の (i)-(iv) が成り立つ。

- (i) $AA^{-1} + BB^{-1} + CC^{-1} + DD^{-1} = 2^{n-1} + 2^{n-1}H$ 。
- (ii) $AB^{-1} + CD^{-1} + (A^{-1}B + C^{-1}D)x^2 = 2^{n-1}H$ 。
- (iii) $AC + BDx^2z = -2^{n-2} + 2^{n-2}H$ 。
- (iv) $(AD + BC)(1 + z) = 2^{n-1}H$ 。

R が半正則相対差集合なら Rg ($\forall g \in G$) も半正則相対差集合なので必要なら R を Ry と置き換えて $|A| + |D| \leq |B| + |C|$ としてよいが、さら

に必要な Rxy と置き換えることにより $|A| \leq |D|$ と仮定できる. このことと上の補題において等式の両辺の単位元の個数を比較することにより $|A| = 2^{n-2} - 2^{\frac{n}{2}-1}$, $|C| = 2^{n-2} + 2^{\frac{n}{2}-1}$ かつ $|B| = |D| = 2^{n-2}$ としてよいことが分かる. とくに n は偶数でなければならないことが分かる.

補題 3.1(iii) は $A^{-1} \cap C = B^{-1}zx^{-2} \cap D = \phi$ であることを言っているので, 上のことと合わせると

$$C = H - A^{-1}, \quad D = H - B^{-1}zx^{-2} \quad (2)$$

が成り立つ. これを補題 3.1(i)(ii) に代入して次を得る.

補題 3.2 (i) $AA^{-1} + BB^{-1} = 2^{n-2} + (2^{n-2} - 2^{\frac{n}{2}-1})H$

(ii) $(AB^{-1} + A^{-1}Bx^2)(1+z) = (2^{n-1} - 2^{\frac{n}{2}})H$

逆に, 補題 3.2 をみたま A, B がもしあれば等式 (2) により C, D がきまり, それは補題 3.1 をみたまので $(2^n, 2^{n-1}, \langle y \rangle)$ 差集合が構成できることになる.

(2) モジュラー 2-群 $M_{n+1}(2)$

モジュラー 2-群 $G = \langle x, y \mid x^{2^n} = y^2 = 1, y^{-1}xy = xz, z = x^{2^{n-1}} \rangle$ の場合について考える. R を G における $(2^a, 2^b, U)$ 差集合とする. $G \triangleright U$ のときは [2] の結果が適用できるので $G \not\subseteq U$ と仮定してよい. モジュラー 2-群の性質より G の位数 4 以上の部分群はすべて normal であるから $|U| = 2$ となるが $M_{n+1}(2)$ の central involution z 以外の involutions は y と yz であるがこれらは共役であるから $U = \langle y \rangle$ と仮定できる. 従って次を得る.

補題 3.3 R が $G = M_{n+1}(2)$ における $(2^a, 2^b, U)$ 差集合ならば次のいずれかが起こると仮定できる.

(i) $n = 3, R = \{1, x, x^3, x^2y\}$ かつ $U = \langle y, z \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

(ii) $U = \langle y \rangle$.

上の補題によりモジュラー 2-群の場合は $U = \langle y \rangle$ のときだけを考えれば十分であることが分かる.

補題 3.4 $U = \langle y \rangle$ であるとし $R = A + Bx + Cy + Dxy$ とおく ($A, B, C, D \subset H = \langle x^2 \rangle$). このとき次のいずれかがおこる.

(i) $AA^{-1} + BB^{-1} + CC^{-1} + DD^{-1} = 2^{n-1} + 2^{n-1}H$.

(ii) $AB^{-1} + CD^{-1} + (A^{-1}B + C^{-1}D)x^2 = 2^{n-1}H$.

(iii) $AC^{-1} + A^{-1}C + (BD^{-1} + B^{-1}D)z = -2^{n-1} + 2^{n-1}H$.

(iv) $(A^{-1}D + BC^{-1})x^2 + (AD^{-1} + B^{-1}C)z = 2^{n-1}H$.

上の補題は補題 3.1 の時と類似の形をしていることがわかる. この時と同様の議論をすることにより $C = H - A, D = H - Bz$ であり, $|A| = 2^{n-2} - 2^{\frac{n}{2}-1}, |C| = 2^{n-2} + 2^{\frac{n}{2}-1}, |B| = |D| = 2^{n-2}$ と仮定してもよい. さらに C, D を上の補題の (i), (ii) に代入することにより次が示される.

補題 3.5

- (i) $AA^{-1} + BB^{-1} = 2^{n-2} + (2^{n-2} - 2^{\frac{n}{2}-1})H.$
 (ii) $(AB^{-1} + A^{-1}Bx^2)(1+z) = (2^{n-1} - 2^{\frac{n}{2}})H.$

(3) 部分集合 A, B

補題 3.2 と補題 3.5 は位数 2^{2m-1} ($m = \frac{n}{2}$) の巡回群 H に関する同一の条件を述べている. 従って以下では次をみたす巡回群について考える.

$$X = \langle t \rangle \simeq \mathbb{Z}_{2^{2m-1}}, \quad m \geq 2 \quad (3)$$

$$A, B \subset X, \quad |A| = 2^{2m-2} - 2^{m-1}, \quad |B| = 2^{2m-2} \quad (4)$$

$$AA^{-1} + BB^{-1} = 2^{2m-2} + (2^{2m-2} - 2^{m-1})X \quad (5)$$

$$(AB^{-1} + A^{-1}Bt)(1+t^{2^{2m-2}}) = (2^{2m-1} - 2^m)X \quad (6)$$

1 の 2^{2m-1} 乗根 $\theta (\neq \pm 1)$ に対して X の指標 χ を $\chi(t) = \theta^2$ により定義する. これは X の位数 2 の元を $z (= t^{2^{2m-1}})$ とおくと $\chi \in (X/\langle z \rangle)^*$, $\chi \neq \chi_0$ をみたす指標 χ を考えることと同じである.

補題 3.6 条件 (3)(4)(5) のもとで $\alpha = \chi(A)$, $\beta = \chi(B)$ とおくと次が成り立つ.

$$\alpha = 2^{m-2}(\theta^r - \theta^{s+1}), \quad \beta = 2^{m-2}(\theta^{r-1} + \theta^s) \quad (\exists r, s \in \mathbb{Z})$$

(証明) : 条件 (5) と (6) により次が成り立つ.

$$\alpha\bar{\alpha} + \beta\bar{\beta} = 2^{2m-2} \quad (7)$$

$$\alpha\bar{\beta} + \bar{\alpha}\beta\theta^2 = 0, \quad (8)$$

よって $(\alpha + \beta\theta)\overline{(\alpha + \beta\theta)} = \alpha\bar{\alpha} + \beta\bar{\beta}\theta\bar{\theta} + \alpha\bar{\beta}\theta + \bar{\alpha}\beta\theta = \alpha\bar{\alpha} + \beta\bar{\beta} = 2^{2m-2}.$
 このことから次が示される.

$$(\alpha + \beta\theta)\overline{(\alpha + \beta\theta)} = 2^{2m-2} \quad (9)$$

θ を 1 の原始 2^w 乗根とする. 仮定より $2 \leq w \leq 2m-1$ であるが等式 (9) を円分体 $\mathbb{Z}[\theta]$ において素イデアル分解して次を得る.

$$((\alpha + \beta\theta)\overline{(\alpha + \beta\theta)}) = (1 - \theta)^{\phi(2^w)(2m-2)}$$

このことから $\mathbb{Z}[\theta]$ の元 τ により $\alpha + \beta\theta = 2^{m-1}\tau$ と表される. (9) 式より $|\tau| = 1$ である. 一方では χ が任意であったことから $|\sigma(\tau)| = 1 \quad \forall \sigma \in \text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ が成り立つ. Kronecker の定理より $\tau = \theta^r \quad \exists r \geq 0$ と表される. 従って次が分かる.

$$\alpha + \beta\theta = 2^{m-1}\theta^r. \quad (10)$$

(10) 式を (7) に代入して

$$\beta\bar{\beta} = 2^{m-2}(\theta^{r-1}\bar{\beta} + \bar{\theta}^{r-1}\beta).$$

であり, この式を変形すると

$$(\beta - 2^{m-2}\theta^{r-1})\overline{(\beta - 2^{m-2}\theta^{r-1})} = 2^{2m-4}$$

を得る. (9) のときと同様にして適当な整数 $s \geq 0$ に対して $\beta - 2^{m-2}\theta^{r-1} = 2^{m-2}\theta^s$ と書ける. これと (10) より補題を得る.

補題 3.7 条件 (3)(4)(5) のもとで $AB\langle t^{2^{2m-2}} \rangle = (2^{2m-2} - 2^{m-1})X$ が成り立つ.

(証明): 補題 3.6 より $\theta^r - \theta^{s+1} (= \theta(\theta^{r-1} - \theta^s)) \in \mathbb{Q}(\theta^2)$ かつ $\theta^{r-1} + \theta^s (= \theta^{-1}(\theta^r - \theta^{s+1})) \in \mathbb{Q}(\theta^2)$ である. よって $r \equiv s+1 \equiv 0 \pmod{2}$ または $r \equiv s+1 \equiv 1 \pmod{2}$ が成り立つ. 前者が成り立つときは $\theta^{r-1} + \theta^s = 0$ つまり $\beta = 0$ となり, 同様に後者のときは $\alpha = 0$ となる. したがって常に $\alpha\beta = 0$ が成り立つ. 補題を示すには次の "Inversion formula" を適用すればよい.

Inversion formula

有限アーベル群 G の群環 $\mathbb{C}[G]$ の元 T が単位指標以外の G の指標 χ に対して $\chi(T) = 0$ をみたせばある複素数 c に対して $T = cG$ が成り立つ.

上にのべた $\{X, A, B\}$ に対して Hadamard 差集合を構成する. まず一般四元数群 $Q = X\langle y \rangle \simeq Q_{2^{2m}}$ を $y^2 = t^{2^{2m-2}}$, $y^{-1}ty = t^{-1}$ で定める. 次に Q の部分集合 D を $D = A + By$ で定める. このとき次が容易に確かめられる.

$$DD^{-1} = AA^{-1} + BB^{-1} + AB(1 + y^2)y.$$

このことは $DD^{-1} = 2^{2m-2} + (2^{2m-2} - 2^{m-1})Q$ を意味するから D は Q の Hadamard 差集合である. ここで $U = \langle y^2 \rangle (\simeq \mathbb{Z}_2)$ とおけば $Q \triangleright U$ で Q/U は 2 面体群である. 2 群の Hadamard 差集合については次の定理が知られている.

定理 3.8 (*K.H. Leung & S.L. Ma*) 位数 2^{2a+2} の群 G が位数 2^b の正規部分群 U で $b < a$ であるものをもつと仮定する. もし G/U が巡回群か 2 面体群ならば G は Hadamard 差集合を持たない.

上の定理を Q に対して適用して次を得る.

補題 3.9 補題 3.6 の仮定のもとでは $m = 2$ が成り立つ.

4 結論と補足

補題 2.4, 2.6, 3.9 を用いて結論として次の定理を得る.

定理 4.1 G を指数 2 の巡回部分群をもつ非可換 2-群とする. G が部分群 U に関する半正則相対差集合をもてば次のいずれかが成り立つ.

- (i) $G \simeq Q_{2^{n+1}}$, $G \triangleright U (\simeq \mathbb{Z}_2)$,
- (ii) $n = 2$, $G \simeq D_8$, $G \not\triangleright U (\simeq \mathbb{Z}_2)$.
- (iii) $n = 3$, $G \simeq Q_{16}$, $G \not\triangleright U (\simeq \mathbb{Z}_4)$.
- (iv) $n = 3$, $G \simeq M_4(2)$, $G \triangleright U (\simeq \mathbb{Z}_4)$.
- (v) $n = 4$, $G \simeq SD_{32}$, $G \not\triangleright U (\simeq \mathbb{Z}_2)$.
- (vi) $n = 4$, $G \simeq M_5(2)$, $G \not\triangleright U (\simeq \mathbb{Z}_2)$.

禁止群 U の正規性の仮定を外しても $Q_{2^{n+1}}$ の場合以外の無限系列は期待に反して現れなかったが, 上記の (ii)(iii)(v)(vi) が定理 1.7 に新たに追加されたことになる. (iii)(iv) は位数 4 の射影平面に関係するが (v)(vi) はその意味付けが分からない.

注意 4.2 p -群で半正則相対差集合の分類が完全に終わっているのは次の 2 つである.

- (Gluck [3], Hiramine [4], Ronayi-Szonyi [11])
 $\mathbb{Z}_p \times \mathbb{Z}_p$ の半正則相対差集合の分類
- (Ma-Pott [7])
 $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ の半正則相対差集合の分類

p -群における半正則相対差集合についてはまだ分かっていないことが多いし, 解決のためには今後いろいろな方法が開発されなければならないと思われる. 最後に, この方面で解決すべきと考える問題を紹介させていただきたい.

問題

- $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ かつ $U \simeq \mathbb{Z}_p$ ($p > 2$) の半正則相対差集合を分類すること. (これが解決すれば位数 p^2 の planar 関数の決定の問題も解決すると考える, cf. [7] p838)
- $G \simeq \mathbb{Z}_{p^m} \times \mathbb{Z}_{p^m}$ かつ $U \simeq \mathbb{Z}_p$ ($p > 2, m > 1$) (多分非存在?)
- $M(p)$ または $M_3(p)$ ($p > 2$) で禁止群が center であるような半正則相対差集合を分類すること. (これが解決すれば位数 p^4 の非可換 p -群における半正則相対差集合が決定できると考えられる)
- $M_n(p)$ ($p > 2, n > 3$) で禁止群が center の位数 p の部分群であるような半正則相対差集合を分類すること. (多分非存在?)

参考文献

- [1] D.T. Elvira and Y. Hiramine, On Non-Abelian Semi-Regular Relative Difference Sets , "Finite Fields and Applications", (2000), Springer, 122-127
- [2] D.T. Elvira and Y. Hiramine, On Semi-Regular Relative Difference Sets in Non-Abelian p-Groups, to appear.
- [3] D. Gluck, A note on permutation polynomials and finite geometries, Discrete Math. **80**(1990) 97-100
- [4] Y. Hiramine, A conjecture on affine planes of prime order, J. of Combinatorial Theory Ser. A **52**(1989), 44-50.
- [5] N. Ito, On Hadamard Groups, J. of Algebra **168** (1994) 981-987.
- [6] K.H. Leung, S.L. Ma, Partial difference triples, J. of Algebraic Combinatorics **2** (1993) 397-409.
- [7] S.L. Ma and A. Pott, Relative difference sets, planar functions, and generalized Hadamard matrices, J. of Algebra **175** (1995) 505-525.
- [8] S.L. Ma and B. Schmidt, On (p^a, p, p^a, p^{a-1}) -Relative difference sets, Designs, Codes and Cryptography **6** (1995) 57-71.
- [9] A. Pott, Finite Geometry and Character Theory. Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995)
- [10] A. Pott, On the structure of abelian groups admitting divisible difference sets, J. of Combin. Ser. A. **65** (1994) 202-213
- [11] L. Ronayi and T. Szonyi, Planar functions over finite fields, Combinatorica **9**(1989), 315-320
- [12] B. Schmidt, On (p^a, p^b, p^a, p^{a-b}) -Relative Difference Sets, J. of Algebraic Combinatorics **6** (1997) 279-297.
- [13] R. J. Turyn, Character sums and difference sets, Pacific J. of Math. **15** (1965) 319-346.

Configuration spaces and root systems

J. Sekiguchi

1 Introduction

This is a survey of my recent works [13], [15], [6], [17] and related topics. The object which I treat in this survey is the configuration space $P(2, n)$ of marked n points on the projective plane. Among others, I concentrate my attention on the spaces $P(2, 6)$, $P(2, 7)$, $P(2, 8)$, because they admit actions of the Weyl groups $W(E_6)$, $W(E_7)$, $W(E_8)$, respectively. Moreover, I treat the configuration spaces on the real number field. In this case, $P(2, n)$ is the union of connected components. Let \mathcal{P}_n be the set of connected components of $P(2, n)$. One of my interests is the determination of $W(E_n)$ -orbital structure of \mathcal{P}_n .

We now restrict our attention to the cases $n = 6, 7$, because these cases are easier to explain the results than the case $n = 8$. One of our purposes is to clarify the relationship between the geometry of 6 lines and 7 lines on the real projective plane $P^2(\mathbf{R})$ and the root systems of types E_6 and E_7 .

For a moment, the number n means 6 or 7. We introduce marked n lines (l_1, l_2, \dots, l_n) on $P^2(\mathbf{R})$. We give conditions on these n lines:

- I. The n lines l_1, l_2, \dots, l_n are mutually different.
- II. No three of l_1, l_2, \dots, l_n intersect at a point.
- III. There is no conic tangent to six of l_1, l_2, \dots, l_n .

The totality of marked n lines on $P^2(\mathbf{R})$ with conditions I, II forms the configuration space $P(2, n)$: the space $P(2, n)$ is defined by

$$P(2, n) = GL(3, \mathbf{R}) \backslash M'(3, n) / (\mathbf{R}^\times)^n,$$

where $M'(3, n)$ is the set of $3 \times n$ real matrices of which no 3-minor vanishes. On the other hand, the totality of marked n lines on $P^2(\mathbf{R})$ with conditions I, II, III forms a subset of $P(2, n)$ which we denote by $P_0(2, n)$. Both $P(2, n)$, $P_0(2, n)$ are affine open subsets of $\mathbf{R}^{2(n-4)}$. Permutations on the n lines l_1, l_2, \dots, l_n induce a biregular S_n -action on $P(2, n)$ (and also that on $P_0(2, n)$). It is stressed here that the S_n -action on $P_0(2, n)$ is naturally extended to a biregular $W(E_n)$ -action (cf. [12], [14]). Let \mathcal{P}_n be the set of connected components of $P_0(2, n)$. The $W(E_n)$ -action on $P_0(2, n)$ naturally induces that on \mathcal{P}_n .

I now explain the motivations of the present study briefly. It is an interesting problem to construct a tame compactification of the configurations space $P_{\mathbf{C}}(n, k)$ of marked k hyperplanes on the complex projective space $P^n(\mathbf{C})$. In the case of $n = 1$, there is a

nice compactification of $P_C(1, k)$, the so called Terada model (cf. [22]). We note here that $P_C(1, k)$ admits S_k -action. What happens if we treat $P(1, k)$ instead of $P_C(1, k)$, where $P(1, k)$ is the configuration space of k -points of $P^1(\mathbb{R})$. In [23], it is shown that the S_k -action on the totality of connected components of $P(1, k)$ is transitive and that each connected component in question is described in terms of "juzu" introduced there. On the other hand, in the case $(n, k) = (2, 6)$, there is a tame compactification of the configuration space of marked six lines of $P^2(\mathbb{C})$ with conditions I, II, III above constructed in [9] which is called Naruki's cross ratio variety and denoted by \mathcal{C} . As an application of the results of [9], [12], already shown is the result which we are going to explain (cf. [17]). We note that $P_0(2, 6)$ admits a $W(E_6)$ -action (cf. [9], [12]). Then the result for the case $P_0(2, 6)$ given in [17] similar to the case of Terada models is that there are 432 connected components in $P_0(2, 6)$ and that the $W(E_6)$ -action on the set is transitive. My attempt for the generalization to the cases $n = 7, 8$ will be given in the main text.

Our results are related with the studies of Commings and White [2], [3], [24] introduced in Grünbaum [7].

2 Root system of type E_n ($n = 6, 7, 8$)

We begin this note by introducing the root system of type E_n ($n = 6, 7, 8$). The description of roots is essentially same as that given in T. Shioda [20].

2.1 Root system of type E_8

Let E be an 8-dimensional Euclidean space with an inner product $\langle \cdot, \cdot \rangle$ and an orthonormal basis $\{e_j; 1 \leq j \leq 8\}$. We define the following 120 vectors of E :

$$\begin{aligned}
 t_1 &= \frac{1}{2}(e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_7 + e_8) \\
 r_{1j} &= t_1 - e_{j-1} - e_8 && (1 < j \leq 8) \\
 r_{ij} &= e_{i-1} - e_{j-1} && (1 < i < j \leq 8) \\
 r_{1jk} &= -e_{j-1} - e_{k-1} && (1 < j < k \leq 8) \\
 r_{ijk} &= t_1 - e_{i-1} - e_{j-1} - e_{k-1} - e_8 && (1 < i < j < k \leq 8) \\
 t_i &= -e_{i-1} - e_8 && (1 < i \leq 8) \\
 t_{1j} &= e_{j-1} - e_8 && (1 < j \leq 8) \\
 t_{ij} &= t_1 - e_{i-1} - e_{j-1} && (1 < i < j \leq 8)
 \end{aligned}$$

The totality $\Delta(E_8)$ of $\pm r_i, \pm r_{ij}, \pm r_{ijk}, \pm t_i, \pm t_{ij}$ forms a root system of type E_8 . It is clear that

$$r_{12}, r_{123}, r_{23}, r_{34}, r_{45}, r_{56}, r_{67}, r_{78}$$

can serve as a system of positive roots; its Dynkin diagram is given as

$$\begin{array}{cccccccc}
 r_{12} & \text{---} & r_{23} & \text{---} & r_{34} & \text{---} & r_{45} & \text{---} & r_{56} & \text{---} & r_{67} & \text{---} & r_{78} \\
 & & & & | & & & & & & & & \\
 & & & & r_{123} & & & & & & & &
 \end{array}$$

Let s_{ij}, s_{ijk} be the reflections on E with respect to r_{ij}, r_{ijk} and let τ_i, τ_{ij} be the reflections on E with respect to t_i, t_{ij} . Before giving the actions of $s_{ij}, s_{ijk}, \tau_i, \tau_{ij}$ on $\Delta(E_8)$, we note that

$$\begin{aligned} r_{ij} \perp r_{kl}, \quad r_{ij} \perp r_{ijk}, \quad r_{ij} \perp r_{klm}, \quad r_{ij} \perp t_k, \quad r_{ij} \perp t_{ij}, \quad r_{ij} \perp t_{kl}, \\ r_{ijk} \perp r_{ilm}, \quad r_{ijk} \perp t_l, \quad r_{ijk} \perp t_i, \quad t_i \perp t_{ij}, \quad t_{ij} \perp t_{kl}. \end{aligned}$$

We note that here and hereafter roots with indices containing different letters denote different roots. The actions of the reflections with respect to Δ (up to signs) are as follows:

$$\begin{aligned} s_{ij} &: \text{permutation of the indices } i \text{ and } j, \\ s_{ijk} &: r_{il} \leftrightarrow r_{jkl}, \quad r_{lmn} \leftrightarrow r_{pq} (\{i, j, k, l, m, n, p, q\} = \{1, 2, \dots, 8\}), \quad t_i \leftrightarrow t_{jk} \\ \tau_i &: r_{ij} \leftrightarrow t_j, \quad r_{ijk} \leftrightarrow t_{jk}, \\ \tau_{ij} &: r_{jk} \leftrightarrow t_{ik}, \quad r_{ijk} \leftrightarrow t_k, \quad r_{klm} \leftrightarrow r_{npq} (\{i, j, k, l, m, n, p, q\} = \{1, 2, \dots, 8\}). \end{aligned}$$

The group generated by the reflections $s_{ij}, s_{ijk}, \tau_i, \tau_{ij}$ is nothing but the Weyl group $W(E_8)$ of type E_8 . In the sequel, the symmetric group S_8 is identified with the subgroup of $W(E_8)$ generated by s_{ij} ($i, j = 1, 2, \dots, 8$) unless otherwise stated.

2.2 Root system of type E_7

For a root $\alpha \in \Delta(E_8)$, the subset of $\Delta(E_8)$ consisting of all roots orthogonal to α becomes a root system of type E_7 . In particular, take t_8 as α . In this case, roots of $\Delta(E_8)$ orthogonal to α are

$$\pm r_{jk} (1 \leq j < k < 8), \quad \pm r_{jkl} (1 \leq j < k < l < 8), \quad \pm t_{j8} (1 \leq j < 8).$$

The totality of these roots becomes a root system of type E_7 . In the sequel, we denote it by $\Delta(E_7)$.

2.3 Root system of type E_6

In this case, the subset of roots of $\Delta(E_8)$ orthogonal to both of t_7 and t_8 becomes a root system $\Delta(E_6)$ of type E_6 . It is easy to see that $\Delta(E_6)$ consists of

$$\pm r_{jk} (1 \leq j < k \leq 7), \quad \pm r_{jkl} (1 \leq j < k < l \leq 7), \quad \pm t_{78}.$$

3 Configurations of n lines on the real projective plane

We introduced marked n lines (l_1, l_2, \dots, l_n) on $\mathbf{P}^2(\mathbf{R})$ with conditions I, II of Introduction. We define p -gons for a marked n lines $(l_j)_{1 \leq j \leq n}$. Each connected component of $\mathbf{P}^2(\mathbf{R}) - \cup_{j=1}^n l_j$ is called a polygon. If it is surrounded by p lines, it is called a p -gon.

The totality of marked n lines on $\mathbf{P}^2(\mathbf{R})$ with conditions I, II forms the configuration space $\mathbf{P}(2, n)$. Permutations on the n lines l_1, l_2, \dots, l_n induce a biregular S_n -action on $\mathbf{P}(2, n)$.

We are going to define the action of $W(E_n)$ on $\mathbf{P}(2, n)$ in a concrete manner. Let $(l_j)_{1 \leq j \leq n}$ be a marked n lines. We assume that l_j is defined by

$$l_j : a_{1j}\xi + a_{2j}\eta + a_{3j}\zeta = 0,$$

where $(\xi : \eta : \zeta)$ is a homogeneous coordinate of $\mathbf{P}^2(\mathbf{R})$. For the marked n lines (l_j) , we define a $3 \times n$ matrix

$$X = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \end{pmatrix}.$$

By a projective linear transformation, we may take l_1, l_2, l_3, l_4 as $\xi = 0, \eta = 0, \zeta = 0, \xi + \eta + \zeta = 0$. Moreover, we may divide the equation of l_j by a_{1j} ($5 \leq j \leq n$). In this manner, it is possible to choose as a representative of any element of $\mathbf{P}(2, n)$ a matrix of the form

$$X = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & 1 & x_1 & x_2 & \cdots & x_{n-4} \\ 0 & 0 & 1 & 1 & y_1 & y_2 & \cdots & y_{n-4} \end{pmatrix}$$

Therefore $\mathbf{P}(2, n)$ is regarded as a quasi-affine subset of $\mathbf{R}^{2(n-4)}$ by the correspondence

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & 1 & x_1 & x_2 & \cdots & x_{n-4} \\ 0 & 0 & 1 & 1 & y_1 & y_2 & \cdots & y_{n-4} \end{pmatrix} \longrightarrow (x_1, x_2, \dots, x_{n-4}, y_1, y_2, \dots, y_{n-4}).$$

We introduce the following n birational transformations $\sigma_1, \dots, \sigma_n, \sigma_R$ on (x, y) -space:

$$\sigma_1 : (x_1, x_2, \dots, x_{n-4}, y_1, y_2, \dots, y_{n-4}) \longrightarrow \left(\frac{1}{x_1}, \frac{1}{x_2}, \dots, \frac{1}{x_{n-4}}, \frac{y_1}{x_1}, \frac{y_2}{x_2}, \dots, \frac{y_{n-4}}{x_{n-4}} \right)$$

$$\sigma_2 : (x_1, x_2, \dots, x_{n-4}, y_1, y_2, \dots, y_{n-4}) \longrightarrow (y_1, y_2, \dots, y_{n-4}, x_1, x_2, \dots, x_{n-4})$$

$$\sigma_3 : (x_1, x_2, \dots, x_{n-4}, y_1, y_2, \dots, y_{n-4}) \longrightarrow (x'_1, x'_2, \dots, x'_{n-4}, y'_1, y'_2, \dots, y'_{n-4})$$

$$\sigma_4 : (x_1, x_2, \dots, x_{n-4}, y_1, y_2, \dots, y_{n-4}) \longrightarrow \left(\frac{1}{x_1}, \frac{x_2}{x_1}, \dots, \frac{x_{n-4}}{x_1}, \frac{1}{y_1}, \frac{y_2}{y_1}, \dots, \frac{y_{n-4}}{y_1} \right)$$

$$\sigma_{k+4} : x_k \leftrightarrow x_{k+1}, y_k \leftrightarrow y_{k+1} \quad (k = 1, 2, \dots, n-5),$$

$$\sigma_0 : x_i \rightarrow \frac{1}{x_i}, \quad y_i \rightarrow \frac{1}{y_i} \quad (i = 1, \dots, n-4),$$

where

$$x'_j = \frac{x_j - y_j}{1 - y_j}, \quad y'_j = \frac{y_j}{y_j - 1}, \quad j = 1, 2, \dots, n-4.$$

The correspondence

$$s_{12} \longrightarrow \sigma_1, \quad s_{123} \longrightarrow \sigma_0, \quad s_{j,j+1} \longrightarrow \sigma_{j-1} \quad (j = 3, \dots, n-1)$$

induces a surjective homomorphism $p_{W(E_n)}$ of $W(E_n)$ to the group $\bar{W}(E_n)$ generated by s_1, \dots, s_{n-1}, s_0 . In the sequel, we frequently confuse $g \in W(E_n)$ with $p_{W(E_n)}(g)$ and subgroups of $W(E_n)$ with their images by $p_{W(E_n)}$ for simplicity.

Remark 1 For arbitrary n , it is possible to define $W(E_n)$. But, in the sequel, we mainly treat the cases $n = 6, 7, 8$.

Now we define a set of irreducible polynomials consisting of f_1, \dots, f_N with the following properties:

1. $f_1 = x_1$.
2. For each $i = 1, \dots, N, j = 0, 1, \dots, n - 1$,

$$f_i \circ \sigma_j = c_{ij} f_1^{m_1} \cdots f_N^{m_N},$$

where c_{ij} is a non-zero constant and $m_k \in \mathbb{Z} (k = 1, \dots, N)$.

3. The set $\{f_1, \dots, f_N\}$ is minimal under the conditions (a), (b).

Let $P_0(2, n)$ be the intersection of $f_j \neq 0 (j = 1, 2, \dots, N)$ in $\mathbb{R}^{2(n-4)}$. Then $W(E_n)$ acts on $P_0(2, n)$ biregularly.

Lemma 1 (i) If $n = 6, 7, 8$, then $N = 15, 35, 84$, respectively.

(ii) Assume that $n = 6, 7$. Let (l_1, l_2, \dots, l_n) be a marked n lines on $P(\mathbb{R})$. Then (l_1, l_2, \dots, l_n) is contained in $P_0(2, n)$ if and only if (l_1, l_2, \dots, l_n) satisfies the conditions I, II, III of Introduction.

Let \mathcal{P}_n be the set of connected components of $P_0(2, n)$. Clearly $W(E_n)$ acts on \mathcal{P}_n . My interest is then the following.

Problem 1 Determine the $W(E_n)$ -orbital structure of \mathcal{P}_n .

4 Geometry of six lines on the real projective plane

The results of this section are based on the joint work with M. Yoshida [17].

4.1 Pentagonal sets and pent-diagrams

Let A be a set of ten letters $a_{ij} (= a_{ji})$ indexed by numbers $i, j (1 \leq i < j \leq 5)$.

Definition 1 (i) An injection f of A to Δ is called a pentagonal map if the following conditions hold:

1. $\langle f(a_{ij}), f(a_{i'j'}) \rangle \geq 0 \quad \forall a_{ij}, a_{i'j'} \in A$.
2. For $a_{ij}, a_{i'j'} \in A$, $\langle f(a_{ij}), f(a_{i'j'}) \rangle = 0$ if and only if $\{i, j\} \cap \{i', j'\} \neq \emptyset$.

(ii) A subset U of Δ is called a pentagonal set if there is a pentagonal map f such that $U = f(A)$.

It follows from the definition that A admits a natural action of S_5 , the symmetric group on five letters. If f is a pentagonal map, so is $f \circ \sigma$ for each $\sigma \in S_5$. This implies in particular that the set $f(A)$ admits an S_5 -action.

To a pentagonal map f , there associates a diagram similar to Dynkin diagrams which we are going to explain.

Definition 2 (i) A pent-diagram consists of ten circles and fifteen segments joining circles (as in the figure at the last page of this note) with the following properties:

1. There is a bijection between A and the totality of ten circles of the pent-diagram.
2. Two circles corresponding to $a_{ij}, a_{i'j'} \in A$ are joined by a segment if and only if $\{i, j\} \cap \{i', j'\} = \emptyset$.

(ii) Let f be a pentagonal map. Then the pent-diagram for f denoted by $\mathcal{P}(f)$ is the pent-diagram the circle of which corresponding to a_{ij} is attached with the root $f(a_{ij})$.

Remark 2 Pent-diagrams are usually called Petersen graphs in a literature.

Example 1 There is a pentagonal map f such that $S = f(A)$, where

$$S = \{r_{124}, r_{126}, r_{245}, r_{134}, r_{156}, r_{135}, r_{235}, r_{456}, r_{236}, r_{346}\}.$$

It is easy to show the theorem below.

Theorem 1 The group $W(E_6)$ acts on the set of pentagonal sets transitively.

Let G_1 be the subgroup of $W(E_6)$ generated by s_{jj+1} ($j = 1, 2, 3, 4, 5$). Clearly G_1 is isomorphic to S_6 . In our application, the S_6 -orbital structure of pentagonal sets is important.

Theorem 2 The set of pentagonal sets is decomposed into four S_6 -orbits whose representatives are given below:

(1)	PO	$\{r_{12}, -r_{23}, r_{34}, -r_{45}, r_{56}, r_{16}, -r_{123}, -r_{156}, -r_{345}, t_{78}\}$
	PI	$\{r_{126}, -r_{135}, -r_{145}, -r_{235}, r_{246}, r_{346}, -r_{15}, r_{26}, -r_{35}, r_{46}\}$
	PII	$\{-r_{145}, r_{356}, r_{235}, r_{234}, r_{246}, r_{126}, r_{136}, -r_{24}, r_{16}, -r_{35}\}$
	PIII	$\{r_{234}, r_{456}, r_{126}, r_{125}, r_{145}, r_{134}, r_{136}, r_{356}, r_{235}, r_{246}\}$

Remark 3 There is an S_5 -action on a pent-diagram (cf. [17]).

4.2 Four types of systems of marked six lines

Given a system $l \in P_0(2, 6)$ of six lines $\{l_1, \dots, l_6\}$. Totality of the systems in $P_0(2, 6)$ which can be obtained by continuous deformations of the l'_j form a connected component of $P_0(2, 6)$, which is a 4-dimensional cell. There are four S_6 -orbits of the sets of connected components of $P_0(2, 6)$, referred to as O, I, II, III. Each orbit is characterized by the numbers of polygons that any of the systems in it cut out (cf. [7]):

Types	hexagon	pentagon	rectangles	triangles
O	1	0	9	6
I	0	2	8	6
II	0	3	6	7
III	0	6	0	10

A system of six lines is said to be of type $T \in \{O, I, II, III\}$ if it belongs to the orbit T. You can see the arrangements of the four types above at the last page of this note.

4.3 A relation between the ten triangles of a system of type III and a pentagonal set

Let l be the system of labeled six lines given in Figure I, there are ten triangles given as follows:

$$123, 125, 136, 146, 234, 246, 256, 345, 356, 145$$

where ijk means the triangle surrounded by the lines l_i, l_j, l_k . You can find that there is a one-one map between the set of ten triangles given above and the pentagonal set in Example 1.

4.4 Naruki's cross ratio variety

We define a map σ_{E_6, D_4} of $P(E')$ to $CR(P)^{45}$ which is actually $W(E_6)$ -equivariant. Here E means the vector space spanned by the root vectors of type E_6 and E' means the set of regular elements. We frequently confuse E and its dual space. Let $C' = \sigma_{\Delta(E_6), D_4}(P(E'))$ and let C be its Zariski closure in $CR(P)^{45}$.

Theorem 3 (cf. [9])

- (i) C is 4-dimensional and non-singular.
- (ii) The $W(E_6)$ -action on C is biregular.
- (iii) $C - C'$ is a divisor with normal crossings. There are 76 irreducible components of $C - C'$ each of which is smooth.

We define a map F of $P(E')$ to R^4 by

$$F(t) = (x_1(t), x_2(t), y_1(t), y_2(t)),$$

where

$$(2) \quad \begin{aligned} x_1(t) &= \frac{h_{24} \cdot h_{234} \cdot h_{15} \cdot h_{135}}{h_{14} \cdot h_{134} \cdot h_{25} \cdot h_{235}}, & x_2(t) &= \frac{h_{24} \cdot h_{234} \cdot h_{16} \cdot h_{136}}{h_{14} \cdot h_{134} \cdot h_{26} \cdot h_{236}}, \\ y_1(t) &= \frac{h_{34} \cdot h_{234} \cdot h_{15} \cdot h_{125}}{h_{14} \cdot h_{124} \cdot h_{35} \cdot h_{235}}, & y_2(t) &= \frac{h_{34} \cdot h_{234} \cdot h_{16} \cdot h_{126}}{h_{14} \cdot h_{124} \cdot h_{36} \cdot h_{236}}, \end{aligned}$$

where h_{ij}, h_{ijk} mean the values of r_{ij}, r_{ijk} at $t \in E$, respectively.

Then F is $W(E_6)$ -equivariant and its image $F(P(E'))$ coincides with $P_0(2, 6) - Q$, where Q is a divisor of $P_0(2, 6)$; a system $l = (l_1, \dots, l_6) \in P_0(2, 6)$ is contained in Q if and only if there is a conic tangent to all of l_1, \dots, l_6 .

We are going to write down the 76 irreducible components of $\mathcal{D} = \mathcal{C} - \mathcal{C}'$. Each component is described in terms of a subroot system of $\Delta(E_6)$. Noting this, we put

$$Y_{ij} = Y_{\Delta(E_6), D_4}(\{\pm r_{ij}\}), \quad Y_{ijk} = Y_{\Delta(E_6), D_4}(\{\pm r_{ijk}\}), \quad Y_{l_78} = Y_{\Delta(E_6), D_4}(\{\pm l_{78}\})$$

following the notation in [11]. Then Y_{ij} and Y_{ijk} are divisors in \mathcal{C} . Roughly speaking, the subvariety Y_{ij} is the image of $h_{ij} = 0$ by the map $cr_{\Delta(E_6), D_4}$.

We now take three subsets $\Delta_1, \Delta_2, \Delta_3$ of $\Delta(E_6)$ with the following condition:

- Condition 1** (i) Each of $\Delta_1, \Delta_2, \Delta_3$ is a root system of type A_2 .
(ii) $\Delta_1, \Delta_2, \Delta_3$ are mutually orthogonal.
(iii) The vectors of $\Delta_1 \cup \Delta_2 \cup \Delta_3$ span E .

Let $Y_{\Delta(E_6), D_4}(\Delta_j)$ ($j = 1, 2, 3$) be the subvarieties of \mathcal{C} defined in [11]. Then as is shown in [11], Lemma 3.5,

$$Y_{\Delta(E_6), D_4}(\Delta_1) = Y_{\Delta(E_6), D_4}(\Delta_2) = Y_{\Delta(E_6), D_4}(\Delta_3).$$

We determine triplets $\{\Delta_1, \Delta_2, \Delta_3\}$ satisfying Condition 4.4. It is easy to see that there are two kinds of such sets. The first one is of the form

$$\Delta_1 = \{\pm r_{i_1 i_2}, \pm r_{i_2 i_3}, \pm r_{i_1 i_3}\}, \quad \Delta_2 = \{\pm r_{i_4 i_5}, \pm r_{i_5 i_6}, \pm r_{i_4 i_6}\}, \quad \Delta_3 = \{\pm r, \pm r_{i_1 i_2 i_3}, \pm r_{i_4 i_5 i_6}\}.$$

We write $Z_{i_1 i_2 i_3, i_4 i_5 i_6}$ for the divisor $Y_{\Delta(E_6), D_4}(\Delta_1)$ in this case. The second one is of the form

$$\Delta_1 = \{\pm r_{i_1 i_2}, \pm r_{i_2 i_3 i_4}, \pm r_{i_1 i_3 i_4}\}, \quad \Delta_2 = \{\pm r_{i_3 i_4}, \pm r_{i_3 i_5 i_6}, \pm r_{i_4 i_5 i_6}\}, \quad \Delta_3 = \{\pm r_{i_5 i_6}, \pm r_{i_1 i_2 i_5}, \pm r_{i_1 i_2 i_6}\}.$$

We write $Z_{i_1 i_2, i_3 i_4, i_5 i_6}$ for the divisor $Y_{\Delta(E_6), D_4}(\Delta_1)$ in this case.

Remark 4 From the definition, we have the following:

- (a) $Z_{i_1 i_2 i_3, i_4 i_5 i_6} = Z_{i_4 i_5 i_6, i_1 i_2 i_3}$.
(b) $Z_{i_1 i_2, i_3 i_4, i_5 i_6} = Z_{i_5 i_6, i_1 i_2, i_3 i_4} \neq Z_{i_1 i_2, i_5 i_6, i_3 i_4}$.

4.5 The main result for the case $n = 6$

The following theorem holds for the case of systems of marked six lines.

Theorem 4 (1) *There is a unique simply connected and connected component P of C' bounded by the 15 divisors below:*

$$Y_{156}, Y_{123}, Y_{345}, Y_{346}, Y_{236}, Y_{256}, Y_{245}, Y_{124}, Y_{146}, Y_{135},$$

$$Z_{13,46,25}, Z_{15,24,36}, Z_{14,35,26}, Z_{16,23,45}, Z_{12,56,34}.$$

(2) *The group consisting of $w \in W(E_6)$ such that $w \cdot P = P$ coincides with S_5' .*

(3) *There are 432 connected components of C' ; they are transitive under the $W(E_6)$ -action.*

It is easy to describe the S_6 -orbit of P and connected components of C' adjacent to P (cf. [17]).

5 Geometry of seven lines on the real projective plane

5.1 Connected components of $C'_R(\Delta(E_7), D_4)$

We start with introducing a 3×7 matrix

$$X = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & -9 & 3/5 & -17/10 & -3/2 \\ 1 & 0 & 1 & 4 & 9/5 & 53/10 & 21/10 \end{pmatrix}.$$

Then by taking the entries of the vector $(1 \ x \ y) \cdot X$, we obtain seven lines L_1, \dots, L_{10} of the real projective plane regarding x, y as inhomogeneous coordinates.

By the seven lines above, we obtain ten triangles (T_j) ($j = 1, 2, \dots, 10$) surrounded by the three lines

(3)	(T_1)	$L_1 L_3 L_6$	γ_{136}
	(T_2)	$L_1 L_2 L_3$	γ_{123}
	(T_3)	$L_2 L_5 L_7$	γ_{257}
	(T_4)	$L_1 L_6 L_7$	γ_{167}
	(T_5)	$L_5 L_6 L_8$	γ_{568}
	(T_6)	$L_2 L_6 L_8$	γ_{268}
	(T_7)	$L_1 L_5 L_8$	γ_{158}
	(T_8)	$L_3 L_5 L_7$	γ_{357}
	(T_9)	$L_3 L_7 L_8$	γ_{378}
	(T_{10})	$L_1 L_7 L_8$	γ_{178}

Corresponding to these ten triangles, there is a 6-polytope of $C'_R(\Delta(E_7), D_4)$.

Theorem 5 (cf.[15]) *There is a simply connected and connected component P of $C_{\mathbb{R}}^1(\Delta(E_7), D_4)$ surrounded by the following divisors:*

A_1	$Y_{126}, Y_{367}, Y_{456}, Y_{235}, Y_{134}, Y_{157},$
A_2	$Y_{237}, Y_{124}, Y_{135}, Y_{457},$
A_3	$Z_{26,145}, Z_{237,456}, Z_{45,267}, Z_{37,246}, Z_{126,457}, Z_{14,236},$ $Z_{57,146}, Z_{12,467}, Z_{67,123}, Z_{46,357}, Z_{23,567}, Z_{124,367},$
A_4	$W_{1,37,45}, W_{3,26,57}, W_{3,12,45}, W_{1,23,46}, W_{5,14,67}, W_{5,12,37},$
A_5	$W_{1,23,45}, W_{5,14,37}, W_{3,12,57},$
A_6	$X_{123}, X_{145}, X_{357}$

Let $\mathcal{H}(P)$ be the totality of these divisors. Then, for each $w \in W(E_7)$, $w \cdot P$ is surrounded by the divisors contained in $w \cdot \mathcal{H}(P)$.

We consider automorphisms of P in $W(E_7)$. Let $s_{ij}, s_{ijk}, \tau_{i8}$ be the reflections defined before. Using this notation, we put

$$\mu_1 = s_{12}s_{34}s_{57}\tau_{68}, \quad \mu_2 = s_{35}s_{24}s_{56}\tau_{28}.$$

Then it is easy to show that

$$\mu_1 \cdot P = \mu_2 \cdot P = P.$$

Let G_P be the group generated by μ_1, μ_2 . Then G_P is isomorphic to S_4 , the symmetric group on four letters. This is proved as follows. First we note that

$$\mu_1^2 = 1, \quad \mu_2^3 = 1, \quad (\mu_1\mu_2)^4 = 1.$$

Putting

$$\nu_1 = \mu_2\mu_1\mu_2^{-1}, \quad \nu_2 = \mu_1, \quad \nu_3 = \mu_1\mu_2^{-1}\mu_1\mu_2\mu_1,$$

we find that the correspondence

$$\nu_1 \rightarrow (12), \quad \nu_2 \rightarrow (23), \quad \nu_3 \rightarrow (34)$$

induces the isomorphism between $\langle \nu_1, \nu_2, \nu_3 \rangle$ and S_4 . On the other hand, since $\nu_2\nu_1\nu_2\nu_3 = \mu_2^{-1}$, it follows that $G_P = \langle \nu_1, \nu_2, \nu_3 \rangle$.

Lemma 2 *By the G_P -action, the divisors in A_j are transitive ($j = 1, 2, 3, 4, 5, 6$).*

The center of $W(E_7)$ which is isomorphic to \mathbb{Z}_2 acts on the 6-polytope P as the identity transformation. Noting that A_2 consists of four divisors, we obtain the following.

Proposition 1 *The isotropy subgroup of P in $W(E_7)$ is isomorphic to the group $S_4 \times \mathbb{Z}_2$.*

5.2 6-polytopes adjacent to P

To study the 6-polytopes adjacent to P , it is better to treat $P' = s_{34}s_{23}s_{236}s_{16}s_{57} \cdot P$ instead of P . Then P' is surrounded by the divisors in TABLE I below:

TABLE I

A_1	$Y_{12}, Y_{127}, Y_7, Y_{56}, Y_{34}, Y_{567},$
A_2	$Y_{67}, Y_{23}, Y_{45}, Y_1,$
(5) A_3	$Z_{67,345}, Z_{67}, Z_{345}, Z_{45,123}, Z_{12}, Z_{234,567}, Z_{567}, Z_{456}, Z_{17}, Z_{123}, Z_{234}, Z_{23,456},$
A_4	$W_{12,345}, W_{34,567}, W_{127}, W_{567}, W_{56,234}, W_{123,456},$
A_5	$W_{167}, W_{1,23,67}, W_{123},$
A_6	X_0, X_{167}, X_{123}

Lemma 3 *The following hold.*

$$\begin{aligned}
 \mathcal{H}(P') \cap \mathcal{H}(s_{12} \cdot P') &= \{H \in \mathcal{H}(P'); s_{12} \cdot H = H\} \\
 &= \{H \in \mathcal{H}(P'); \overline{H} \cap \overline{Y_{12}} \neq \emptyset\} \\
 \mathcal{H}(P') \cap \mathcal{H}(s_{67} \cdot P') &= \{H \in \mathcal{H}(P'); s_{67} \cdot H = H\} \\
 &= \{H \in \mathcal{H}(P'); \overline{H} \cap \overline{Y_{67}} \neq \emptyset\} \\
 \mathcal{H}(P') \cap \mathcal{H}(s_{13} \cdot P') &= \{H \in \mathcal{H}(P'); s_{13} \cdot H = H\} \\
 &= \{H \in \mathcal{H}(P'); \overline{H} \cap \overline{Z_{123}} \neq \emptyset\} \\
 \mathcal{H}(P') \cap \mathcal{H}(s_{14}s_{23} \cdot P') &= \{H \in \mathcal{H}(P'); s_{14}s_{23} \cdot H = H\} \\
 &= \{H \in \mathcal{H}(P'); \overline{H} \cap \overline{W_{567}} \neq \emptyset\} \\
 \mathcal{H}(P') \cap \mathcal{H}(s_{47}s_{56} \cdot P') &= \{H \in \mathcal{H}(P'); s_{47}s_{56} \cdot H = H\} \\
 &= \{H \in \mathcal{H}(P'); \overline{H} \cap \overline{W_{123}} \neq \emptyset\} \\
 \mathcal{H}(P') \cap \mathcal{H}(us_1 \cdot P') &= \{H \in \mathcal{H}(P'); us_1 \cdot H = H\} \\
 &= \{H \in \mathcal{H}(P'); \overline{H} \cap \overline{X_0} \neq \emptyset\}
 \end{aligned}$$

where $u = (1765432) \in W(E_7)$.

As a consequence of Lemma 2, we find the following.

Theorem 6 *The following statements hold:*

- (i) *The 6-polytopes P' and $s_{12} \cdot P'$ are adjacent to each other and $\overline{P'} \cap s_{12} \cdot \overline{P'} \subset Y_{12}$.*
- (ii) *The 6-polytopes P' and $s_{67} \cdot P'$ are adjacent to each other and $\overline{P'} \cap s_{67} \cdot \overline{P'} \subset Y_{67}$.*
- (iii) *The 6-polytopes P' and $s_{13} \cdot P'$ are adjacent to each other and $\overline{P'} \cap s_{13} \cdot \overline{P'} \subset Z_{123}$.*
- (iv) *The 6-polytopes P' and $s_{14}s_{23} \cdot P'$ are adjacent to each other and $\overline{P'} \cap s_{14}s_{23} \cdot \overline{P'} \subset W_{567}$.*
- (v) *The 6-polytopes P' and $s_{47}s_{56} \cdot P'$ are adjacent to each other and $\overline{P'} \cap s_{47}s_{56} \cdot \overline{P'} \subset W_{123}$.*
- (vi) *The 6-polytopes P' and $us_1 \cdot P'$ are adjacent to each other and $\overline{P'} \cap us_1 \cdot \overline{P'} \subset X_0$.*

This leads to the following.

Theorem 7 *The $W(E_7)$ -action on \mathcal{P}_7 is transitive.*

5.3 Diagrams corresponding to 6-polytopes

Let P' be the 6-polytope introduced in the previous section. From TABLE I, we find that there are 10 divisors in A_1, A_2 corresponding to positive roots of type E_7 below:

TABLE II

A_1	$\gamma_{12}, \gamma_{127}, \gamma_7, \gamma_{56}, \gamma_{34}, \gamma_{567}$
A_2	$\gamma_{67}, \gamma_{23}, \gamma_{45}, \gamma_1$

From these 10 roots, it is possible to construct a diagram similar to Dynkin diagrams. Namely, the diagram in question consists of 10 circles attached with the 10 roots in TABLE II. Two circles are connected by a segment if and only if the roots attached to them are not orthogonal each other. Then we find that there are 12 segments in this diagram.

In the same way, to each 6-polytope in \mathcal{P}_7 , there associates a diagram which is called a *tetradigraph* for the reason that in the case of P' , the 4 circles corresponding to the roots in A_2 of TABLE II are regarded as 4 vertices of a tetrahedron and the 6 circles corresponding to the roots in A_1 of TABLE II are regarded as 6 middle points of the sides of the referred tetrahedron.

To avoid the complexity, we neglect the \pm signs of tetradigraphs. In this manner, we finally obtain a tetra-diagram corresponding to each $P'' \in \mathcal{P}_7$. We denote by \mathcal{TP}_7 the set of tetra-diagrams.

We here note that the classification of the arrangements of 7 lines (l_1, l_2, \dots, l_7) on the real projective plane with conditions I, II, III is accomplished if we determine the decomposition of \mathcal{TP}_7 into S_7 -orbits.

5.4 Tetradigraphs

We have already introduced tetradigraphs in the previous section. In this section, we treat them in the language of root systems systematic manner. (You can find the diagram at the last page of this note.)

Definition 3 Let a_i ($i = 1, 2, 3, 4$), b_{ij} ($1 \leq i < j \leq 4$) be roots of $\Delta(E_7)$. (Assume that $b_{ij} = b_{ji}$ for all i, j .) Then the set

$$A = \{a_i; i = 1, 2, 3, 4\} \cup \{b_{ij}; 1 \leq i < j \leq 4\}$$

is called a *tetrahedral set* if the following conditions hold:

- (i) $\langle a_i, a_j \rangle = 0$ ($i \neq j$).
- (ii) $\langle b_{ij}, b_{i'j'} \rangle = 0$ ($\{i, j\} \neq \{i', j'\}$).
- (iii) $|\langle a_i, b_{jk} \rangle| = 0$ if and only if $i \notin \{j, k\}$.

Example 2 The set

$$U = \{\gamma_{345}, \gamma_{123}, \gamma_{136}, \gamma_{256}, \gamma_{135}, \gamma_{167}, \gamma_{347}, \gamma_{124}, \gamma_{236}, \gamma_{257}\}$$

is a tetrahedral set. In particular, the correspondence

$$\begin{array}{lll} \gamma_{345} \longrightarrow A_1 & \gamma_{135} \longrightarrow B_{12} & \gamma_{124} \longrightarrow B_{23} \\ \gamma_{123} \longrightarrow A_2 & \gamma_{167} \longrightarrow B_{13} & \gamma_{236} \longrightarrow B_{24} \\ \gamma_{146} \longrightarrow A_3 & \gamma_{347} \longrightarrow B_{14} & \gamma_{257} \longrightarrow B_{34} \\ \gamma_{256} \longrightarrow A_4 & & \end{array}$$

induces a tetradiagram for U.

For a tetrahedral set $A = \{a_i\} \cup \{b_{ij}\}$, we put $\tilde{A} = \{\pm a_i\} \cup \{\pm b_{ij}\}$ and call it an extended tetrahedral set. Let A' be also a tetrahedral set. Then A and A' are *equivalent* if and only if $\tilde{A} = \tilde{A}'$. In this case, we confuse a tetradiagram for A and that for A' , for simplicity.

The G_1 -orbit structure will be also important. For this purpose, we will introduce fourteen extended tetrahedral sets in TABLE III. If A is a tetrahedral set whose extended tetrahedral set has the name X in TABLE III, we denote by O_X the S_7 -orbit of \tilde{A} . If B is a tetrahedral set such that $\tilde{B} \in O_X$, we call B a tetrahedral set of type X . Similarly, we call a tetradiagram for B that of type X .

We are going to give a classification of S_7 -orbital structure of extended tetrahedral sets. For this purpose, we define

$$L = \{A, B1, \dots, B5, C1, \dots, C4, D1, \dots, D4\}.$$

Theorem 8 *The set \mathcal{T} of extended tetrahedral sets is decomposed into fourteen S_7 -orbits O_X ($X \in L$).*

It is clear from the definition that \mathcal{T} and \mathcal{TP}_7 are isomorphic. Therefore the classification of S_7 -orbits of \mathcal{T} is accomplished by Theorem 8.

TABLE III

Name	Extended tetrahedral set	Isotropy
A	$\pm\{\gamma_{345}, \gamma_{123}, \gamma_{146}, \gamma_{256}, \gamma_{135}, \gamma_{167}, \gamma_{347}, \gamma_{124}, \gamma_{236}, \gamma_{257}\}$	\mathbb{Z}_3
B1	$\pm\{\gamma_{345}, \gamma_{123}, \gamma_{146}, \gamma_{256}, \gamma_{25}, \gamma_{167}, \gamma_{347}, \gamma_{34}, \gamma_{16}, \gamma_{257}\}$	\mathbb{Z}_3
B2	$\pm\{\gamma_{345}, \gamma_{123}, \gamma_{146}, \gamma_{256}, \gamma_{14}, \gamma_2, \gamma_{57}, \gamma_{124}, \gamma_{236}, \gamma_{257}\}$	1
B3	$\pm\{\gamma_{14}, \gamma_{25}, \gamma_{146}, \gamma_{256}, \gamma_{135}, \gamma_{167}, \gamma_{347}, \gamma_{124}, \gamma_{236}, \gamma_{257}\}$	1
B4	$\pm\{\gamma_{345}, \gamma_{123}, \gamma_{146}, \gamma_{256}, \gamma_6, \gamma_{167}, \gamma_{23}, \gamma_{17}, \gamma_{236}, \gamma_{45}\}$	1
B5	$\pm\{\gamma_2, \gamma_{123}, \gamma_{47}, \gamma_{256}, \gamma_{135}, \gamma_{167}, \gamma_{347}, \gamma_{124}, \gamma_{236}, \gamma_{257}\}$	1
C1	$\pm\{\gamma_{15}, \gamma_{24}, \gamma_{36}, \gamma_7, \gamma_{25}, \gamma_{167}, \gamma_{17}, \gamma_{34}, \gamma_{346}, \gamma_6\}$	1
C2	$\pm\{\gamma_{25}, \gamma_{14}, \gamma_{146}, \gamma_{256}, \gamma_{345}, \gamma_5, \gamma_{27}, \gamma_{34}, \gamma_{16}, \gamma_{257}\}$	1
C3	$\pm\{\gamma_{36}, \gamma_7, \gamma_{15}, \gamma_{24}, \gamma_{246}, \gamma_{167}, \gamma_{347}, \gamma_{356}, \gamma_{145}, \gamma_{257}\}$	\mathbb{Z}_3
C4	$\pm\{\gamma_6, \gamma_{37}, \gamma_{146}, \gamma_{256}, \gamma_{157}, \gamma_{26}, \gamma_{347}, \gamma_{34}, \gamma_{267}, \gamma_{15}\}$	1
D1	$\pm\{\gamma_{56}, \gamma_{123}, \gamma_{13}, \gamma_{256}, \gamma_{136}, \gamma_{157}, \gamma_{57}, \gamma_{124}, \gamma_{24}, \gamma_1\}$	1
D2	$\pm\{\gamma_{47}, \gamma_{123}, \gamma_2, \gamma_{256}, \gamma_{14}, \gamma_{146}, \gamma_{57}, \gamma_6, \gamma_{236}, \gamma_{23}\}$	1
D3	$\pm\{\gamma_{46}, \gamma_{123}, \gamma_{146}, \gamma_{23}, \gamma_{14}, \gamma_{147}, \gamma_{367}, \gamma_7, \gamma_{25}, \gamma_{257}\}$	1
D4	$\pm\{\gamma_{37}, \gamma_6, \gamma_{146}, \gamma_{256}, \gamma_{157}, \gamma_{136}, \gamma_{57}, \gamma_{124}, \gamma_1, \gamma_{24}\}$	1

(Here $\pm\{\gamma_{345}, \gamma_{123}, \gamma_{146}, \dots\}$ is an abbreviation of $\{\pm\gamma_{345}, \pm\gamma_{123}, \pm\gamma_{146}, \dots\}$.)

6 Geometry of eight lines on the real projective plane

I first note that the results of this section are based on the joint works with T. Fukui [5], [6].

6.1 A remarkable configuration of eight lines

From now on, we focus our attention to the case $n = 8$. In addition to conditions I, II, III, we consider the following:

- IV. Let P_j be the point of $\mathbf{P}^2(\mathbf{R})$ dual to l_j ($j = 1, 2, \dots, 8$). Then there is no cubic curve C such that C passes through all the points P_1, \dots, P_8 and that one of the points P_1, \dots, P_8 is a cusp point of C .

The totality of systems of marked 8 lines on $\mathbf{P}^2(\mathbf{R})$ with conditions I, II, III and IV forms a subset of $\mathbf{P}(2, 8)$ which we denote by $\mathbf{P}_0(2, 8)$. Both $\mathbf{P}(2, 8)$ and $\mathbf{P}_0(2, 8)$ are Zariski open subsets of \mathbf{R}^8 . Permutations on the 8 lines l_1, l_2, \dots, l_8 induce a biregular S_8 -action on $\mathbf{P}(2, 8)$ (and also that on $\mathbf{P}_0(2, 8)$). Let \mathcal{P}_8 be the set of connected components of $\mathbf{P}_0(2, 8)$. The $W(E_8)$ -action on $\mathbf{P}_0(2, 8)$ naturally induces that on \mathcal{P}_8 . Then it is interesting to attack the problem below (cf. Problem 1):

Problem 2 Determine the $W(E_8)$ -orbital structure of \mathcal{P}_8 .

The first step to attack Problem 2 is to find out a $W(E_8)$ -orbit \mathcal{O} of \mathcal{P}_8 and parametrize elements of \mathcal{O} in terms of graphs attached with roots of Δ . For this purpose, we first treat the following problem.

Problem 3 Find out such a system of marked 8 lines $(l_j)_{1 \leq j \leq 8}$ that there is no hexagon for any system of marked six lines constructed from $(l_j)_{1 \leq j \leq 8}$ by taking off two lines.

For a moment, we identify \mathbf{R}^2 with an open dense subset of $\mathbf{P}^2(\mathbf{R})$ by the map $(u, v) \mapsto (1 : u : v)$, where (u, v) is a linear coordinate of \mathbf{R}^2 . We consider the 3×8 matrix

$$(6) \quad X_0 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & -27/10 & -9 & 3/5 & -17/10 & -3/2 \\ 1 & 0 & 1 & 12 & 4 & 9/5 & 53/10 & 21/10 \end{pmatrix}.$$

By taking the entries of the vector $(\xi \eta \zeta) \cdot X_0 = (f_1 \dots f_8)$, we obtain a system of marked 8 lines $(l_j^0)_{1 \leq j \leq 8}$, where

$$(7) \quad l_j^0 : f_j = 0 \quad (1 \leq j \leq 8).$$

By the 8 lines (6), we obtain ten triangles (T_k) ($k = 1, 2, \dots, 10$) surrounded by the three lines given below (you can find the arrangement of the 8 lines at the last page of this note.):

(T_1)	$l_1^0 l_2^0 l_3^0$	r_{123}
(T_2)	$l_1^0 l_4^0 l_6^0$	r_{146}
(T_3)	$l_1^0 l_5^0 l_8^0$	r_{158}
(T_4)	$l_1^0 l_6^0 l_7^0$	r_{167}
(T_5)	$l_2^0 l_5^0 l_7^0$	r_{257}
(T_6)	$l_2^0 l_6^0 l_8^0$	r_{268}
(T_7)	$l_3^0 l_4^0 l_5^0$	r_{345}
(T_8)	$l_3^0 l_7^0 l_8^0$	r_{378}
(T_9)	$l_4^0 l_7^0 l_8^0$	r_{478}
(T_{10})	$l_5^0 l_6^0 l_8^0$	r_{568}

It is easy to see that the system of marked 8 lines (6) gives an answer to Problem 2, namely, that there are no hexagon, heptagon, octagon for $(l_j^0)_{1 \leq j \leq 8}$. In the sequel, we denote by AE_8 the system (l_j^0) . Let C_{AE_8} be the connected component of \mathcal{P}_8 containing AE_8 .

6.2 8LC sets and 8LC diagrams for the root system of type E_8

In this section, we give an interpretation of the system of marked 8 lines AE_8 in the previous section in terms of the root system Δ . For this purpose, we first introduce the notions of 8LC sets and 8LC diagrams for the root system of type E_8 .

Definition 4 Let a_i ($i = 1, 2, \dots, 8$) and b_1, b_2 be roots of Δ . Then the set

$$(8) \quad A = \{a_i; i = 1, 2, \dots, 8\} \cup \{b_1, b_2\}$$

is called an 8LC (= 8 lines configuration) set if the following conditions hold:

- (i) $\langle a_i, a_j \rangle \neq 0$ if and only if $i - j \equiv 0$ or $\pm 1 \pmod{8}$.
- (ii) $\langle b_1, b_2 \rangle = 0$.
- (iii.1) $\langle a_i, b_1 \rangle \neq 0$ if and only if $i = 1$.
- (iii.2) $\langle a_i, b_2 \rangle \neq 0$ if and only if $i = 5$.

We would like to visualize each 8LC set by associating a diagram (similar to a Dynkin diagram). Let $A = \{a_i; i = 1, \dots, 8\} \cup \{b_1, b_2\}$ be an 8LC set. Then an 8LC diagram for A is a figure consisting of ten circles attached with roots of A and segments constructed in the figure at the last page of this note. An 8LC diagram for A gives a complete information of orthogonality condition of elements of A . Namely, let c_1, c_2 ($c_1 \neq c_2$) be roots of A . The $\langle c_1, c_2 \rangle \neq 0$ if and only if the circles corresponding to c_1, c_2 are connected by a segment.

For an 8LC set $A = \{a_i; i = 1, \dots, 8\} \cup \{b_1, b_2\}$, we put

$$(9) \quad \bar{A} = \{\pm a_i; i = 1, \dots, 8\} \cup \{\pm b_1, \pm b_2\}$$

and call it an extended 8LC set. Let A' be also an 8LC set. Then A and A' are equivalent if and only if $\bar{A} = \bar{A}'$. In this case, we always identify an 8LC diagram for A and that for A' for simplicity.

Example 3 The set $U = \{r_{123}, r_{146}, r_{158}, r_{167}, r_{257}, r_{268}, r_{345}, r_{378}, r_{478}, r_{568}\}$ is an 8LC set. In particular, the correspondence

$$\begin{array}{cccc} r_{568} & \longrightarrow & a_1 & r_{123} & \longrightarrow & a_2 & r_{478} & \longrightarrow & a_3 & r_{378} & \longrightarrow & a_4 \\ r_{146} & \longrightarrow & a_5 & r_{167} & \longrightarrow & a_6 & r_{345} & \longrightarrow & a_7 & r_{268} & \longrightarrow & a_8 \\ r_{158} & \longrightarrow & b_1 & r_{257} & \longrightarrow & b_2 & & & & & & & \end{array}$$

induces an 8LC diagram for U .

Put

$$g_1 = s_{16}s_{38}s_{57}t_{24}, \quad g_2 = s_{18}s_{27}s_{45}t_{36}, \quad g_3 = s_{23}s_{123}s_{45}s_{145}s_{67}s_{167}t_{8}t_{18}.$$

Then g_1, g_2, g_3 generate the isotropy subgroup $\text{Iso}_{W(E_8)}(\tilde{U})$ of \tilde{U} in $W(E_8)$, where \tilde{U} is the extended 8LC set of U . In particular, $\text{Iso}_{W(E_8)}(\tilde{U}) \simeq (\mathbb{Z}_2)^3$. Note that g_3 is the generator of the center of $W(E_8)$.

The following lemma is shown by a direct computation.

Lemma 4 If an 8LC set A contains $\{r_{12}, r_{123}, r_{23}, r_{34}, r_{45}, r_{56}, r_{67}, r_{78}\}$ (these become simple roots of Δ), then \tilde{A} coincides with

$$\{\pm r_{12}, \pm r_{123}, \pm r_{23}, \pm r_{34}, \pm r_{45}, \pm r_{56}, \pm r_{67}, \pm r_{78}, \pm t_{18}, \pm t_8\}.$$

In virtue of this lemma, the classification of 8LC sets is essentially reduced to that of fundamental systems of roots of Δ , which is well-known, and we get

Proposition 2 Let A and A' be 8LC sets. Then there exists $w \in W(E_8)$ such that $w \cdot \tilde{A} = \tilde{A}'$.

Conjecture 1 Retain the notation in Example 3. Then $g_j \cdot C_{AE_8} = C_{AE_8}$ ($j = 1, 2, 3$). Moreover, $\{g \in W(E_8); g \cdot C_{AE_8} = C_{AE_8}\}$ coincides with $\text{Iso}_{W(E_8)}(\tilde{U})$.

There are 14 S_7 -orbits of \mathcal{P}_7 which are called of types A, B1, B2, B3, B4, B5, C1, C2, C3, C4, D1, D2, D3, D4 as explained before. We generated 1629 simple 2-arrangements of 8 lines from the 14 simple 2-arrangements of 7 lines by experimental computation. We classified those arrangements into 91 different kinds. For the details, see [6].

We end this section by noting the difference between systems of 8 lines with conditions I, II and those with conditions I-IV. Two systems of 8 lines with conditions I, II are equivalent provided there exists a one-to-one incidence-preserving correspondence between their polygons. Then any two systems of 8 lines having an octagon are equivalent but the set of systems of 8 lines having an octagon can be decomposed into at least 15 different sets of systems with conditions I-IV (cf. [5]).

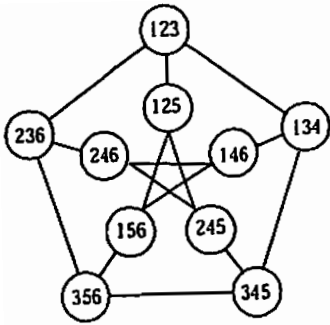
References

- [1] N. Bourbaki: *Groupes et Algèbres de Lie*. Chaps. 4, 5, 6, Herman, Paris (1968).
- [2] L. D. Cummings: Hexagonal systems of seven lines in a plane. *Bulletin of the American Math. Soc.* **38** (1932), 105-110.
- [3] L. D. Cummings: Heptagonal systems of eight lines in a plane. *Bulletin of the American Math. Soc.* **38** (1932), 700-702.
- [4] I. Dolgachev and D. Ortland: *Point sets in projective spaces and theta functions*. *Astérisque* **165** (1988).
- [5] T. Fukui and J. Sekiguchi: A remark on labelled 8 lines on the real projective plane. *Reports of Faculty of Science, Himeji Inst. Tech.* **8** (1997), 1-11.
- [6] T. Fukui and J. Sekiguchi: Eight lines arrangements on the real projective plane and the root system of type E_8 . *Proc. Third Asian Tech. Conference in Math.*, August 24-28, 1998, 377-388.
- [7] B. Grünbaum: *Convex Polytopes*. Interscience, 1967.
- [8] Yu. Manin: *Cubic Forms*. North-Holland (1974).
- [9] I. Naruki: Cross ratio variety as a moduli space of cubic surfaces. *Proc. London Math. Soc.* **45** (1982), 1-30.
- [10] I. Naruki and J. Sekiguchi: A modification of Cayley's family of cubic surfaces and birational action of $W(E_6)$ over it. *Proc. Japan Acad.* **56** Ser. A (1980), 122-125.
- [11] J. Sekiguchi: The versal deformation of the E_6 -singularity and a family of cubic surfaces. *J. Math. Soc. Japan*, **46** (1994), 355-383.
- [12] J. Sekiguchi: Cross ratio varieties for root systems. *Kyushu J. Math.*, **48** (1994), 123-168.
- [13] J. Sekiguchi: Configurations of seven lines on the real projective plane and the root system of type E_7 . *J. Math. Soc. Japan*, **51**(1999), 987-1013.
- [14] J. Sekiguchi: Cross ratio varieties for root systems, II. *Kyushu J. Math.*, **54** (2000), 7-37.
- [15] J. Sekiguchi: Geometry of 7 lines on the real projective plane and the root system of type E_7 . *RIMS Kokyuroku*, **986**, 1-8.
- [16] J. Sekiguchi and T. Tanabata: Tetradiagrams for the root system of type E_7 and its application. *Reports of Faculty of Science, Himeji Inst. Tech.* **7** (1996), 1-10.
- [17] J. Sekiguchi and M. Yoshida: $W(E_6)$ -action on the configuration space of 6 points of the real projective plane. *Kyushu J. Math.* **51** (1997), 297-354.
- [18] T. Shioda: Construction of elliptic curves with high rank via the invariants of the Weyl groups. *J. Math. Soc. Japan*, **43** (1991), 673-719.
- [19] T. Shioda: Plane quartics and Mordell-Weil lattices of type E_7 . *Comment. Math. Univ. St. Pauli*, **42** (1993), 61-79.

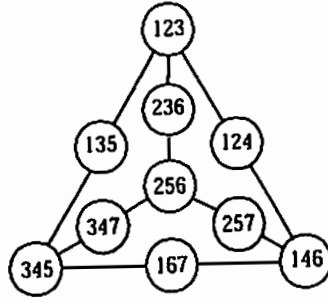
- [20] T. Shioda: A uniform construction of the root lattices E_6, E_7, E_8 and their dual lattices. *Proc. Japan Acad.* 71 Ser. A (1995), 140-143.
- [21] J. Stienstra and M. Yoshida: The arrangements of six colored lines on the real projective plane. Preprint.
- [22] T. Terada: Fonction hypergéométriques F_1 et fonctions automorphes I. *J. Math. Soc. Japan* 35 (1983), 451-475.
- [23] M. Yoshida: Democratic compactification of the configuration spaces of point sets on the real projective line. *Kyushu J. Math.* 50 (1996), 493-512.
- [24] H. S. White: The plane figure of seven lines. *Bulletin of the American Math. Soc.* 38 (1932), 59-65.

Jiro Sekiguchi
Department of Mathematics
Tokyo University of Agriculture and Technology
Koganei, Tokyo 184-8588
JAPAN
e-mail address: sekiguti@cc.tuat.ac.jp

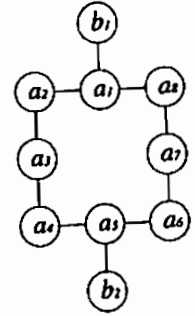
184-8588
小金井市中町 2-24-16
東京農工大学工学部
数学教室
関口次郎



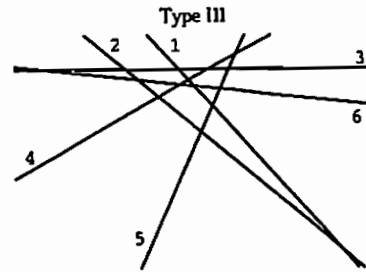
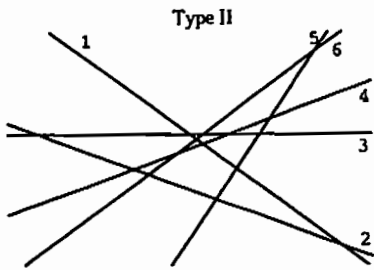
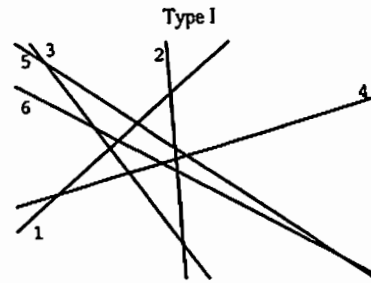
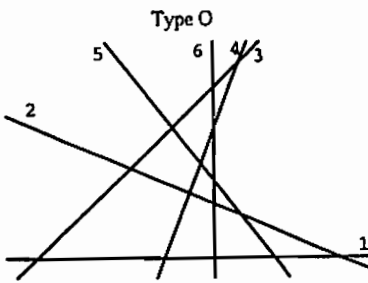
Pent - diagram



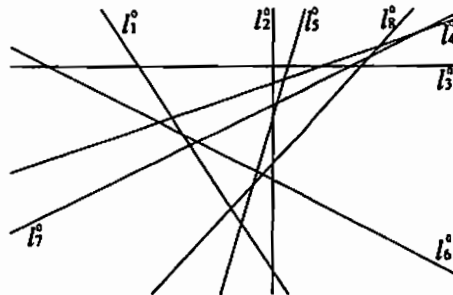
Tetra diagram



8LC diagram



Four types of systems of six lines



The 8 lines configuration (AE8) of X_0

Parabolic Burnside rings and symmetric functions

小田 文仁 (ODA Fumihito) *

1 はじめに

G は有限群, \mathfrak{X} はある条件 $(C)_p$ を満たす G の部分群の族とする. 一般バーンサイド環 $\Omega(G, \mathfrak{X})$ は Yoshida により研究が始められた [10]. 有限群 G として対称群, 族 \mathfrak{X} としてその Young 部分群全体を考えたとき, 一般バーンサイド環 $\Omega(G, \mathfrak{X})$, と G の指標環との間に環同型が存在することの証明が [10] にある. この同型を用いて parabolic Burnside rings (一般バーンサイド環) から対称関数環 Λ を構成することが本稿の目的である. 一般バーンサイド環における積, 誘導写像, 制限写像が Λ における積を定義することが本質的な事実である.

S_n は n 次の対称群, \mathfrak{Y}_n は S_n の Young 部分群全体からなる族とする. A_{n-1} 型の有限 Coxeter 群 W_{n-1} の parabolic Burnside ring $\Pi(W_{n-1})$ は一般バーンサイド環 $\Omega(S_n, \mathfrak{Y}_n)$ である. A 型の parabolic Burnside rings の次数付き環を $\Omega = \bigoplus_{n=0}^{\infty} \Omega(S_n, \mathfrak{Y}_n)$ とする. Λ_n は次数 n のすべての対称関数のつくる \mathbb{Z} -加群とし, $\Lambda = \bigoplus_{n=0}^{\infty} \Lambda_n$ を対称関数環とする. 次の結果が主定理である:

(4.4) Theorem. *The two graded rings Ω and Λ are isomorphic.*

Λ が対称群の表現環の直和に同型であることは良く知られている [6], [2], [3], [8]. この環が Burnside ring の部分環から構成されるということはあまり良く知られた事実ではなかったようである.

2 The generalized Burnside ring

(2.1) Burnside homomorphism G は有限群, G の部分群の族 \mathfrak{X} は条件

$$\text{if } H \in \mathfrak{X}, \text{ then } {}^g H \in \mathfrak{X}, \text{ where } {}^g H = gHg^{-1} \text{ and } g \in G$$

を満たすものとする. 有限集合 X に対し $|X|$ は X に含まれる要素の個数を表す. $\Omega(G, \mathfrak{X})$ は, 自由可換群で基底 $\{|[G/H]|(H) \in C(G), H \in \mathfrak{X}\}$ を持つものとする. ここで, $C(G)$ は G の部分群の共役類の族, (H) は H を含む G の部分群の G -共役類である. $C(\mathfrak{X})$

*富山工業高等専門学校一般科目, oda@toyama-nct.ac.jp

は \mathfrak{X} に含まれる部分群の G -共役類の族とする。有理整数環の $|C(\mathfrak{X})|$ 個の直積の環を $\tilde{\Omega}(G, \mathfrak{X}) = \prod_{(S) \in C(\mathfrak{X})} \mathbb{Z}$ で表し、 \mathfrak{X} に関する *ghost ring* と呼ぶ。任意の $S \in \mathfrak{X}$ に対し写像 $\varphi_S : \Omega(G, \mathfrak{X}) \rightarrow \mathbb{Z}$, $[X] \mapsto |X^S|$ を定める。ここで、 X^S は S -固定点の集合である。このように得られる加法群としての準同型 $\varphi := (\varphi_S)_{(S)} : \Omega(G, \mathfrak{X}) \rightarrow \tilde{\Omega}(G, \mathfrak{X})$, $x \mapsto (\varphi_S(x))_{(S)}$, を \mathfrak{X} に関する *Burnside homomorphism* と呼ぶ。ここで、 $(S) \in C(\mathfrak{X})$ とする。

(2.2) **The generalized Burnside rings.** R を可換環とする。 R -加群 $R \otimes_{\mathbb{Z}} \Omega(G, \mathfrak{X})$ は Burnside 準同型 $1 \otimes \varphi : R \otimes_{\mathbb{Z}} \Omega(G, \mathfrak{X}) \rightarrow R \otimes_{\mathbb{Z}} \tilde{\Omega}(G, \mathfrak{X})$ が入射的環準同型になるように単位元を持つ環の構造が定義されるとき *generalized Burnside ring* と呼ばれる。

(2.3) **The condition $(C)_p$.** 加群 $\Omega(G, \mathfrak{X})$ が *generalized Burnside ring* になるための \mathfrak{X} の条件について述べる。 \mathfrak{X} が共通部分をとるという操作について閉じていて、 G を含んでいるならば $\Omega(G, \mathfrak{X})$ は Burnside ring $\Omega(G)$ の部分環になることに注意する。 G の部分群 H に対して、 $\overline{H} = \cap \{S \in \mathfrak{X} | H \subseteq S\}$ を定める。もし、 H を含むような \mathfrak{X} の元が存在しないといには $\overline{H} = G$ とする。 $\mathbb{Z}_{(p)}$ は \mathbb{Z} の素数 p による局所環とする： $\mathbb{Z}_{(p)} = \{a/b | a \in \mathbb{Z}, b \in \mathbb{Z} - p\mathbb{Z}\} \subseteq \mathbb{Q}$ 。自由可換群 A に対して $A_{(p)} = \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} A$ と書く。次の条件を考える：

$$(C)_p \quad gS \in (WS)_p, S \in \mathfrak{X} \implies \overline{(g)}S \in \mathfrak{X},$$

ここで、 $(WS)_p$ は $WS := N_G(S)/S$ の Sylow p -部分群である。 $p = \infty$ に対しては、条件 $(C)_p$ を次のように読みかえる：

$$(C)_\infty \quad gS \in WS, S \in \mathfrak{X} \implies \overline{(g)}S \in \mathfrak{X}.$$

条件 $(C)_p$ と $(C)_\infty$ の関係について注する (see [10]).

(2.4) **Lemma.** The condition $(C)_\infty$ is equivalent to the conditions $(C)_p$ for all prime p .

この節の結果を述べるために次の命題を準備する。Yoshida は条件 $(C)_p$ のもとでの *generalized Burnside ring* の存在性と一意性を示した：

(2.5) **Theorem.** [Yoshida] (a) Under the condition $(C)_p$, $\Omega(G, \mathfrak{X})_{(p)}$ has a unique ring structure such that $\varphi^{(p)} : \Omega(G, \mathfrak{X})_{(p)} \rightarrow \tilde{\Omega}(G, \mathfrak{X})_{(p)}$ is a ring homomorphism.

(b) In particular, under the condition $(C)_\infty$, $\Omega(G, \mathfrak{X})$ has a unique ring structure such that $\varphi : \Omega(G, \mathfrak{X}) \rightarrow \tilde{\Omega}(G, \mathfrak{X})$ is a ring homomorphism. Furthermore, for a prime p , the two ring structures on $\mathbb{Z}_{(p)} \otimes \Omega(G, \mathfrak{X}) = \Omega(G, \mathfrak{X})_{(p)}$ defined by (a) and (b) coincide.

(2.6) **Inductions and restrictions.** 任意の有限群 H に対して、 $\text{Sub}(H)$ で H のすべての部分群のつくる束を表す。このとき群 H はこの部分群束に共役で作用する。 H の部分群の族 \mathfrak{H} が H -共役について閉じているならば、 $\mathfrak{H} \subseteq \text{Sub}(H)$ と書く。この節を通じて \mathfrak{X} はそのような G の部分群の族、つまり、 $\mathfrak{X} \subseteq \text{Sub}(G)$ とする。族 $\cap \mathfrak{X} \subseteq_G \text{Sub}(G)$ を $\cap \mathfrak{X} = \{S_1 \cap \dots \cap S_n | n \geq 0, S_i \in \mathfrak{X}\}$ で定義する。この族は G を含む。さらに、 p は素数、 0 または、 ∞ を表すものとする。任意の $H \in \cap \mathfrak{X}$ に対して、族 \mathfrak{X}_H を $\mathfrak{X}_H =$

$\mathfrak{X} \cap \text{Sub}(H) = \{T \in \mathfrak{X} \mid T \subseteq H\}$ で定める. \mathfrak{X} は p に対して条件 $(C)_p$ を満たすものとする. [10] の Corollary 6.6 により, 任意の対 $H \leq K \in \cap \mathfrak{X}$ に対して次のような写像 (制限写像と誘導写像) が存在する:

$$\begin{aligned} \text{res}_H^K &: \Omega(K, \mathfrak{X}_K)_{(p)} \longrightarrow \Omega(H, \mathfrak{X}_H)_{(p)} \\ &: [K/T] \longmapsto \sum_{g \in [H \backslash K/T]} [H/H \cap {}^g T] \\ \text{ind}_H^K &: \Omega(H, \mathfrak{X}_H)_{(p)} \longrightarrow \Omega(K, \mathfrak{X}_K)_{(p)} \\ &: [H/T] \longmapsto [K/T]. \end{aligned}$$

さらに, $H \in \cap \mathfrak{X}$ と $g \in G$ に対して, 共役写像は

$$\begin{aligned} \text{con}_H^g &: \Omega(H, \mathfrak{X}_H)_{(p)} \longrightarrow \Omega({}^g H, \mathfrak{X}_{{}^g H})_{(p)} \\ &: [H/T] \longmapsto [{}^g H/{}^g T], \end{aligned}$$

により定義される. ここで, ${}^g H = gHg^{-1}$ である.

(2.7) **Parabolic Burnside rings.** 有限 Coxeter 群の parabolic Burnside ring の定義について述べる. (W, S) 有限 Coxeter system とする. 任意の部分集合 $J \subseteq S$ と部分群 $W_J = \langle J \rangle \subseteq W$ を考える. このとき, W_J は W の *parabolic subgroup* と呼ばれる. W -set X が *parabolic W -set* であるとは, Burnside ring $\Omega(W)$ の中で $[X] = [W/W_J]$ for some $J \subseteq S$ と表されることである. 二つの parabolic W -sets の積が $\Omega(W)$ の中で transitive parabolic W -sets に分解されることはよく知られている (see [1], [4]). 集合 $\{[W/W_J] \mid J \subseteq S\}$ は $\Omega(W)$ の部分環 $\Pi(W)$ の \mathbb{Z} -basis となる. この, $\Pi(W)$ を W あるいは (W, S) の *parabolic Burnside ring* と呼ぶ (see [9], [1], [4]).

(2.8) **Lemma.** Let \mathfrak{X} be the family of all parabolic subgroups of W . Then the parabolic Burnside ring $\Pi(W)$ is a generalized Burnside ring of W with respect to \mathfrak{X} .

PROOF. Let $\Omega(W, \mathfrak{X})$ be the \mathbb{Z} -module of W with respect to \mathfrak{X} . Since \mathfrak{X} is closed under intersection, the condition $(C)_\infty$ holds, and so $\Omega(W, \mathfrak{X})$ is a generalized Burnside ring by Theorem 2.5. Moreover, $\Omega(W, \mathfrak{X})$ is a subring of $\Omega(W)$ because W is a parabolic. We conclude that $\Pi(W)$ and $\Omega(W, \mathfrak{X})$ coincide. \square

本稿を通して A_{n-1} 型の parabolic Burnside ring $\Pi(W_{n-1})$ のみを考える. これは, 対称群 S_n のすべての Young 部分群 \mathfrak{Y}_n についての generalized Burnside ring $\Omega(S_n, \mathfrak{Y}_n)$ と同型である. そこで, $\Pi(W_{n-1})$ と $\Omega(S_n, \mathfrak{Y}_n)$ を同一視する.

G と H を有限群とする. G, H の任意の部分群の族 $\mathfrak{X}, \mathfrak{Y}$ に対し $\mathfrak{X} \times \mathfrak{Y} = \{S \times T \mid S \in \mathfrak{X}, T \in \mathfrak{Y}\}$ を定める.

(2.9) **Lemma.** Let G and H be finite groups. Let \mathfrak{X} and \mathfrak{Y} be families of G and H respectively, where \mathfrak{X} and \mathfrak{Y} satisfy the condition $(C)_p$. Then $\Omega(G \times H, \mathfrak{X} \times \mathfrak{Y})$ is a generalized Burnside ring.

PROOF. It is to verify that the family $\mathfrak{X} \times \mathfrak{Y}$ satisfies the condition $(C)_p$. By Theorem (2.5), $\Omega(G \times H, \mathfrak{X} \times \mathfrak{Y})$ is a generalized Burnside ring of $G \times H$ with respect to $\mathfrak{X} \times \mathfrak{Y}$. \square

(2.10) The graded ring Ω . $\Omega_n = \Omega(W_n, \mathfrak{Y}_n)$ を A_{n-1} 型の parabolic Burnside ring とする. ここで, \mathfrak{Y}_n は Coxeter 群 (symmetric group S_n) のすべての parabolic subgroups (resp. Young subgroups) の族とする. 次数付き環 Ω を次の命題のように定義する.

(2.11) Proposition. Let $\Omega = \bigoplus_{n=0}^{\infty} \Omega_n$, where $\Omega_0 = \mathbb{Z}$. Then Ω has a graded ring structure.

PROOF. By Lemma 2.8, $\Omega(S_n \times S_m, \mathfrak{Y}_n \times \mathfrak{Y}_m)$ is a generalized Burnside ring of $S_n \times S_m$ with respect to $\mathfrak{Y}_n \times \mathfrak{Y}_m$. Since $\mathfrak{Y}_n \times \mathfrak{Y}_m = (\mathfrak{Y}_{n+m})_{S_n \times S_m}$, we can consider the induction $\text{ind}_{S_n \times S_m}^{S_{n+m}}$ from $\Omega(S_n \times S_m, \mathfrak{Y}_n \times \mathfrak{Y}_m)$ to Ω_{n+m} . We define the product $\Omega_n \times \Omega_m \rightarrow \Omega_{n+m}$, denoted $*$, by the formula

$$[S_n/S] * [S_m/T] = \text{ind}_{S_n \times S_m}^{S_{n+m}} ([S_n \times S_m/S] \cdot [(S_n \times S_m)/T]), \quad (2.11.1)$$

where \cdot is product in $\Omega(S_n \times S_m, \mathfrak{Y}_n \times \mathfrak{Y}_m)$. It is straightforward to verify that this product is well defined, and makes Ω into a commutative, associative, graded ring with unit. \square

3 The ring of symmetric functions

[6], [2] に従って対称関数の理論について述べる.

(3.1) Symmetric polynomials. m を正整数, $f(x) = f(x_1, \dots, x_m)$ を m 変数の多項式とする. 分割 $\lambda = (\lambda_1 \geq \dots \geq \lambda_k)$ に対して多項式

$$h_\lambda(x) = h_{\lambda_1}(x) \cdot \dots \cdot h_{\lambda_k}(x), \quad (3.1.1)$$

が得られる. ここで, $h_p(x)$ は p^{th} complete symmetric polynomials in variables x_1, \dots, x_m である. さらに, 主定理の証明のため, power sums を準備する. p_λ を Newton power sums

$$p_\lambda(x) = p_{\lambda_1}(x) \cdot \dots \cdot p_{\lambda_k}(x), \quad p_r(x) = x_1^r + \dots + x_m^r. \quad (3.1.2)$$

とする. 整数 $z(\lambda)$ を公式

$$z(\lambda) = \prod_r r^{m_r} m_r! \quad (3.1.3)$$

で定める. ここで, m_r は λ の中の r の重複度とする. 形式的べき級数を計算することにより, 正整数 m, n に対して次の等式を得る (see Lemma 6.1 in [2]).

$$h_n(x_1, \dots, x_m) = \sum_{\lambda \vdash n} \frac{1}{z(\lambda)} p_\lambda(x_1, \dots, x_m). \quad (3.1.4)$$

(3.2) **The ring of symmetric functions.** n 次の対称関数とは、任意の正整数 m に対して、 m 変数の n 対称多項式 $p(x_1, \dots, x_m)$ とする。 Λ_n は n 次対称関数全体がつくる、 \mathbb{Z} -加法群とする。 Complete symmetric polynomials h_λ は Λ_n の \mathbb{Z} -basis となる。ただし、 λ は n のすべての分割を動く。また、power sums は $\mathbb{Q} \otimes \Lambda_n$ の \mathbb{Q} -basis となる。

$$\Lambda = \bigoplus_{n=0}^{\infty} \Lambda_n, \quad (3.2.1)$$

を対称関数の次数付き環とする。環 Λ は変数 h_1, h_2, \dots の多項式の環と同一視される。この同一視は有限のレベルで証明される。

(3.3) **The Grothendieck ring of representations.** R_n を対称群 S_n の \mathbb{C} 上の表現の直和に関する Grothendieck group とする。 $R = \bigoplus_{n=0}^{\infty} R_n$ を S_n の表現の Grothendieck ring とする。ただし、積は公式

$$[V_n] \circ [U_m] = [\text{Ind}_{S_n \times S_m}^{S_{n+m}}(V_n \otimes U_m)] \quad (3.3.1)$$

で与えられるものとする。ここで、 $[V_n]$ と $[U_m]$ はそれぞれ R_n と R_m 中の同値類とする。この積が well-defined であること、また、 R が可換、結合的で単位元を持つ次数付き環であることが証明されることは良く知られている。

(3.4) **The homomorphisms φ and ψ .** n の分割 λ に対し M^λ を λ に対応する Young 部分群 Y_λ の自明な表現の S_n への誘導表現とする:

$$M_n^\lambda = \text{Ind}_{Y_\lambda}^{S_n}(1) = \mathbb{C}[S_n] \otimes_{Y_\lambda} \mathbb{C}. \quad (3.4.1)$$

Complete symmetric polynomials h_λ が対称関数環 Λ の基底を張るので、加法群としての準同型 $\varphi: \Lambda \rightarrow R$ が公式

$$\varphi(h_\lambda) = [M_n^\lambda]. \quad (3.4.2)$$

により定義される。

(3.5) **Theorem.** The homomorphism φ is a homomorphism of graded rings, and is an isomorphism of Λ with R .

PROOF. We refer to reader 7.3 in [2] for the details. □

R から Λ への逆写像 ψ が公式

$$\psi([V]) = \sum_{\mu \vdash n} \frac{1}{z(\mu)} \chi_V(C(\mu)) p_\mu, \quad (3.5.1)$$

により定義される。ここで、 χ_V は表現 V の指標、 $C(\mu)$ は μ に対応する共役類とする (see 7.3 in [2]).

4 The graded rings Ω and R

(4.1) The homomorphism π . 加法群としての準同型 $\pi_n : \Omega_n \rightarrow R_n$ を公式

$$\pi_n(S_n/Y_\lambda) = [M_n^\lambda]. \quad (4.1.1)$$

により定める.

(4.2) Lemma. The homomorphism π_n is an isomorphism of rings.

PROOF. We refer the reader to [5] or [10] for the details. \square

加法群としての準同型 π を $\pi = (\pi_n)_n : \Omega \rightarrow R$, と定義する. ここで, n は非負整数全体を動く.

(4.3) Theorem. The homomorphism π is a homomorphism of graded rings, and is an isomorphism of Ω with R .

PROOF. Since $\pi_n(\Omega_n) = R_n$ by Lemma 4.2, π is a graded additive homomorphism. In order to complete the proof that π is an algebra homomorphism. Let $[S_n/Y_\lambda] \in \Omega_n$ and $[S_m/Y_\mu] \in \Omega_m$, where λ and μ are partitions of n and m respectively. Consider the definition of product in Ω and the isomorphisms on the theory of G -sets

$$\begin{aligned} [S_n/Y_\lambda] * [S_m/Y_\mu] &= \text{ind}_{S_n \times S_m}^{S_n+m} ((S_n \times S_m)/Y_\lambda \cdot [(S_n \times S_m)/Y_\mu]) \\ &= \text{ind}_{S_n \times S_m}^{S_n+m} \left(\sum_{s \in [Y_\lambda \setminus S_n \times S_m / Y_\mu]} [(S_n \times S_m)/Y_\mu \cap {}^s Y_\lambda] \right) \\ &= \sum_{s \in [Y_\lambda \setminus S_n \times S_m / Y_\mu]} \text{ind}_{S_n \times S_m}^{S_n+m} ((S_n \times S_m)/Y_\mu \cap {}^s Y_\lambda) \\ &= \sum_{s \in [Y_\lambda \setminus S_n \times S_m / Y_\mu]} [S_{n+m}/Y_\mu \cap {}^s Y_\lambda]. \end{aligned}$$

So we obtain

$$\pi([S_n/Y_\lambda] * [S_m/Y_\mu]) = \bigoplus_{s \in [Y_\lambda \setminus S_n \times S_m / Y_\mu]} M_{n+m}^{\lambda_s}, \quad (4.3.1)$$

where λ_s 's are partitions of $n + m$ corresponding the Young subgroups $Y_\mu \cap {}^s Y_\lambda$ of S_{n+m} . On the other hand, by the formula (3.3.1) and the Mackey's tensor product theorem, we

deduce that

$$\begin{aligned}
& \pi([S_n/Y_\lambda]) \circ \pi([S_m/Y_\mu]) \\
&= [\text{Ind}_{Y_\lambda}^{S_n}(1)] \circ [\text{Ind}_{Y_\mu}^{S_m}(1)] \\
&= \text{Ind}_{S_n \times S_m}^{S_n+m} \left(\text{Ind}_{Y_\lambda}^{S_n \times S_m}(1) \otimes \text{Ind}_{Y_\mu}^{S_n \times S_m}(1) \right) \\
&= \text{Ind}_{S_n \times S_m}^{S_n+m} \left(\bigoplus_{t \in [Y_\mu \setminus S_n \times S_m / Y_\lambda]} \text{Ind}_{Y_\mu \cap^t Y_\lambda}^{S_n \times S_m} \left(\text{Res}_{Y_\mu \cap^t Y_\lambda}^{t Y_\lambda}(1) \otimes \text{Res}_{Y_\mu \cap^t Y_\lambda}^{Y_\mu}(1) \right) \right) \\
&= \bigoplus_{t \in [Y_\mu \setminus S_n \times S_m / Y_\lambda]} \text{Ind}_{Y_\mu \cap^t Y_\lambda}^{S_n+m}(1).
\end{aligned}$$

We verify

$$\pi([S_n/Y_\lambda] * [S_m/Y_\mu]) = \pi([S_n/Y_\lambda]) \circ \pi([S_m/Y_\mu]) \quad (4.3.2)$$

by the formula (3.4.1) and (4.3.1). This complete the proof. \square

以下が主定理である.

(4.4) Theorem. Let $\Omega = \bigoplus_{n=0}^{\infty} \Omega_n$ be the graded ring of parabolic Burnside rings of type A and Λ the ring of symmetric functions. Then two graded rings Ω and Λ are isomorphic.

PROOF. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be the Grothendieck ring of the representations of the symmetric groups. Using Theorem 4.3 we have an isomorphism of graded rings

$$\begin{aligned}
\pi : \quad \Omega & \longrightarrow R \\
& : ([S_n/Y_\lambda])_{(n)} \longmapsto ([M_n^\lambda])_{(n)}.
\end{aligned}$$

By the proof of Theorem 7.3 in [2], we can consider the inverse map ψ of φ which is given by the formula (3.5.1) as follows :

$$\begin{aligned}
\psi : \quad R & \longrightarrow \Lambda \\
& : ([V_n])_{(n)} \longmapsto \left(\sum_{\mu \vdash n} \frac{1}{z(\lambda)} \chi_{V_n}(C(\mu)) p_\mu \right)_{(n)}
\end{aligned}$$

Since the composite $\psi\pi\pi^{-1}\varphi$ is the identity of Λ , the theorem is now fully proved. \square

Acknowledgement 筆者は、 Ω と Λ に関する有益な御助言をいただいた岡田聡一先生と山田裕史先生に感謝いたします。

参考文献

- [1] F. Bergeron, N. Bergeron, R. B. Howlett and D. E. Taylor, *A decomposition of the decent algebra of a finite Coxeter group*, J. Algebraic Combinatorics, 1 (1992), 23–44.

- [2] W. Fulton, "Young tableaux: with applications to representation theory and geometry", London Mathematical Society Student Texts 35, Cambridge University Press, 1997.
- [3] W. Fulton and J. Harris, "Representation theory", GTM 129, Springer-Verlag, New York, 1991.
- [4] M. Geck and G. Pfeiffer, "Characters of finite Coxeter groups and Iwahori-Hecke algebras", Oxford Science publications, 2000.
- [5] G. James-A. Kerber, "The Representation Theory of the Symmetric Group", Encyclopedia of Mathematics and its Applications, Vol. 16, 1981.
- [6] I. G. Macdonald, "Symmetric functions and Hall polynomials", Oxford mathematical monographs, 2nd. edition, 1995.
- [7] F. Oda, *A note on the parabolic Burnside ring of finite Coxeter groups of exceptional type*, preprint, (2001).
- [8] B. E. Sagan, "The symmetric group" 2nd edition, GTM 203, Springer-Verlag, New York, 2001.
- [9] L. Solomon, *A Mackey formula in the group ring of a Coxeter group*, J. Algebra, 41 (1976), 255-268.
- [10] T. Yoshida, *The generalized Burnside ring of a finite group*, Hokkaido Math. J., 19 (1990), 509-574.

分解する Schur 関数

水川裕司(北大理)

Division of Mathematics, Hokkaido University

mzh@math.sci.hokudai.ac.jp

0 Introduction

シュア関数は A 型 (= $SU(N)$) の古典群の有限次元既約表現の指標を与える極大トーラス上の複素数値多項式関数である。これはワイルの指標公式によってその具体的な形が与えられている。そのワイルの指標公式は A 型に限らず、 B 型、 C 型、 D 型及び例外型の指標を与えている。そこでこれらの関数達をその型のシュア関数として定義する ([2])。ここでは主に B 型と C 型のシュア関数の間に成り立つ関係式を考える。

もともと A 型のシュア関数に対して次のような式が知られている ([3],[5]):

$$s_{2\lambda}(\mathbf{x}_{N,2}) = s_{2\lambda^{(0)}}(\mathbf{x}_N^2) s_{2\lambda^{(1)}}(\mathbf{x}_N^2). \quad (1)$$

ここで $2\lambda = (2\lambda_1, 2\lambda_2, \dots, 2\lambda_N)$ は $SU(N)$ の最高ウェイトである。ここで、

$$\mathbf{x}_{N,2} = (x_1, \dots, x_N, -x_1, \dots, -x_N),$$

$$2\lambda^{(0)} = (\lambda_2, \lambda_4, \dots), 2\lambda^{(1)} = (\lambda_1, \lambda_3, \dots)$$

である。この形の式を分解公式と呼ぶことにして C 型のシュア関数 ($sc_{2\lambda}$) を考えることにする。すると分解公式は次のような形で得られる:

$$sc_{2\lambda}(\mathbf{x}_{N,2}) = sc_{2\lambda^{(0)}}(\mathbf{x}_N^2) sb_{2\lambda^{(1)}}(\mathbf{x}_N^2). \quad (2)$$

ここで $sb_{2\lambda^{(1)}}$ は B 型のシュア関数である。 A 型は A 型で閉じた式であったが、今度はこの様にタイプの異なる関数が現れる。この記事の主定理はこの (2) である。

以下で、まず分割の”割り算”に相当する概念である core と quotient について説明する。これは、上記の式はウエイトを 2λ に限定したが、もう少し一般の式を与えるためである。またその際 A 型のシューア関数との関係を詳しく見てみることにする。その後、古典群の最高ウエイトに関する復習をし、それぞれの型のシューア関数の定義をする。そして (2) の証明を与える。

1 Quotients and Cores of Partitions

r を 2 以上の整数, λ を分割, m を $m \geq l(\lambda)$ 且つ $m \equiv 0 \pmod{r}$ であるような整数とする。次のような記号を定義する。

$$\begin{aligned} M_k &= \left\{ \frac{\xi_i - k}{r} \mid \xi_i \equiv k \pmod{r} \right\} \\ m_k &= |M_k| \\ \xi^{(k)} &= (\xi_1^{(k)}, \dots, \xi_{m_k}^{(k)}), \xi_i^{(k)} \in M_k, (0 \leq i \leq m_k), \xi_1^{(k)} > \dots > \xi_{m_k}^{(k)}. \end{aligned}$$

そして, $\delta_n = (n-1, n-2, \dots, 1, 0)$ を用いて,

$$\lambda^{(k)} = \xi^{(k)} - \delta_{m_k}.$$

と置いて λ の r -quotient を次のように定義する。

Definition 1.1. (r -quotient for λ) r 個の分割の組,

$$\lambda^* = (\lambda^{(0)}, \lambda^{(1)}, \dots, \lambda^{(r-1)})$$

を λ の r -quotient とよぶ。

次に,

$$\begin{aligned} C_k &= \{rs + k \mid 0 \leq s \leq m_k - 1\} \\ C &= \bigcup_{k=0}^{r-1} C_k \\ \bar{\xi} &= (\bar{\xi}_1, \bar{\xi}_2, \dots, \bar{\xi}_m), \bar{\xi}_i \in C, \bar{\xi}_1 > \bar{\xi}_2 > \dots > \bar{\xi}_m \end{aligned}$$

と置く。そして,

$$\lambda^c = \bar{\xi} - \delta_m.$$

と置いて λ の r -core を次のように定義する。

Definition 1.2. (r -core for λ)

λ^c を λ の r -core と言う .

一つ例を見ておく .

Example 1.3. ここでは $\lambda = (7, 7, 4, 4, 1)$ の 3-quotient および 3-core を計算する . 始めに $\delta_6 = (5, 4, 3, 2, 1, 0)$ と取ることにする (これは $l(\lambda) = 5$ より大きな 3 の倍数なら何でも良かったことに注意) . すると,

$$\begin{aligned}\xi &= (12, 11, 7, 6, 2, 0), \\ M_0 &= \{4, 2, 0\}, M_1 = \{2\}, M_2 = \{3, 0\}.\end{aligned}$$

のように決まる . これを定義通りに計算すると,

$$\lambda^{(0)} = (2, 1, 0), \lambda^{(1)} = (2), \lambda^{(2)} = (2, 0).$$

の様にして 3-quotient が求まる . 3-core の方も同様にして,

$$\begin{aligned}C_0 &= \{6, 3, 0\}, C_1 = \{1\}, C_2 = \{5, 2\}, \\ \xi &= (6, 5, 3, 2, 1, 0).\end{aligned}$$

から,

$$\lambda^c = (1, 1).$$

が得られる .

次の簡単な命題を用意しておく .

Proposition 1.4. λ^c を分割 λ の r -core とすると次が成り立つ .

$$\lambda^c = \emptyset \Rightarrow |\lambda| \equiv 0 \pmod{r}.$$

Proposition 1.5. Let λ^c を分割 λ の r -core とすると次が成立 .

$$\lambda^c = \emptyset \Leftrightarrow |M_0| = |M_1| = \dots = |M_{r-1}| \equiv m/r.$$

以下, $\lambda \vdash rn$ 且つ, $\lambda^c = \emptyset$ と仮定する . そして λ の r -quotient と Schur 関数との関係を見る . 次のような記号を用意する,

$$\begin{aligned}\mathbf{x}_N &= (x_1, x_2, \dots, x_N), \\ \mathbf{x}_N^r &= (x_1^r, x_2^r, \dots, x_N^r) \\ \mathbf{x}_{N,r} &= (x_1, x_2, \dots, x_{rN}) \quad (x_{kN+i} = \omega^k x_i \quad (0 \leq k \leq r-1, 1 \leq i \leq N)).\end{aligned}$$

ここで,

$$\omega = \exp(2\pi\sqrt{-1}/r)$$

としておく. この $\mathbf{x}_{N,r}$ を \mathbf{x}_N の “ r -inflation” と呼ぶ. 数列 $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_M)$ に対して, $N \times M$ 行列を,

$$A_\alpha(\mathbf{x}_N) = (x_i^{\alpha_j})_{1 \leq i \leq N, 1 \leq j \leq M}$$

と置く. 分割 λ に対して $N \times N$ 行列を,

$$A_{\lambda+\delta_{rN}}(\mathbf{x}_{rN}) = \begin{pmatrix} x_1^{\lambda_1+rN-1} & x_1^{\lambda_2+rN-2} & \dots & x_1^{\lambda_{rN}} \\ x_2^{\lambda_1+rN-1} & x_2^{\lambda_2+rN-2} & \dots & x_2^{\lambda_{rN}} \\ \vdots & \vdots & \ddots & \vdots \\ x_{rN}^{\lambda_1+rN-1} & x_{rN}^{\lambda_2+rN-2} & \dots & x_{rN}^{\lambda_{rN}} \end{pmatrix}$$

と定義する. ここで Schur 関数の定義を与える.

Definition 1.6. $\lambda = (\lambda_1, \dots, \lambda_N)$, $N \leq l(\lambda)$ に対して,

$$s_\lambda(\mathbf{x}_N) = \frac{A_{\lambda+\delta_N}(\mathbf{x}_N)}{A_{\delta_N}(\mathbf{x}_N)}$$

を Schur 関数と言う.

さて, これから Schur 関数の分子の変数を r -inflation してみよう. つまり, $A_{\lambda+\delta_{rN}}(\mathbf{x}_{N,r})$ を考える.

以下,

$$\eta_k = (r\xi_1^{(k)} + k, r\xi_2^{(k)} + k, \dots, r\xi_N^{(k)} + k)$$

と置く.

$$\det A_{\lambda+\delta_{rN}}(\mathbf{x}_{N,r}) = \bar{\varepsilon}_{\lambda,r} \det(A_{\eta_0}(\mathbf{x}_{N,r}), A_{\eta_1}(\mathbf{x}_{N,r}), \dots, A_{\eta_{r-1}}(\mathbf{x}_{N,r}))$$

ここで $\bar{\varepsilon}_{\lambda,r}$ は λ と r に依存する符号である.

$$A_{\eta_k}(\mathbf{x}_{N,r}) = \begin{pmatrix} p^k A_{\xi^{(k)}}(\mathbf{x}_N^r) \\ \omega^k p^k A_{\xi^{(k)}}(\mathbf{x}_N^r) \\ \vdots \\ \omega^{(r-1)k} p^k A_{\xi^{(k)}}(\mathbf{x}_N^r) \end{pmatrix},$$

なので

$$\det A_{\lambda+\delta_{rN}}(\mathbf{x}_{N,r}) = \tilde{\varepsilon}_{\lambda,r} \begin{vmatrix} 1_N & 1_N & \dots & 1_N \\ 1_N & \omega 1_N & \dots & \omega^{r-1} 1_N \\ 1_N & \omega^2 1_N & \dots & \omega^{2(r-1)} 1_N \\ \vdots & \vdots & \ddots & \vdots \\ 1_N & \omega^{(r-1)} 1_N & \dots & \omega^{(r-1)(r-1)} 1_N \end{vmatrix} \times$$

$$\begin{vmatrix} p^0 & & & 0 \\ & p^1 & & \\ & & \ddots & \\ 0 & & & p^{r-1} \end{vmatrix} \begin{vmatrix} A_{\lambda^{(0)}+\delta_N}(\mathbf{x}_N^r) & & & 0 \\ & A_{\lambda^{(1)}+\delta_N}(\mathbf{x}_N^r) & & \\ & & \ddots & \\ 0 & & & A_{\lambda^{(r-1)}+\delta_N}(\mathbf{x}_N^r) \end{vmatrix}$$

を得る, ここで $p = \text{diag}(x_1, \dots, x_N)$ と置いた. 以上より λ の r -quotient と $A_\lambda(X_{rN})$ に自然な関係が得られた. それを Schur 関数に関する 定理として述べる.

Theorem 1.7. (Inflation for type A [5]) λ を r -core のない分割 ($\lambda^c = \emptyset$) としたとき次の式が成立する:

$$s_\lambda(\mathbf{x}_{N,r}) = \varepsilon_{\lambda,r} s_{\lambda^{(0)}}(\mathbf{x}_N^r) s_{\lambda^{(1)}}(\mathbf{x}_N^r) \dots s_{\lambda^{(r-1)}}(\mathbf{x}_N^r).$$

ここで $\varepsilon_{\lambda,r} = \tilde{\varepsilon}_{\lambda,r} / \tilde{\varepsilon}_{\emptyset,r}$.

Proof. $s_\lambda(\mathbf{x}_{N,r})$ の分子に関する式は, 分子の計算を $\lambda = \emptyset$ と置くことで得られる. □

2 C 型の分解公式

この章では B 型及び, C 型のシューア関数を次のワイルの指標公式によって定義する. そして C 型のシューア関数が 2-inflation によってどのように分解するのかを見る.

$\lambda = (\lambda_1, \dots, \lambda_N)$ として古典群の最高ウェイトを列挙しておく:

$$A_{N-1}: P_{A_{N-1}}^+ = \{\lambda \in \mathbb{Z}^N \mid \lambda_1 \geq \dots \geq \lambda_N \geq 0\}.$$

$$B_N: P_{B_N}^+ = \{\lambda \in \mathbb{Z}^N \mid \lambda_1 \geq \dots \geq \lambda_N \geq 0\}.$$

$SO(2N+1)$ の普遍被覆群である $Spin(2N+1)$ の最高ウェイトは

$$P_{B_N}^+ = \{\lambda \in \mathbb{Z}^N, \mathbb{Z}^N + 1/2(1, \dots, 1) \mid \lambda_1 \geq \dots \geq \lambda_N \geq 0\}$$

で与えられる.

$$C_N: P_{C_N}^+ = \{\lambda \in \mathbb{Z}^N \mid \lambda_1 \geq \dots \geq \lambda_N \geq 0\}.$$

$$D_N: P_{D_N}^+ = \{\lambda \in \mathbb{Z}^N \mid \lambda_1 \geq \dots \geq |\lambda_N|\}.$$

$SO(2N)$ の普遍被覆群である $Spin(2N)$ の最高ウェイトは

$$P_{D_N}^+ = \{\lambda \in \mathbb{Z}^N, \mathbb{Z}^N + 1/2(1, \dots, 1) \mid \lambda_1 \geq \dots \geq |\lambda_N|\}$$

で与えられる. さてこれを踏まえてワイルの指標公式を述べよう.

Proposition 2.1. (ワイルの指標公式) 最高ウェイトが $\lambda = (\lambda_1, \lambda_2, \dots)$ で与えられる A 型, B 型, C 型, D 型の古典群の既約指標は (t_1, \dots, t_N) を各最大トーラス乗の座標としたとき次のように与えられる:

$$\begin{aligned} \pi_\lambda^A(t) &= \frac{\det(t_i^{\lambda_j + N - j})_{1 \leq i, j \leq N}}{\det(t_i^{N - j})_{1 \leq i, j \leq N}}, \\ \pi_\lambda^B(t) &= \frac{\det(t_i^{\lambda_j + N - j + 1/2} - t_i^{-(\lambda_j + N - j + 1/2)})_{1 \leq i, j \leq N}}{\det(t_i^{N - j + 1/2} - t_i^{-(N - j + 1/2)})_{1 \leq i, j \leq N}}, \\ \pi_\lambda^C(t) &= \frac{\det(t_i^{\lambda_j + N - j + 1} - t_i^{-(\lambda_j + N - j + 1)})_{1 \leq i, j \leq N}}{\det(t_i^{N - j + 1} - t_i^{-(N - j + 1)})_{1 \leq i, j \leq N}}, \\ \pi_\lambda^D(t) &= \frac{\det(t_i^{\lambda_j + N - j} - t_i^{-(\lambda_j + N - j)}) + \det(t_i^{\lambda_j + N - j} + t_i^{-(\lambda_j + N - j)})}{\det(t_i^{N - j} + t_i^{-(N - j)})_{1 \leq i, j \leq N}}. \end{aligned}$$

この定理を踏まえて

$$B_\alpha(\mathbf{x}_N) = (x_i^{\alpha_j + 1/2} - x_i^{-(\alpha_j + 1/2)})_{1 \leq i \leq N, 1 \leq j \leq M},$$

$$C_\alpha(\mathbf{x}_N) = (x_i^{\alpha_j + 1} - x_i^{-(\alpha_j + 1)})_{1 \leq i \leq N, 1 \leq j \leq M}.$$

のように行列をおいて次のように定義する ([2]).

Definition 2.2. (Schur functions for type B and type C)

$\lambda = (\lambda_1, \dots, \lambda_N)$ を分割 $\delta_N = (N-1, N-2, \dots, 1, 0)$ とする. このとき B 型及び, C 型のシューア関数を次で定義する.

$$sb_\lambda(\mathbf{x}_N) = \frac{B_{\lambda + \delta_N}(\mathbf{x}_N)}{B_{\delta_N}(\mathbf{x}_N)},$$

$$sc_\lambda(\mathbf{x}_N) = \frac{C_{\lambda + \delta_N}(\mathbf{x}_N)}{C_{\delta_N}(\mathbf{x}_N)}.$$

では C 型のシューア関数の分解公式を述べよう.

Theorem 2.3. (Inflation for type C) $\lambda = (\lambda_1, \dots, \lambda_N)$ を 2 -core が空であるような分割とする. このとき次の式が成り立つ.

$$sc_\lambda(\mathbf{x}_{N,2}) = \varepsilon_{\lambda,2} sb_{\lambda^{(0)}}(\mathbf{x}_N^2) sc_{\lambda^{(1)}}(\mathbf{x}_N^2).$$

ここで $\varepsilon_{\lambda,2}$ は λ に依存する符号である.

Proof.

$$\varphi_{\alpha_j}(x_i) = x_i^{\alpha_j} - x_i^{-\alpha_j}.$$

と置いてまずは C 型のシューア関数の定義式の分子から見てみよう. すると,

$$C_{\lambda+\delta_{2N}}(\mathbf{x}_{N,2}) = \begin{pmatrix} \varphi_{\lambda_1+2N}(x_1) & \varphi_{\lambda_2+2N-1}(x_1) & \cdots & \varphi_{\lambda_{2N}+1}(x_1) \\ \vdots & \vdots & & \vdots \\ \varphi_{\lambda_1+2N}(x_N) & \varphi_{\lambda_2+2N-1}(x_N) & \cdots & \varphi_{\lambda_{2N}+1}(x_N) \\ \varphi_{\lambda_1+2N}(-x_1) & \varphi_{\lambda_2+2N-1}(-x_1) & \cdots & \varphi_{\lambda_{2N}+1}(-x_1) \\ \vdots & \vdots & & \vdots \\ \varphi_{\lambda_1+2N}(-x_N) & \varphi_{\lambda_2+2N-1}(-x_N) & \cdots & \varphi_{\lambda_{2N}+1}(-x_N) \end{pmatrix}.$$

であるから, $\eta_0 = (2\xi_1^{(0)} + 1, 2\xi_2^{(0)} + 1, \dots, 2\xi_N^{(0)} + 1)$ かつ $\eta_1 = (2\xi_1^{(1)} + 2, 2\xi_2^{(1)} + 2, \dots, 2\xi_N^{(1)} + 2)$ と置くと,

$$\det C_{\lambda+\delta_{2N}}(\mathbf{x}_{N,2}) = \tilde{\varepsilon}_{\lambda,2} \det(C_{\eta_0}(\mathbf{x}_{N,2}), C_{\eta_1}(\mathbf{x}_{N,2}))$$

を得る. したがって,

$$C_{\eta_0}(\mathbf{x}_{N,2}) = \begin{pmatrix} B_{\xi^{(0)}}(\mathbf{x}_N^2) \\ -B_{\xi^{(0)}}(\mathbf{x}_N^2) \end{pmatrix},$$

$$C_{\eta_1}(\mathbf{x}_{N,2}) = \begin{pmatrix} C_{\xi^{(1)}}(\mathbf{x}_N^2) \\ C_{\xi^{(1)}}(\mathbf{x}_N^2) \end{pmatrix}.$$

である. それゆえ

$$\det C_{\lambda+\delta_{2N}}(\mathbf{x}_{N,2}) = \tilde{\varepsilon}_{\lambda,2} \begin{vmatrix} 1_N & 1_N \\ -1_N & 1_N \end{vmatrix} \begin{vmatrix} B_{\lambda^{(0)}+\delta_N}(\mathbf{x}_N^2) & 0 \\ 0 & C_{\lambda^{(1)}+\delta_N}(\mathbf{x}_N^2) \end{vmatrix}$$

となる. $sc_\lambda(\mathbf{x}_{N,2})$ の分母は, $\lambda = \emptyset$ と置いて上の計算をすればわかる. 以上をまとめて,

$$\begin{aligned} sc_\lambda(\mathbf{x}_{N,2}) &= \frac{C_{\lambda+\delta_{2N}}(\mathbf{x}_{N,2})}{C_{\delta_{2N}}(\mathbf{x}_{N,2})} \\ &= \frac{\tilde{\varepsilon}_{\lambda,2} C_{\lambda^{(0)}+\delta_N}(\mathbf{x}_N^2) B_{\lambda^{(1)}+\delta_N}(\mathbf{x}_N^2)}{\tilde{\varepsilon}_{\emptyset,2} C_{\delta_N}(\mathbf{x}_N^2) B_{\delta_N}(\mathbf{x}_N^2)} \\ &= \varepsilon_{\lambda,2} sb_{\lambda^{(0)}}(\mathbf{x}_N^2) sc_{\lambda^{(1)}}(\mathbf{x}_N^2) \end{aligned}$$

を得る. □

上の定理に現れる符号, $\tilde{\varepsilon}_{\lambda,2}$, は上で定義した行列の基本変形により現れるものであり, それは λ と N に依存するが分子と分母で割り算することで $\varepsilon_{\lambda,2}$ は, N には依存しなくなること注意到しておく.

さらに同様に D 型に対しても分解公式を作ることが出来る ([6]). 同様の公式は例えば Lie 超代数のシューア関数などに対しても作ることが出来る. 分解公式の応用としては対称関数の plethysm の計算に有用であることが知られている ([1]). さらにシューア関数はシューア-ワイル相互律を通じてそれぞれの交換団である代数の指標の母関数であることに注意すれば ([8]), 交換団の指標に関する公式も得られることに注意しておく ([3],[5]).

またその他にシューアの Q -関数として知られる対称関数の分解公式も作ることが出来る, この場合は core と quotient にあたるものとして bar-core, bar-quotien と云った概念を用い記述することが出来る ([5]).

参考文献

- [1] Y. Chen, A. Garsia and J. Remmel, Algorithms for plethysm, in Combinatorics and Algebra, Contemporary Math., 34, 109-153. Adv. Math., 128, (1997), 40-81.
- [2] K. Koike, Representations of spinor groups and the difference characters of $SO(2n)$, Adv. Math., 128, (1997), 40-81.
- [3] D. E. Littlewood, *The Theory of Group Characters, 2nd. ed.*, Oxford, 1950.

- [4] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd. ed. , Oxford, 1995.
- [5] H. Mizukawa and H.-F. Yamada, Littlewood's multiple formula for spin characters of symmetric groups, J. London Math. Soc., to appear.
- [6] H. Mizukawa, Inflation of variables for Schur functions, preprint, 2001.
- [7] A. Knapp, *Lie Groups Beyond an Introduction.*, Progress in Mathematics Volume 140, Birkhauser, Boston-Basel-Berlin, 1996.
- [8] A. Ram, Characters of Brauer's centralizer algebras, Pacific J. of Math., 169, (1995), 173-200.
- [9] H. Weyl, *The Classical Groups, Their Invariants and Representations*, 2nd. ed. , Princeton Univ. Press, Princeton, NJ, 1946. Oxford, 1995.

Morita equivalence of Isaacs correspondence for blocks of finite groups

渡辺アツミ (熊本大学理学部)

§1. Introduction

Two rings R and S are Morita equivalent if there are additive equivalences between the categories of R -modules and S -modules. If S is isomorphic to the matrix ring $M(n, R)$ over R with degree n , then R and S are Morita equivalent.

Let $(\mathcal{K}, \mathcal{R}, \mathcal{F})$ be a p -modular system such that \mathcal{K} is algebraically closed, and let A and G be finite groups such that A acts on G via automorphism and that $(|A|, |G|) = 1$ throughout this talk. We denote by $\text{Irr}(G)$ the set of irreducible \mathcal{K} -characters of G and by $\text{Irr}_A(G)$ the set of A -invariant irreducible characters of G as usual. It is well known that there is a one to one correspondence $\pi(G, A)$, what we call Glauberman-Isaacs correspondence, between $\text{Irr}_A(G)$ and $\text{Irr}(C)$ where $C = C_G(A)$ by [G] and [I]. When A is solvable, $\pi(G, A)$ is the Glauberman correspondence, and when $|G|$ is odd, $\pi(G, A)$ is the Isaacs correspondence. Here we recall briefly the definition of Isaacs correspondence.

Lemma 1 ([I, Corollary 10.7]; [Wo1, Corollary 4.3]) *With the above notations we assume that $|G|$ is odd. Let $[G, A]'C \leq H \leq G$ such that H is A -invariant. Then there exists a bijection $\sigma(G, H, A) : \text{Irr}_A(G) \rightarrow \text{Irr}_A(H)$ such that for $\chi \in \text{Irr}_A(G)$, $\sigma(G, H, A)(\chi)$ is the unique A -invariant irreducible character α of H with the inner product (χ_H, α) odd.*

Definition ([I, §10]) *With the notations and assumptions in the above lemma, if $C < G$, then let*

$$G = G_0 > G_1 > G_2 > G_3 > \cdots > G_n = C$$

by $G_{i+1} = [G_i, A]'C$, for $i \geq 0$. *The Isaacs character correspondence $\pi(G, A) : \text{Irr}_A(G) \rightarrow \text{Irr}(C)$ is the composition map*

$$\sigma(G_{n-1}, C, A)\sigma(G_{n-2}, G_{n-1}, A) \cdots \sigma(G_2, G_1, A)\sigma(G, G_1, A)$$

if $C < G$, otherwise $\pi(G, A)$ is the identity map.

The Glauberman-Isaacs correspondence gives a correspondence between the A -invariant p -blocks of G and the blocks of C as follows.

Theorem 2 ([Wa1, Theorem 1], [H1, Theorem 1] and [P, Theorem 39])
Let B be an A -invariant p -block of G such that a defect group D of B is contained in $C_G(A)$. Then there exists a block b of $C_G(A)$ such that B and b are perfect isometric by $\pi(G, A)$ in the sense of M. Broué [B].

Here a p -block of G denotes a block algebra of $\mathcal{R}G$. b is called the Glauberman correspondent and the Isaacs correspondent of B when A is solvable and when $|G|$ is odd, respectively. In fact B and b are isotypic [Wa2, Theorem 3.6] and [P, Theorem 39]. It is also known that b has D as a defect group. Recently in [K-M, Theorem 3.1] S. Koshitani and G.O. Michler showed that the Brauer correspondents of B and b are Morita equivalent over \mathcal{F} , and in particular if D is normal in G then $\bar{B} = \mathcal{F} \otimes_{\mathcal{R}} B$ and $\bar{b} = \mathcal{F} \otimes_{\mathcal{R}} b$ are Morita equivalent. Moreover in [H2, Theorem 1] H. Horimoto showed that B and b are Morita equivalent if S is solvable and G is p -solvable by using a result of Dade-Koshitani-Michler in [K-M]. L. Puig also proved it. In this talk I will show that if $|G|$ is odd then B and b are Morita equivalent.

Theorem 3 *Assume $|G|$ is odd and let B be an A -invariant p -block of G such that a defect group D of B is contained in $C_G(A)$ and let b be the Isaacs correspondent of B . Then B and b are Morita equivalent.*

§2. Outline of a proof of Theorem 3

We prove the theorem by $|G|$ -induction. The following results by Isaacs and Wolf are important in our arguments as in [H1] and [Wa2].

Lemma 4 ([Wo1, Theorem 4.6]) *Assume $|G|$ is odd. Let $K = [G, A]$ and let U be an A -invariant subgroup of G such that $K' C \leq U \leq G$. Let $\chi \in \text{Irr}_A(G)$ and $\psi = \sigma(G, U, A)(\chi)$. Then*

- (a) $\sigma(G, K'C, A)(\chi) = \sigma(H, K'C, A)(\psi)$, and
- (b) $\pi(G, A)(\chi) = \pi(U, A)(\psi)$.

Lemma 5 ([Wo2, Lemma 2.5]) *Let N be an A -invariant normal subgroup of G . Let $\chi \in \text{Irr}_A(G)$, $\theta \in \text{Irr}_A(N)$, $T = T_G(\theta)$ the inertial subgroup of θ in G , $\mu = \pi(G, A)(\chi)$, and $\nu = \pi(N, A)(\theta)$. Then*

- (a) $(\chi_N, \theta) \neq 0$ if and only if $(\mu_{N \cap C}, \nu) \neq 0$,
- (b) $T \cap C = T_C(\nu)$ and $\pi(G, A)(\psi^G) = (\pi(T, A)(\psi))^C$ for $\psi \in \text{Irr}_A(T|\theta)$.

Our proof of Theorem 3 is essentially reduced to a fully ramified correspondence case for blocks (see [H1, §1]). Here we recall the fully ramified correspondence for characters due to Isaacs, using notations in [I]. Let $L \leq K \triangleleft G$ with $L \triangleleft G$ and K/L is abelian. Suppose that $\phi \in \text{Irr}(L)$ is fully ramified with respect to K/L and is G -invariant. Let θ be the unique irreducible constituent of ϕ^K , so that θ is G -invariant. Then (G, K, L, θ, ϕ) is called a character five.

Theorem 6 ([I, Theorem 9.1 ; Corollary 6.4]) *Let (G, K, L, θ, ϕ) be a character five such that either $|G : K|$ or $|K : L|$ is odd. Let $\Psi^{(K/L)}$ be the character of G/K defined with respect to the form \ll, \gg_ϕ on K/L , and view $\Psi^{(K/L)}$ as a character of G . Then there exists a G -conjugacy class \mathcal{U} of subgroups $U \leq G$ such that*

- (a) $(\Psi^{(K/L)}(x))^2 = \pm |C_{K/L}(x)|$ for $x \in G$, in particular $\Psi^{(K/L)}(1) = \sqrt{|K/L|}$;
- (b) $UK = G$ and $U \cap K = L$;
- (c) U^a is G -conjugate to U for all $a \in \text{Aut}(G)$ such that $K^a = K$, $L^a = L$ and $\phi^a = \phi$;
- (d) the equation $\chi_U = (\Psi^{(K/L)})_U \xi$, for $\chi \in \text{Irr}(G|\theta)$ and $\xi \in \text{Irr}(U|\phi)$ defines a 1-1 correspondence between these sets of characters, and
- (e) if $|G : K|$ is odd, $\chi \in \text{Irr}(G|\theta)$ and $\xi \in \text{Irr}(U|\phi)$, then $\chi_U = (\Psi^{(K/L)})_U \xi$ if and only if (χ_U, ξ) is odd.

The correspondence in Theorem 6, (d) is called a fully ramified correspondence with respect to (G, K, L, θ, ϕ) .

Now in our situation let $K = [G, A]$ and θ be an A -invariant irreducible character of K covered by B . By a lemma of Glauberman we have $G =$

CK and we have also $C \cap K \subseteq K'$. By the induction hypothesis we may assume that D is a Sylow p -subgroup of G , and hence K is a p' -group. Let $\Gamma = AG$ the semi direct product of G by A , K/L be a chief factor group of Γ and $U = CL$. Then $G = UK$, $U \cap K = L$ and $U < G$ because we may assume $C < G$. Besides a Sylow p -subgroup of U also is centralized by A . Let χ_0 be an element of $\text{Irr}(B)$. By [I, Theorem (10.7)] and Lemma 1, there exists a unique A -invariant constituent α_0 of χ_{0U} with odd multiplicity because $U \geq CK'$. Let B_U be a block of U which contains α_0 . Then B_U is A -invariant and b is the Isaacs correspondent of B_U by Lemma 4. Hence in order to complete the proof it suffices to show that B_U and B are Morita equivalent by the induction hypothesis for B_U . Now let ϕ be an A -invariant irreducible character of L covered by B_U . Then ϕ is a constituent of θ_L and we can assume that (G, K, L, θ, ϕ) is a character five. Moreover there is a fully ramified correspondence between $\text{Irr}(G|\theta)$ and $\text{Irr}(U|\phi)$. Moreover since α_0 is an irreducible constituent of χ_{0U} with odd multiplicity, α_0 is the fully ramified correspondent of χ_0 with respect to (G, K, L, θ, ϕ) . Suppose that θ is extended to G and let $\hat{\theta}$ be an extension of θ . Let $\hat{\phi} \in \text{Irr}(U)$ be the fully ramified correspondent of $\hat{\theta}$. Since $\theta(1) = \sqrt{|K/L|}\phi(1)$, and $\hat{\theta}(1) = \sqrt{|K/L|}\hat{\phi}(1)$ by Theorem 6 (a), $\hat{\phi}$ is an extension of ϕ . Then we can see that there exists a block \bar{B} of $\bar{G} = G/K$ such that $B \cong M(\theta(1), \bar{B})$ and $B_U \cong M(\phi(1), \bar{B})$ where we identify G/K with U/L . Hence B and b are Morita equivalent.

Let e_θ be the central idempotent of $\mathcal{R}K$ corresponding to θ . We have an \mathcal{R} -algebra isomorphism $\Theta : \mathcal{R}Ke_\theta \cong M(n, \mathcal{R})$ where $n = \theta(1)$. Let

$$\hat{G} = \{(g, u) \in G \times (\mathcal{R}Ke_\theta)^\times \mid (ke_\theta)^g = (ke_\theta)^u \ (\forall k \in K), (\det \Theta(u))^{|K|} = 1\}$$

where $(\mathcal{R}Ke_\theta)^\times$ is the group of units in $\mathcal{R}Ke_\theta$. Then \hat{G} forms a group and $Z = \{(1, u) \in \hat{G}\}$ is a central p' -subgroup of \hat{G} of order $n|K|$. Moreover $\hat{G}/Z \cong G$. In particular $(|\hat{G}|, |A|) = 1$. Let

$$\hat{K} = \{(k, ke_\theta) \in \hat{G} \mid k \in K\}, \hat{L} = \{(l, le_\theta) \in \hat{G} \mid l \in L\}.$$

Then we have $\hat{K} \cong K$ and $\hat{L} \cong L$. As A acts on $\mathcal{R}Ke_\theta$ as an \mathcal{R} -algebra automorphism, an action of A on \hat{G} via automorphism is defined as follows : $(g, u)^a = (g^a, u^a)$ for $a \in A$ and $(g, u) \in \hat{G}$. Then we have $\hat{G} = C_{\hat{G}}(A)\hat{K}$ and $[\hat{G}, A] = \hat{K}$. Now we regard θ and ϕ as characters of \hat{K} and \hat{L} respectively. Then $(\hat{G}, \hat{K}, \hat{L}, \theta, \phi)$ is an A -invariant character five.

Let $\hat{U} = C_{\hat{G}}(A)\hat{L}$. This is the inverse image of U of the homomorphism $\hat{G}/Z \rightarrow G$. By Theorem 6 again there exists a fully ramified correspondence between $\text{Irr}(\hat{G}|\theta)$ and $\text{Irr}(\hat{U}|\phi)$. Moreover when we regard χ_0 and α_0 as irreducible characters of \hat{G} and \hat{U} respectively by the inflations, α_0 is the fully ramified correspondent of χ_0 with respect to $(\hat{G}, \hat{K}, \hat{L}, \theta, \phi)$. Now

$$\hat{\Theta} : \hat{G} \rightarrow \text{GL}(n, \mathcal{K}) \quad ((g, u) \mapsto \Theta(u))$$

is an irreducible representation of \hat{G} such that $\Theta_{\hat{K}}$ affords the character θ . Let \hat{B} and \hat{B}_U be the inflations of B and B_U to \hat{G} and \hat{U} , respectively. By the above \hat{B} and \hat{B}_U are Morita equivalent. On the other hand we have $B \cong \hat{B}$ and $B_U \cong \hat{B}_U$. Therefore B and B_U are Morita equivalent. This completes the proof.

See [Wa3] for a detail of a proof of the theorem.

References

- [B] M. Broué ; Isométries parfaites, types de blocs, catégories dérivés, *Astérisque*, **181-182**(1990), 61-92.
- [G] G. Glauberman ; Correspondences of characters for relatively prime operator groups, *Canad. J. Math.* **20**(1968), 1465-1488.
- [H1] H. Horimoto ; On a correspondence between blocks of finite groups induced from the Isaacs character correspondence, *Hokkaido Math. J.*, **30**(2001), 65-74.
- [H2] H. Horimoto ; A correspondence of the Glauberman correspondence of p -blocks of finite p -solvable groups, to appear in *Hokkaido Math. J.*.
- [I] I.M. Isaacs ; Characters of solvable and symplectic groups, *Amer.J. Math.*, **95**(1973), 594-635.
- [K-M] S. Koshitani - G.O. Michler ; Glauberman correspondence of p -blocks of finite groups, to appear in *J. Algebra*.
- [P] L. Puig ; On the Brauer-Glauberman correspondence, preprint.
- [Wa1] A. Watanabe ; The Glauberman character correspondence and perfect isometries for blocks of finite groups, *J. Algebra*, **216**(1999), 548-565.

[Wa2] A. Watanabe ; The Isaacs character correspondence and isotypies between blocks of finite groups, to appear in "Groups and Combinatorics, in memory of Michio Suzuki", Advanced Studies in Pure Mathematics.

[Wa3] A. Watanabe ; Morita equivalence of Isaacs correspondence for blocks of finite groups.

[Wo1] T.R. Wolf ; Character correspondence in solvable groups, Illinois J. Math., **22**(1978), 327-340.

[Wo2] T.R. Wolf ; Character correspondences induced by subgroups of operator groups, J. Algebra **57**(1979), 502-521.

Some results on the graded rings coming from coding theory

大浦 学 (Manabu OURA)
札幌医科大学医学部数学教室

還暦をむかえられた小関道夫先生 (山形大学) の初期の業績について、特に二つの論文に注目したいと思います。テータ級数と似た性質を持つ級数について調べた論文 [5] と、種数 2 のジーゲルモジュラ形式の重さが 4 の倍数であるような環の生成元を、偶ユニモジュラ格子のテータ級数を用いてあらわした論文 [6] について、それらに関連する事柄も含めて解説します。その後、Steven Dougherty (Scranton 大, アメリカ), Aaron Gulliver (Victoria 大, カナダ) との共著のなかで符号に関する次数付き環を決定しましたので、その部分について報告します。

この講演 (およびこの報告) のタイトルは、内容を的確にあらわすものではありませんが、プログラムのままにしておきました。

筆者が聞いたかぎりでは、先生は整数論、特に二次形式への興味から研究を始められ、テータ級数、モジュラ形式の研究へと進んでいかれたと思います。ここで取り上げた二つの論文は、その特徴をあらわすものと思います。

1. 論文 [5] について。この節では主に種数 (genus) が 1 の場合のモジュラ形式を取り扱うことになります。

$\Gamma_1 = SL(2, \mathbb{Z})$ に関する整数係数のモジュラ形式のなす環は、代数的独立な二つのアイゼンシュタイン級数 $\mathfrak{E}_2(\tau)$, $\mathfrak{E}_3(\tau)$ で生成することができます。ここで τ は上半平面上の点をあらわします。長さ n の偶ユニモジュラ格子のテータ級数は、重さ $n/2$ のモジュラ形式となりますが、そのフーリエ係数は、非負整数であり、定数項は 1 です。この論文では次の問題を考えます。

定数項が 1 である、非負整数のフーリエ係数を持つ重さ 12, 16 のモジュラ形式を全て求めよ。

ところで重さが 12 であるアイゼンシュタイン級数 $\mathfrak{E}_6(\tau)$ は、次のフーリエ展開を持ちます：

$$\mathfrak{E}_6(\tau) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) e^{2\pi i n \tau}$$

ここで、 $\sigma_{11}(n) = \sum_{d|n, d>0} d^{11}$ 。また、重さ 12 の尖点形式 $\Delta(\tau)$ は次のフーリエ展開を持ちます：

$$\Delta(\tau) = \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n \tau},$$

ここで $\tau(1) = 1, \tau(2) = -24, \tau(3) = 252, \tau(4) = -1472, \tau(5) = 4830, \dots$ です。
 また偶ユニモジュラ格子のテータ級数との関係は

$$\begin{aligned} \vartheta_{E_8^3}(\tau) &= \mathfrak{E}_6(\tau) + \left(720 - \frac{65520}{691}\right) \Delta(\tau), \\ \vartheta_{D_{24}^+}(\tau) &= \mathfrak{E}_6(\tau) + \left(1104 - \frac{65520}{691}\right) \Delta(\tau) \end{aligned}$$

となります。

$\varphi(\tau)$ を定数項 1 の非負整数フーリエ係数を持つ、重さ 12 のモジュラ形式とします。すると

$$\begin{aligned} \varphi(\tau) &= s\vartheta_{E_8^3}(\tau) + t\vartheta_{D_{24}^+}(\tau) \\ &= (s+t) \left(\mathfrak{E}_6(\tau) - \frac{65520}{691} \Delta(\tau) \right) + (720s + 1104t) \Delta(\tau) \end{aligned}$$

と書くことができます。ここで、 s, t は複素数です。今、

$$\varphi(\tau) = 1 + \sum_{n=1}^{\infty} b(n)e^{2\pi in\tau}$$

とおくと、 $s+t=1$ の条件を考えると

$$b(n) = \frac{65520}{691}(\sigma_{11}(n) - \tau(n)) + (1104 - 384s)\tau(n) \quad (1)$$

が得られます。 $(65520, 691) = 1$ に注意します。故に全ての自然数 n に対して $b(n)$ が非負整数であればいいわけです。低い n については

$$\begin{aligned} b(1) &= 1104 - 384s \\ b(2) &= 3 \cdot 66520 - 24(1104 - 384s) \end{aligned}$$

となります。

まず、 $1104 - 384s$ が整数ならば、ラマヌジャンの合同式

$$\sigma_{11}(n) \equiv \tau(n) \pmod{691}$$

とあわせて、(1) より、全ての自然数 n に対して $b(n)$ は整数であることが分かります。

次に、 $b(1), b(2)$ が零以上、つまり

$$-7086 \leq 384s \leq 1104$$

という条件 (整数条件は入っていない) から、 $n \geq 2$ ならば $b(n) \geq 0$ という事実が示されます。この部分の証明は幾つか補題を必要とします。

以上から

Theorem 1 in [5]. $\varphi(\tau)$ が定数項 1 の非負整数フーリエ係数を持つ重さ 12 のモジュラ形式である為の必要十分条件は, $384s$ が整数であり, かつ $-7086 \leq 384s \leq 1104$ を満たすことである. そのような $\varphi(\tau)$ は 8191 個ある.

重さが 16 の場合のそのようなモジュラ形式の数は 19343 です (**Theorem 2** in [5]).

似たような問題の符号版を考えてみます.

二元符号の重み多項式は

$$W_C(x, y) = \sum_{v \in C} x^{n - \text{wt}(v)} y^{\text{wt}(v)}$$

で定義されます. ここで, $\text{wt}(v)$ は $v_i = 1$ となる i の数をあらわします. 全ての自己双対重偶符号の重み多項式で生成される C 上の環を \mathfrak{M} と書くと, これは代数的独立な二つの元 $W_{e_8}(x, y)$, $W_{g_{24}}(x, y)$ で C 上生成された環であることが知られています.

$$I_8 = W_{e_8}(x, y), \quad I_{24} = W_{g_{24}}(x, y)$$

とおきます. I の添字は斉次多項式としてのそれぞれの次数をあらわしています. さて, \mathfrak{M} の次数 24 の元で

$$\begin{aligned} x^{24} \text{ の係数は } 1 \\ \text{他の係数は非負整数} \end{aligned}$$

であるようなものの数をかぞえてみます (ここで, \mathfrak{M} の元は全て変数 x, y に関して対称であることに注意しておきます). 実際, そのような元を φ と書きますと,

$$\begin{aligned} \varphi &= sI_8^3 + tI_{24} \\ &= (s+t)x^{24} + 42sx^{20}y^4 + (591s + 759t)x^{16}y^8 + (2828s + 2576t)x^{12}y^{12} + \dots \end{aligned}$$

と書くことができます. ここで s, t は複素数です. 先の条件を実際書き下すと

$$\begin{aligned} s + t &= 1, \\ 42s, 591s + 759t, 2828s + 2576t &\text{ は全て非負整数} \end{aligned}$$

となります. この条件を満たす φ は, 少々計算をしますと

$$42s = 0, 1, 2, \dots, 189$$

に対応した 190 個があることとなります.

2. 論文 [6] について. この節では主に種数が 2 の場合のモジュラ形式を取り扱うこととなります.

$\Gamma_2 = Sp(4, \mathbb{Z}) \subset GL(4, \mathbb{Z})$ に関するジーゲルモジュラ形式の成す環 $A(\Gamma_2)$ は, 代数的独立な四つのアイゼンシュタイン級数 $\psi_4, \psi_6, \psi_{10}, \psi_{12}$ と重さが 35 の尖点形式 χ_{35} で生成されることが知られています. 2 次のジーゲル上半空間の点をあらわす τ は省略します. χ_{35}^2 は上にあげた四つのアイゼンシュタイン級数の多項式としてあらわすことができるので, ここでの話には関係ありません.

重さが偶数のモジュラ形式で生成される環 $A(\Gamma_2)^{(2)}$ は, 四つのアイゼンシュタイン級数 $\psi_4, \psi_6, \psi_{10}, \psi_{12}$ で生成され, その次元公式は

$$\begin{aligned} \sum_k \dim A_{2k}(\Gamma_2) &= \frac{1}{(1-t^4)(1-t^6)(1-t^{10})(1-t^{12})} \\ &= 1 + t^4 + t^6 + t^8 + 2t^{10} + 3t^{12} + 2t^{14} + 4t^{16} + 4t^{18} + 5t^{20} + \dots \end{aligned}$$

となります. ここではとくに $t^4, t^{12}, t^{16}, t^{20}$ の係数, つまり

$$\dim A_4(\Gamma_2) = 1, \dim A_{12}(\Gamma_2) = 3, \dim A_{16}(\Gamma_2) = 4, \dim A_{20}(\Gamma_2) = 5 \quad (2)$$

が後で必要となります.

さて, 重さが 4 の倍数であるようなモジュラ形式が成す環 $A(\Gamma_2)^{(4)}$ の構造を知りたいのですが, その為に

$$4p_1 + 6p_2 + 10p_3 + 12p_4 = 4q$$

を満たす非負整数の五つ組 $(p_1, p_2, p_3, p_4; q)$ の成す加法的モノイドを考えます. これは重さが $4q$ のモジュラ形式 $\psi_4^{p_1} \psi_6^{p_2} \psi_{10}^{p_3} \psi_{12}^{p_4}$ に対応しています. このモノイドは

$$(1, 0, 0, 0; 1), (0, 2, 0, 0; 3), (0, 1, 1, 0; 4), (0, 0, 2, 0; 5), (0, 0, 0, 1; 3)$$

で生成することができるので,

$$A(\Gamma_2)^{(4)} = \mathbb{C}[\psi_4, \psi_6^2, \psi_6\psi_{10}, \psi_{10}^2, \psi_{12}]$$

となります. これら生成元の重さはそれぞれ 4, 12, 16, 20, 12 です. もし (2) を満たす十分な数のモジュラ形式が得られれば, $A(\Gamma_2)^{(4)}$ の生成元をすべて含んでいることとなります. 実際, 次にそのような元を与えます.

$A(\Gamma_2)^{(4)}$ の生成元を与える為に, 格子から得られるテータ級数を考えます.

次元 n の偶ユニモジュラ格子から得られる種数 2 のテータ級数は, 重さ $n/2$ のジーゲルモジュラ形式の例を与えています. 偶ユニモジュラ格子が存在するのは, n が 8 の倍数である時, またその時のみに限られますので, 得られたモジュラ形式は $A(\Gamma_2)^{(4)}$ の元であることが分かります. そこで次のような環を考えます:

$$R = \mathbb{C}[\vartheta_{E_8}, \vartheta_{A_{24}}, \vartheta_{D_{24}^+}, \vartheta_{D_{32}^+}, \vartheta_{D_{40}^+}].$$

R が $A(\Gamma_2)^{(4)}$ に含まれるのは当然ですが, 実は一致します. 上の議論から示すべきことは次です:

ϑ_{E_8} が 1 次元ベクトル空間をなすこと,
 $\vartheta_{E_8}^3, \vartheta_{A_{24}}, \vartheta_{D_{24}^+}$ が 3 次元ベクトル空間をなすこと,
 $\vartheta_{E_8}^4, \vartheta_{E_8} \vartheta_{A_{24}}, \vartheta_{E_8} \vartheta_{D_{24}^+}, \vartheta_{D_{32}^+}$ が 4 次元ベクトル空間をなすこと,
 $\vartheta_{E_8}^5, \vartheta_{E_8}^2 \vartheta_{A_{24}}, \vartheta_{E_8}^2 \vartheta_{D_{32}^+}, \vartheta_{E_8} \vartheta_{D_{40}^+}$ が 5 次元ベクトル空間をなすこと.

これより次の定理が得られます:

THEOREM in [6] 環 $A(\Gamma_2)^{(4)}$ は \mathbb{C} 上 $\vartheta_{E_8}, \vartheta_{A_{24}}, \vartheta_{D_{24}^+}, \vartheta_{D_{32}^+}, \vartheta_{D_{40}^+}$ で生成することができる.

W. Duke は論文 [2] において, この定理を応用して, 自己双対重偶符号に対する種数 2 の重み多項式のなす環 $\mathfrak{M}^{(2)}$ (この記号は後で定義されます) を決定しました.

論文 [6] においてもそうですが, ジーゲルモジュラ形式のフーリエ係数は重要な役割を果たします. 小関先生は, 具体的にフーリエ係数を求めた論文¹, フーリエ係数のもつ性質を与えた論文, フーリエ係数を求める為に必要な議論を行った論文等を幾つか発表されております.

また, 小関先生のお仕事に少なからず関係していると思われる種数 3 のジーゲルモジュラ形式環の問題や, アイゼンシュタイン級数のフーリエ係数の問題については, [14], [4] の結果が知られています.

3. 論文 [1] について. 論文 [1] において符号に関連して, ある種類の重み多項式のなす環を決定したので報告します.

言葉の定義をします.

\mathbb{F}_2^n の部分空間 D に対して

$$\|D\| = \#\{i; \exists v \in D, v_i \neq 0\}$$

とおきます.

二元線型符号 C に対して r 番目の一般化されたハミング重さ $d_r(C)$ は

$$d_r(C) = \text{Min}\{\|D\|; D \text{ は } C \text{ の次元 } r \text{ の部分空間}\}$$

で定義されますが, ここでは特に必要ではありません.

符号 C に対して次のような斉次多項式 (r -th higher weight enumerator) を定義します:

$$H_C^{(r)}(x, y) = \sum_{D \subset C, \dim D=r} x^{n-\|D\|} y^{\|D\|}.$$

全ての自己双対重偶符号 C の $H_C^{(k)}(x, y)$, $0 \leq k \leq r$, 達で \mathbb{C} 上生成される環 $\mathfrak{H}^{(r)}$ を考えます. この環を決定したいのですが, それには今まで研究されてきた別の斉次多項式を利用することにします.

¹小関先生は知っておられましたが, 論文 [9] の p.10, Table II の T_3 , $k = 10$ は 14980 0950573120 のミスプリントです.

符号 C に対して種数 g の重み多項式を

$$W_C^{(g)}(x_a) = W_C^{(g)}(x_a : a \in \mathbb{F}_2^g) = \sum_{v_1, \dots, v_g \in C} \prod_{a \in \mathbb{F}_2^g} x_a^{n_a(v_1, \dots, v_g)},$$

ここで $n_a(v_1, \dots, v_g)$ は $a = (v_{1i}, \dots, v_{gi})$ となるような i ($1 \leq i \leq n$) の数をあらわします。

長さ n の自己双対重偶符号の種数 g の重み多項式で生成される C 上の環を $\mathfrak{M}^{(g)}$ であらわします。第一章の後半部分にできた \mathfrak{M} は、種数が 1 の場合にあたります: $\mathfrak{M} = \mathfrak{M}^{(1)}$ 。 $\mathfrak{M}^{(g)}$ は一般種数に対して、ある有限群の不変式環と等しいことが知られています。具体的な結果については、次元公式については種数 4 まで、生成元等を含めた構造は種数 2 までの場合が知られています。 $\mathfrak{M}^{(1)}$ は代数的独立な二元 $W_{c_8}^{(1)}(x_a)$, $W_{g_{24}}^{(1)}(x_a)$ で生成されます。 $\mathfrak{M}^{(2)}$ は代数的独立な四元 $W_{c_8}^{(2)}(x_a)$, $W_{g_{24}}^{(2)}(x_a)$, $W_{d_{24}^+}^{(2)}(x_a)$, $W_{d_{10}^+}^{(2)}(x_a)$ と $W_{d_{32}^+}^{(2)}(x_a)$ で生成されます。 $W_{d_{32}^+}^{(2)}(x_a)$ の二乗は代数的独立な四元の多項式としてあらわされます。 $\mathfrak{M}^{(2)}$ の構造は先にも述べましたように、論文 [6] の THEOREM を応用して得られた結果です (W. Duke [2])。 $\mathfrak{M}^{(2)}$ はある有限群の不変式環として理解することもできます。

符号に関連して、二つの斉次多項式 $H_C^{(r)}(x, y)$, $W_C^{(g)}(x_a)$ を定義した訳ですが、 $H_C^{(r)}(x, y)$ は二変数であるのに対し、 $W_C^{(g)}(x_a)$ は 2^g -変数あります。そこで次のような変数の特殊化を行います:

$$x_a \longrightarrow \begin{cases} x, & a = 0 \in \mathbb{F}_2^g \text{ の場合,} \\ y, & \text{それ以外.} \end{cases}$$

この特殊化を行った $W_C^{(g)}(x_a)$ を $W_C^{(g)}(x, y)$ と書くことにしますと、 $H_C^{(r)}(x, y)$ との関係は次で与えられます:

$$W_C^{(g)}(x, y) = \sum_{0 \leq r \leq g} [g]_r H_C^{(r)}(x, y), \quad (3)$$

ここで $1 \leq g \leq \dim C$, $[g]_0 = 1$, $[g]_r = (2^g - 1)(2^g - 2) \cdots (2^g - 2^{r-1})$ ($r \geq 1$) です。実際、

$$\begin{aligned}
W_C^{(g)}(x, y) &= \sum_{v_1, \dots, v_g \in C} x^{n_0(v_1, \dots, v_g)} y^{n - n_0(v_1, \dots, v_g)} \\
&= \sum_{r=0}^g \sum_{\substack{v_1, \dots, v_g \in C \\ \dim(v_1, \dots, v_g) = r}} [g]_r x^{n_0(v_1, \dots, v_g)} y^{n - n_0(v_1, \dots, v_g)} \\
&= \sum_{r=0}^g \sum_{\substack{D \subseteq C \\ \dim D = r}} \#\{(v_1, \dots, v_g) \in C^g; \langle v_1, \dots, v_g \rangle = D\} \\
&\quad \times x^{n_0(v_1, \dots, v_g)} y^{n - n_0(v_1, \dots, v_g)} \\
&= \sum_{r=0}^g \sum_{\substack{D \subseteq C \\ \dim D = r}} [g]_r x^{n_0(v_1, \dots, v_g)} y^{n - n_0(v_1, \dots, v_g)} \\
&= \sum_{r=0}^g [g]_r \sum_{\substack{D \subseteq C \\ \dim D = r}} x^{n - \|D\|} y^{\|D\|} \\
&= \sum_{r=0}^g [g]_r H_C^{(r)}(x, y),
\end{aligned}$$

すなわち (3) が得られます。

この公式を利用して、 $W_C^{(g)}(x_a)$ の持つ性質を $H_C^{(r)}(x, y)$ の性質へと翻訳することができますが、ここでは省略します。

低い g について計算してみますと、

$$\begin{aligned}
W_C^{(1)}(x, y) &= H_C^{(0)}(x, y) + H_C^{(1)}(x, y), \\
W_C^{(2)}(x, y) &= H_C^{(0)}(x, y) + 3H_C^{(1)}(x, y) + 6H_C^{(2)}(x, y), \\
W_C^{(3)}(x, y) &= H_C^{(0)}(x, y) + 7H_C^{(1)}(x, y) + 42H_C^{(2)}(x, y) + 168H_C^{(3)}(x, y)
\end{aligned}$$

が得られます。

簡単な例をあげます。符号の長さを n としますと、常に $H_C^{(0)}(x, y) = x^n$ となります。また、これから $\mathfrak{h}^{(0)} = C[x^8]$ であることが分かります。拡張されたハミング符号 e_8 については、

$$H_{e_8}^{(1)}(x, y) = W_{e_8}^{(1)}(x, y) - H_{e_8}^{(0)}(x, y) = 14x^4y^4 + y^8$$

となります。

$\mathfrak{h}^{(r)}$ の構造について考えていきます。

上で述べましたように、 $\mathfrak{h}^{(0)} = C[x^8]$ です。

さて、 $\mathfrak{h}^{(1)}$ についてですが、

$$\begin{aligned}
X_8 &= H_{e_8}^{(0)}(x, y), \quad Y_8 = H_{e_8}^{(1)}(x, y), \\
X_{24} &= H_{e_8}^{(1)}(x, y) = 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}
\end{aligned}$$

とし、これらで生成される C 上の環を \mathfrak{R} とします。ここで X_8, Y_8, X_{24} の添字は齊次多項式としての次数をあらわしています ($\mathfrak{h}^{(2)}$ の時も同じような書き方をします)。この時、 $\mathfrak{h}^{(1)}$ は \mathfrak{R} と一致します。実際、 $\mathfrak{h}^{(1)} \supset \mathfrak{R}$ は明かなので、逆を示します。任意の自己双対重偶符号 C の重み多項式 $W_C^{(1)}(x, y)$ は、 $\mathfrak{W}^{(1)} = C[W_{c_8}^{(1)}(x, y), W_{g_{24}}^{(1)}(x, y)]$ という事実より、ある二変数多項式 $P(*, *)$ を用いて $W_C^{(1)}(x, y) = P(W_{c_8}^{(1)}(x, y), W_{g_{24}}^{(1)}(x, y))$ としてあらわすことができます。ところで (3) より

$$\begin{aligned} H_C^{(1)} &= W_C^{(1)}(x, y) - H_C^{(0)}(x, y) \\ &= P(W_{c_8}^{(1)}(x, y), W_{g_{24}}^{(1)}(x, y)) - x^n \\ &= P(X_8 + Y_8, X_8^3 + X_{24}) - X_8^{n/8} \\ &= \tilde{P}(X_8, Y_8, X_{24}) - X_8^{n/8} \quad (\tilde{P}(*, *, *) \text{ はある三変数多項式}) \end{aligned}$$

となるので、 $H_C^{(1)}$ は \mathfrak{R} の元であることが分かります。つまり $\mathfrak{h}^{(1)} = \mathfrak{R}$ が言えました。

後は、Gröbner 基底の理論を使って計算しますと、

$$\mathfrak{h}^{(1)} = C[X_8, Y_8](1 \oplus X_{24}), \quad X_8, Y_8 \text{ は代数的独立}$$

ということが分かります。

同様な方法で、 $\mathfrak{h}^{(2)}$ の場合も考えることができます。

$$\begin{aligned} X_8, Y_8, X_{24} &\text{ は } \mathfrak{h}^{(1)} \text{ の時と同じ,} \\ Z_8 &= H_{c_8}^{(2)}(x, y), \quad Y_{24} = H_{g_{24}}^{(2)}(x, y) \end{aligned}$$

とおきますと、

$$\mathfrak{h}^{(2)} = C[X_8, Y_8](1 \oplus Z_8 \oplus Z_8^2 \oplus Z_8^3) \oplus C[X_8]X_{24} \oplus C[X_8]Y_{24}$$

が得られます。

我々の論文 [1] の中で議論されているもう一つの関係式を述べます。

\mathbb{F}_2^g の元 v_1, \dots, v_g , 及び \mathbb{F}_2^g の部分空間 F に対して、 $P_F(v_1, \dots, v_g)$ という記号は全ての i に対して $(v_{1i}, \dots, v_{gi}) \in F$ である、を意味するとします。この時、

$$\begin{aligned} [g]_g H_C^{(g)}(x, y) &= W_C^{(g)}(x, y) + \sum_{\substack{F \subset \mathbb{F}_2^g \\ \dim F = g-1}} W_C^{(g)} \left(x_a \mapsto \begin{cases} x & a = 0 \in \mathbb{F}_2^g \\ y & a \in F \setminus \{0\} \\ 0 & \text{それ以外} \end{cases} \right) \\ &- \sum_{v_1, \dots, v_g \in C} (\#\{F \subset \mathbb{F}_2^g; \dim F = g-1, P_F(v_1, \dots, v_g)\} - 1) x^{n_0(v_1, \dots, v_g)} y^{n - n_0(v_1, \dots, v_g)} \end{aligned}$$

が成り立ちます。特に $g = 2$ の場合は、

$$6H_C^{(2)}(x, y) = W_C^{(2)}(x, y, y, y) - W_C^{(2)}(x, 0, 0, y) - W_C^{(2)}(x, 0, y, 0) - W_C^{(2)}(x, y, 0, 0) + 2x^n$$

となります。

この講演に関連して、横山和弘先生(九州大)には Gröbner 基底について、桂田英典先生(室蘭工大)には小関先生のお仕事についての話を伺いました。また、原田昌晃先生(山形大)からはこの原稿に対するコメントを頂きました。どうもありがとうございました。

参考文献

- [1] Dougherty, S., Gulliver, A., Oura, M., Higher weights and graded rings for binary self-dual codes, preprint.
- [2] Duke, W., On codes and Siegel modular forms, Inter. Math. Res. Notices, No. 5 (1993), 125-136.
- [3] Igusa, J., On Siegel modular forms of genus two, Amer. J. Math. **84** (1962), 175-200; (II), *ibid.*, **86** (1964), 392-412.
- [4] Katsurada, H., An explicit formula for Siegel series, Amer. J. Math. **121** (1999), 415-452.
- [5] Ozeki, M., On modular forms whose Fourier coefficients are non-negative integers with the constant term unity, Math. Ann. **206** (1973), 187-203.
- [6] Ozeki, M., On basis problem for Siegel modular forms of degree 2, Acta Arithmetica, **31** (1976), 17-30.
- [7] Ozeki, M., On a relation satisfied by Fourier coefficients of theta-series of degree one and two, Math. Ann. **222** (1976), 225-228.
- [8] Ozeki, M., On a property of Siegel theta-series, Math. Ann. **228** (1977), 249-258.
- [9] Ozeki, M., Washio, T., An extended table of the Fourier coefficients of Eisenstein series of degree two. Bull. Fac. Lib. Arts, Nagasaki Univ., Nat. Sci. **23**, No.1 (1982), 1-16. Corrigenda **23**, No.2, 16 (1983).

- [10] Ozeki, M., Washio, T., Table de coefficients Fourieriens des series d'Eisenstein de degre deux, II, Bull. Fac. Lib. Arts, Nagasaki Univ., Nat. Sci. 23, No.2 (1983), 1-15.
- [11] Ozeki, M., Washio, T., Explicit formulas for the Fourier coefficients of Eisenstein series of degree 3, J. Reine Angew. Math. 345 (1983), 148-171.
- [12] Ozeki, M., Washio, T., Table of the Fourier coefficients of Eisenstein series of degree 3, Proc. Japan Acad., Ser. A 59 (1983), 252-255.
- [13] Runge, B., Codes and Siegel modular forms, Discrete Math. 148 (1996), 175-204.
- [14] Tsuyumine, S., On Siegel modular forms of degree three, Amer. J. Math. 108 (1986), 755-862. Addendum (1986), 1001-1003.

McKay's 40 dimensional even unimodular lattice as ternary code construction

小関 道夫
山形大学理学部

3. July, 2001

1 Definition of the McKay's lattice M_{40}

Let p be a prime such that $p \equiv -1 \pmod{4}$, and H be a Hadamard matrix of order $p+1$ of the form: $H = S - I$ and S is a skew-symmetric matrix. We put $n = 2(p+1) = 8k$. Let M_n be the lattice in \mathbb{R}^n generated by the rows of the matrix

$$\frac{1}{\sqrt{k+1}} \begin{pmatrix} (k+1)I & O \\ S-2I & I \end{pmatrix}.$$

The Gram matrix of M_n is

$$\frac{1}{(k+1)} \begin{pmatrix} (k+1)I & O \\ S-2I & I \end{pmatrix} \begin{pmatrix} (k+1)I & S-2I \\ O & I \end{pmatrix} = \begin{pmatrix} (k+1)I & -S-2I \\ S-2I & 4I \end{pmatrix}.$$

Therefore M_n are even unimodular lattices of dimension n ($n = 16, 24, 40, \dots$). Especially

$$M_{40} = \frac{1}{\sqrt{6}} \begin{pmatrix} 6I & O \\ S-2I & I \end{pmatrix}.$$

In SPLAG p.221 Conway and Sloane give a slightly changed generator matrix of M_{40} by negating the first column of the second half in the original generator matrix

$$M_{40}: \frac{1}{\sqrt{6}} \begin{pmatrix} 6I & O \\ B & I \end{pmatrix},$$

where B is given in the same page of SPLAG.

2 Interpretation of M_{40} as a ternary code construction

It is easy to see that M_{40} contains the following shape of vectors

$$\mathbf{g}_i = \frac{1}{\sqrt{6}} (0, \dots, 0, \overset{i}{6}, 0, \dots, 0) \quad 1 \leq i \leq 40,$$

and

$$h_i = \frac{1}{\sqrt{6}} (3, 0, \dots, 0, \overset{i}{3}, 0, \dots, 0, \overset{21}{3}, 0, \dots, 0, \overset{20+i}{3}, 0, \dots, 0) \quad 2 \leq i \leq 20.$$

the lattice J_{40} generated by the vectors $\pm g_i$ ($1 \leq i \leq 40$) and $\pm h_i$ ($2 \leq i \leq 20$) is proved to be isometric to the scaled root lattice $D_{40}^{\sqrt{3}}$ with the scaling factor $\sqrt{3}$. We form a system of mutually orthogonal 3-vectors (norm 3 vector) :

$$\begin{aligned} f_1 &= \frac{1}{\sqrt{6}} (3, 0, \dots, 0, \overset{21}{3}, 0, \dots, 0), & f_2 &= \frac{1}{\sqrt{6}} (3, 0, \dots, 0, \overset{21}{-3}, 0, \dots, 0), \\ f_3 &= \frac{1}{\sqrt{6}} (0, 3, 0, \dots, 0, \overset{22}{3}, 0, \dots, 0), & f_4 &= \frac{1}{\sqrt{6}} (0, 3, 0, \dots, 0, \overset{22}{-3}, 0, \dots, 0), \\ & & & \vdots \\ f_{39} &= \frac{1}{\sqrt{6}} (0, \dots, 0, \overset{20}{3}, 0, \dots, 0, 3), & f_{40} &= \frac{1}{\sqrt{6}} (0, \dots, 0, \overset{20}{-3}, 0, \dots, 0, 3) \end{aligned}$$

Remark 1 The vectors $\pm f_i \pm f_j$ generate J_{40} , but each $f_i \notin M_{40}$. We see that $f_1 + f_2 = g_1, f_3 + f_4 = g_2, \dots, f_{39} + f_{40} = g_{20}, f_1 - f_2 = g_{21}, f_3 - f_4 = g_{22}, \dots, f_{39} - f_{40} = g_{40}$.

Here we express each row of the generator matrix of M_{40} by means of f_1, \dots, f_{40} . We have already done with g_1, \dots, g_{20} .

The 21st row x_1 has the shape

$$x_1 = \frac{1}{\sqrt{6}} (2, \overbrace{1, \dots, 1}^{20}, \overbrace{0, \dots, 0}^{19}).$$

It is verified that the equation

$$x_1 = \frac{1}{6} (3f_1 + f_2 + \dots + f_{40})$$

holds. The 22nd row x_2 is expressed as

$$x_2 = \frac{1}{6} (f_1 + f_2 - f_3 - 3f_4 + f_5 + f_6 - f_7 - f_8 - f_9 - f_{10} + f_{11} + f_{12} + f_{13} + f_{14} + f_{15} + f_{16} + f_{17} + f_{18} - f_{19} - f_{20} + f_{21} + f_{22} - f_{23} - f_{24} + f_{25} + f_{26} - f_{27} - f_{28} - f_{29} - f_{30} - f_{31} - f_{32} - f_{33} - f_{34} + f_{35} + f_{36} + f_{37} + f_{38} - f_{39} - f_{40})$$

From x_3 till x_{20} they are produced from x_2 by twice cyclic shift process of the coordinates 3 to 40. For instance

$$x_3 = \frac{1}{6} (f_1 + f_2 - f_3 - f_4 - f_5 - 3f_6 + f_7 + f_8 - f_9 - f_{10} - f_{11} - f_{12} + \dots).$$

Consider the lattice K_{40} generated by J_{40} and $2x_j$ ($2 \leq j \leq 40$). Combining the arguments and theorem in our 1989 paper [5] we can prove

Theorem 1 The quotient K_{40}/J_{40} is isomorphic to a ternary self-dual $[40, 20, 12]$ code whose

19840	$(1_{39} 0)$	<i>total</i>
3972	$(1_{20} (-1)_{19} 0)$	
228	$(1_{21} (-1)_{18} 0)$	
2052	$(1_{22} (-1)_{17} 0)$	
2223	$(1_{23} (-1)_{16} 0)$	
684	$(1_{24} (-1)_{15} 0)$	
684	$(1_{25} (-1)_{14} 0)$	
19	$(1_{26} (-1)_{13} 0)$	
57	$(1_{27} (-1)_{12} 0)$	
1	$(1_{28} (-1)_{11} 0)$	
	$(1_{29} (-1)_{10} 0)$	
	$(1_{30} (-1)_{9} 0)$	
	$(1_{31} (-1)_{8} 0)$	
	$(1_{32} (-1)_{7} 0)$	
	$(1_{33} (-1)_{6} 0)$	
	$(1_{34} (-1)_{5} 0)$	
	$(1_{35} (-1)_{4} 0)$	
	$(1_{36} (-1)_{3} 0)$	
	$(1_{37} (-1)_{2} 0)$	
	$(1_{38} (-1)_{1} 0)$	
	$(1_{39} 0)$	
<i>number</i>		

From the codewords we get lattice vectors in $\Lambda_4(M_{40})$ first by viewing the components as elements in \mathbb{Z} and then by multiplying the factor $\frac{1}{\sqrt{3}}$. We also exhibit the shapes of the codewords of weight 39 in C as a table

19760	$(1_{12} 0_{28})$	<i>total</i>
19	$(1_{10} (-1)_{12} 0_{28})$	
57	$(1_{10} (-1)_{10} 0_{28})$	
2280	$(1_{13} (-1)_{9} 0_{28})$	
1539	$(1_{14} (-1)_{8} 0_{28})$	
1368	$(1_{15} (-1)_{7} 0_{28})$	
9234	$(1_{16} (-1)_{6} 0_{28})$	
	$(1_{17} (-1)_{5} 0_{28})$	
	$(1_{18} (-1)_{4} 0_{28})$	
	$(1_{19} (-1)_{3} 0_{28})$	
	$(1_{20} (-1)_{2} 0_{28})$	
	$(1_{21} (-1)_{1} 0_{28})$	
	$(1_{22} 0_{28})$	
<i>number</i>		

We exhibit the shapes of the codewords of weight 12 in C as a table (ternary field \mathbb{F}_3 consists of $0, 1, -1$):

$$|C_4| + |C_{39}| = 39600 = |\Lambda_4(M_{40})|$$

To each codeword in C_{12} there corresponds unique vector in $\Lambda_4(M_{40})$. We can also show that to each codeword in C_{39} there corresponds unique vector in $\Lambda_4(M_{40})$. These facts match with the equation

$$|C_4| = 19760, |C_{39}| = 19840.$$

and

$$|\Lambda_4(M_{40})| = 39600,$$

we know that

C_{12} (resp. C_{39}) : the set of codewords of weight 12 (resp. 39) .

The lattice vectors are given by

$$\frac{1}{\sqrt{12}} \times \begin{cases} (1^{39} 3) & ((-1)^{39} - 3) & 1 \\ (1^{28} (-1)^{11} - 3) & (1^{11} (-1)^{28} 3) & 57 \\ (1^{27} (-1)^{12} 3) & (1^{12} (-1)^{27} - 3) & 19 \\ (1^{26} (-1)^{13} - 3) & (1^{13} (-1)^{26} 3) & 684 \\ (1^{25} (-1)^{14} 3) & (1^{14} (-1)^{25} - 3) & 684 \\ (1^{23} (-1)^{16} 3) & (1^{16} (-1)^{23} - 3) & 2223 \\ (1^{22} (-1)^{17} - 3) & (1^{17} (-1)^{22} 3) & 2052 \\ (1^{21} (-1)^{18} 3) & (1^{18} (-1)^{21} - 3) & 228 \\ (1^{20} (-1)^{19} - 3) & (1^{19} (-1)^{20} 3) & 3972 \end{cases}$$

4 How to distinguish ternary code construction from binary code construction

4.1 Appealing to the analytic invariants of the lattices

Such as Siegel theta series or Jacobi theta series.

To compute analytic invariants it is necessary to know the values of the inner product between many vectors in the lattice. In the case when the lattice is constructed from the code the knowledge from the combinatorial polynomials are of great help for that purpose. Let L be an even unimodular lattice of dimension n ($n \equiv 0 \pmod{8}$). Theta series for the lattice L is by definition

$$\theta(\tau, L) = \sum_{\mathbf{x} \in L} e^{\pi i(\mathbf{x}, \mathbf{x})\tau},$$

where $\tau \in H = \{\tau \in \mathbb{C} | \text{Im}(\tau) > 0\}$

Theta series associated with the extremal even unimodular lattices of rank 40 is

$$\theta_{40} = 1 + 39600q^2 + 87859200q^3 + 20779902000q^4 + \dots,$$

$q = e^{2\pi\tau}$. Since theta series is unique for the extremal even unimodular lattices of rank 40, it does not serve for our present problem.

Let Λ_{2m} be the set of vectors \mathbf{x} in L such that $(\mathbf{x}, \mathbf{x}) = 2m$ holds. For any $\mathbf{y} \in \Lambda_{2m}$ Jacobi theta series of index m is defined to be

$$\theta_{\mathbf{y}, L} = \sum_{\mathbf{x} \in L} e^{\pi i((\mathbf{x}, \mathbf{x})\tau + 2(\mathbf{x}, \mathbf{y})z)},$$

here $z \in \mathbb{C}$.

Fact: Any Jacobi theta series of weight 20 and index 2 associated with an extremal lattice of rank 40 is expressed as $\theta_{40,2} + \alpha\Psi$, where

$$\theta_{40,2} = 1 + q^2(t^4 + 7904t + 23790) + q^3(7904t^3 + 1525056t^2 + 20186400t + 44420480) + \dots$$

and

$$q^2(t^2 - 4t + 6) + q^3(-4t^3 - 24t^2 + 132t - 208) + \dots$$

Here $\zeta = e^{2\pi iz}$, $t^i = \zeta^i + \zeta^{-i}$, $i = 1, 2, \dots$. $\alpha = \#\{x \in \Lambda_4 \mid (x, y) = 2\}$, $7904 - 4\alpha = \#\{x \in \Lambda_4 \mid (x, y) = 1\}$, $23790 + 6\alpha = \#\{x \in \Lambda_4 \mid (x, y) = 0\}$.

Lattices coming from Binary codes

We give the results of computing of Jacobi theta series of index, where the lattices coming from binary codes. However we do not give the process of the computation, nor we give the generator matrix of the binary codes used here. The reader may consult [4].

Ex. 1 L_1

1-(i) There are 36560 $y \in \Lambda_4(L_1)$ with

$$\begin{aligned} \theta_{y, L_1} &= \theta_{40,2} + 152\Psi \\ &= 1 + q^2(t^4 + 152t^2 + 7296t + 24702) + \dots \end{aligned}$$

1-(ii) There are 1520 $y \in \Lambda_4(L_1)$ with

$$\begin{aligned} \theta_{y, L_1} &= \theta_{40,2} + 440\Psi \\ &= 1 + q^2(t^4 + 440t^2 + 6144t + 26430) + \dots \end{aligned}$$

1-(iii) There are 1520 $y \in \Lambda_4(L_1)$ with

$$\begin{aligned} \theta_{y, L_1} &= \theta_{40,2} + 536\Psi \\ &= 1 + q^2(t^4 + 536t^2 + 3760t + 27006) + \dots \end{aligned}$$

Ex. 2. L_2

2-(i) There are 20480 $y \in \Lambda_4(L_2)$ with $\theta_{y, L_2} = \theta_{40,2} + 152\Psi$

2-(ii) There are 15360 $y \in \Lambda_4(L_2)$ with $\theta_{y, L_2} = \theta_{40,2} + 248\Psi$

2-(iii) There are 3440 $y \in \Lambda_4(L_2)$ with $\theta_{y, L_2} = \theta_{40,2} + 440\Psi$

2-(iv) There are 320 $y \in \Lambda_4(L_2)$ with $\theta_{y, L_2} = \theta_{40,2} + 824\Psi$

Ex. 3. L_3

3-(i) There are 30720 $y \in \Lambda_4(L_3)$ with $\theta_{y, L_3} = \theta_{40,2} + 248\Psi$

3-(ii) There are 8720 $y \in \Lambda_4(L_3)$ with $\theta_{y, L_3} = \theta_{40,2} + 440\Psi$

3-(iii) There are 160 $y \in \Lambda_4(L_3)$ with $\theta_{y, L_3} = \theta_{40,2} + 160\Psi$

Ex. 4. L_4

4-(i) There are 38400 $y \in \Lambda_4(L_4)$ with $\theta_{y, L_4} = \theta_{40,2} + 376\Psi$

4-(ii) There are 1200 $y \in \Lambda_4(L_4)$ with $\theta_{y, L_4} = \theta_{40,2} + 952\Psi$

A Lattice coming from Ternary code

Of course we are going to treat the ternary code studied in the preceding sections. Modified Jacobi polynomials associated with codewords u of weight 12 or 39 in McKay [40, 20, 12] ternary self-dual code C_{Mc} .

Definition:

$$MJ(C_{Mc}, u, X, Y, Z) = \sum_{v \in C_{Mc}} X^{wt(v)} Y^{n \cdot 1 - v} Z^{n \cdot 2 - v}.$$

Here $u * v = \#\{i \mid u_i = v_i\}$ for $2 \leq i \leq 40$ and $u * v = \#\{i \mid u_i = 1, v_i = 2\}$.
 $2, v_i = 1 \leq i \leq 40$ for $u = (u_1, u_2, \dots, u_{40}), v = (v_1, v_2, \dots, v_{40}) \in GF(3)^{40}$.

(I) For 1520 of codewords u of weight 12 we have

$$MJ(C_{Mc}, u, X, Y, Z) = 1 + X_{12} \{Y_{12} + Z_{12} + 54Y^4Z^4 + 216(Y^6 + Z^6) + 1584Y^3Z^3 + 1152(Y^4Z + YZ^4) + 6534Y^2Z^2 + 1920(Y^3 + Z^3) + 4704YZ + 306\} + \dots + X_{39} \{56(Y_{12} + Z_{12}) + 1920(Y^9Z^3 + Y^3Z^9) + 9936Y^6Z^6\} + 168(Y_{10}Z + YZ_{10}) + 2808(Y^7Z^4 + Y^4Z^7)\}$$

(II) For 4560 of codewords u of weight 12 we have

$$MJ(C_{Mc}, u, X, Y, Z) = 1 + X_{12} \{Y_{12} + Z_{12} + 42Y^4Z^4 + 108(Y^5Z^2 + Y^2Z^5) + 72(Y^6 + Z^6) + 1236Y^3Z^3 + 1512(Y^4Z + YZ^4) + 6138Y^2Z^2 + 2028(Y^3 + Z^3) + 4572YZ + 330\} + \dots + X_{39} \{20(Y_{12} + Z_{12}) + 2208(Y^9Z^3 + Y^3Z^9) + 9432Y^6Z^6\} + 96(Y_{10}Z + YZ_{10}) + 2880(Y^7Z^4 + Y^4Z^7)\}$$

(III) For 13680 of codewords u of weight 12 we have

$$MJ(C_{Mc}, u, X, Y, Z) = 1 + X_{12} \{Y_{12} + Z_{12} + 48Y^4Z^4 + 108(Y^5Z^2 + Y^2Z^5) + 72(Y^6 + Z^6) + 1212Y^3Z^3 + 1512(Y^4Z + YZ^4) + 6174Y^2Z^2 + 2028(Y^3 + Z^3) + 4548YZ + 336\} + \dots + X_{39} \{20(Y_{12} + Z_{12}) + 2208(Y^9Z^3 + Y^3Z^9) + 9432Y^6Z^6\} + 96(Y_{10}Z + YZ_{10}) + 2880(Y^7Z^4 + Y^4Z^7)\}$$

(IV) For 18320 of codewords u of weight 39 we have

$$MJ(C_{Mc}, u, X, Y, Z) = 1 + X_{12} \{19Y_{12} + 19Z_{12} + 2208(Y^9Z^3 + Y^3Z^9) + 9378Y^6Z^6\} + 93(Y_{10}Z + YZ_{10}) + 2871(Y^7Z^4 + Y^4Z^7)\} + \dots + X_{39} \{Y_{39} + Z_{39} + 19(Y_{12}Z_{27} + Z_{27}Y_{12}) + 36(Y_{24}Z_{15} + Y_{15}Z_{24})\}$$

$$192(\gamma_{21}Z_{18} + \gamma_{18}Z_{21}) + 93(\gamma_{28}Z_{10} + \gamma_{10}Z_{28}) \\ 1224(\gamma_{25}Z_{13} + \gamma_{13}Z_{25}) + 4455(\gamma_{22}Z_{16} + \gamma_{16}Z_{22}) + 7800\gamma_{19}Z_{19}$$

(IV) For 1520 of codewords u of weight 39 we have

$$MJ(C_{M_{40}}, \mathbf{n}, X, \gamma, Z) = \\ 1 + X_{12}\{67\gamma_{12} + 19Z_{12} + 1800(\gamma_9 Z_3 + \gamma_3 Z_9) + 10098\gamma_6 Z_6 \\ + 201(\gamma_{10}Z + \gamma Z_{10}) + 2763(\gamma^7 Z^4 + \gamma^4 Z^7)\} \\ + \dots + X_{39}\{\gamma_{39} + Z_{39} + 67(\gamma_{12}Z_{27} + \gamma_{27}Z_{12}) + \\ 180(\gamma_{21}Z_{18} + \gamma_{18}Z_{21}) + 201(\gamma_{28}Z_{10} + \gamma_{10}Z_{28}) \\ 1080(\gamma_{25}Z_{13} + \gamma_{13}Z_{25}) + 3843(\gamma_{22}Z_{16} + \gamma_{16}Z_{22}) + 9096\gamma_{19}Z_{19}\}$$

$$\sum_{v \in C} X_{w(v)} \gamma_{u^* v} Z_{u^* v} / u^* v / u^* v / \gamma_{v^* u} Z_{v^* u}$$

where $u^* v = \#\{i \mid u_i = 1, v_i = 0\} \leq 40$, $u^* v = \#\{i \mid u_i = 2, v_i = 0\} \leq 40$, $\ell_2(v) = \#\{i \mid v_i = 2, 1 \leq i \leq 40\} \bmod 2$.
With the help of these polynomials we compute that

(1) there are 18240 vectors $y \in \Lambda_4(M_{40})$ coming from codewords of weight 12 which lead Jacobi theta series of index 2 of the form :

$$\theta_{40,2} + 128\psi = 1 + q^1(t^4 + 128t^2 + 7392t + 24558) + \dots,$$

and (11) there are 1520 vectors $y \in \Lambda_4(M_{40})$ coming from codewords of weight 12 which lead Jacobi theta series of index 2 of the form :

$$\theta_{40,2} + 272\psi = 1 + q^1(t^4 + 272t^2 + 6816t + 25422) + \dots$$

We have not determined Jacobi theta series of index 2 coming from codewords of weight 39. When we have completed the computations in this case, we may judge that the lattice M_{40} is not equivalent to the lattice coming from the binary codes.
In fact comparing the examples 1 to 4 in this section with the computations of M_{40} we can say these lattices are not equivalent to each other.

4.2 By using the geometric configuration

We are not content with the examples in the preceding subsection. We want to show that even unimodular extremal lattices coming from ternary self-dual codes are never equivalent to the even unimodular extremal 40 dimensional lattices coming from binary self-dual extremal codes.

For this the following remark would be an important clue .

If an even unimodular extremal 40 dimensional lattice L_0 comes from a binary self-dual extremal code, then by construction L_0 must contain a sublattice \mathcal{D}_{40} isometric to the scaled root lattice $D_{40}^{\sqrt{2}}$. If we take an element $y \in \mathcal{D}_{40}$, (note that $(y, y) = 4$) then Jacobi theta series of index 2 θ_{y, L_0} associated with y and L_0 must have the shape : $\theta_{40,2} + \alpha\Psi$ with $\alpha \geq 152$, and such α exist at least 3120 in number.

If we could show that a totality of Jacobi theta series of index 2 associated with each even unimodular extremal 40 dimensional lattice coming from ternary self-dual code has not this property, then we would attain our objective.

It would be a closing time to report an unsubmitted work before going too much further.

References

- [1] J.H. Conway and N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag 1988. Third Edition (1998)
- [2] M. Eichler and D. Zagier, The Theory of Jacobi Forms, Birkhäuser, 1985
- [3] F.J. MacWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes", North-Holl and, Amsterdam, 1977.
- [4] M. Ozeki, Examples of even unimodular extremal lattices of rank 40 and their Siegel theta-series of degree 2, J. Number Th. **28** (1988) 119-131
- [5] M. Ozeki, Ternary code construction of even unimodular lattices, in Théorie des nombres. Quebec 1987, Gruyter, Berlin, (1989) 772-784
- [6] M. Ozeki, Mckay's even unimodular 40 dimensional lattice as a ternary construction, in preparation 2001
- [7] E.M. Rains and N.J.A.Sloane, Self-Dual Codes, in Handbook of Coding Theory V. Pless (ed), North-Holland (1998)

テンソル積加群とモジュラー変換

宮本雅彦 (筑波大学)

平成13年7月3日

1 序文

頂点作用素代数 (VOA) は無限次元空間上に無限個の演算を持つ代数です。それ故、色々な不思議な性質を示すことが知られています。この講演では、一つの加群からすべての既約加群を構成したり、加群のテンソル積加群を実際に頂点作用素まで含めて構成する方法を紹介します。しかも、この方法により、テンソル積加群と相対加群がモジュラー群を通して関係していることを紹介します。

一般に U をベクトル空間とし、 $\text{End}(U)$ の元 v_n を係数とする形式的べき級数

$$v(z) = \sum_{n \in \mathbb{Z}} v_n z^{-n-1}$$

が量子作用素 (quantum operator または weakly vertex operator) であるとは、任意の $u \in U$ に対して $N \in \mathbb{N}$ があって

$$v_n u = 0 \quad \text{for } n > N$$

を満たしているものです。

この量子作用素全体は n -th 正規積 ($n \in \mathbb{Z}$) と呼ばれる次の演算

$$a(z) \times_n b(z) = \text{Res}_w \{ (w-z)^n a(w)b(z) - (-z+w)^n b(z)a(w) \}$$

によって無限個の演算を持つ代数となっています。

また、 U, W を2つのベクトル空間とし、 $\text{Hom}(U, W)$ の元 b_r ($r \in \mathbb{R}$) を係数に持つ形式的べき級数

$$b(z) = \sum_{r \in \mathbb{R}} b_r z^{-r-1}$$

に対して、 U 上と W 上の量子作用素

$$\begin{aligned} a^U(z) &\in \text{End}(U)[[z, z^{-1}]], \\ a^W(z) &\in \text{End}(W)[[z, z^{-1}]] \end{aligned}$$

の組

$$a(z) = (a^U(z), a^W(z))$$

による作用を、 n -正規積

$$a(z) \times_n b(z) = \text{Res}_w \{(w-z)^n a^W(w) b(z) - (-z+w)^n b(z) a^U(w)\}$$

によって定義することが出来ます。以下、 a^U も a^W も a で表していきます。

これらを成分（係数）で見ると、

$$(a_n b)_m = \sum_{i=0}^{\infty} \binom{n}{i} \{a_{n-i} b_{m+i} - (-1)^n b_{m+n-i} a_i\}$$

となっており、結合律と呼んでいます。

この正規積の成分表示が今日の話の中心で、重要なことは、展開の係数はあまり m が関係していないということです。

設定は $(V, Y(\cdot, z))$ を頂点作用素代数とし、 (U, Y^U) , (W, Y^W) , (X, Y^X) 等を V -加群とします。即ち、 $v \in V$ に対して、 V 上、 U (W, X) 上の量子作用素 $Y(v, z)$, $Y^U(v, z)$ ($Y^W(v, z), Y^X(v, z)$) が定義されています。特に、上の条件は満たしています。

また、タイプ $U: W \rightarrow X$ の交絡作用素 intertwining operator $I(*, z)$ も考えるわけですが、ここでも、 $u \in U$ に対して $\text{Hom}(W, X)$ の元 u_r を係数とする

$$I(u, z) = \sum_{r \in \mathbb{R}} u_r z^{-r-1} \in I(U: W \rightarrow X)$$

は、先の条件を満たしています。

頂点作用素代数の場合には、加群に次数が定義されており、加群 U の次数 r の斉次空間を U_r で表示します。ここで考える頂点作用素代数の加群はすべて斉次空間の直和に分解しています。

頂点作用素代数の既約加群 U 上の次数は、下に有界であり、その最小次数を t とすると、次数全体は $\{t, t+1, t+2, \dots\}$ の部分集合となっており、

$$U = \bigoplus_{n=0}^{\infty} U_{t+n}$$

と分解します。最小次数の空間（トップ加群）を $U(0)$ 、次を $U(1)$ など表し、全体で、

$$U = \bigoplus_{n=0}^{\infty} U(n)$$

と表示したりします。

$a \in U$ の次数が r の場合には、頂点作用素や交絡作用素

$$I(a, z) = \sum a_r z^{-r-1}$$

における a_{r-1} は常に次数を保つ作用であり、 a_{r-i-j} は次数を j 増やす作用となっています。

このことから、正規積

$$\begin{aligned} (a_n b)_m &= \sum_{i=0}^{\infty} \binom{n}{i} \{a_{n-i} b_{m+i} - (-1)^n b_{m+n-i} a_i\} \\ &= a_n b_m + n a_{n-1} b_{m+1} + \dots \\ &\quad - (-1)^n b_{m+n} a_0 - (-1)^n n b_{m+n-1} a_1 + \dots \end{aligned}$$

は i が 1 つずつ増えるに従って、2 つの作用の積で与えられている各項の右側の成分は次数を 1 つずつ多く下げている、同時に、左側の成分は次数を 1 つずつ多く上げています。

例えば、 $n < m+1$ とすると第一項の左の成分 a_n は次数を本当に上げる作用です。

U は V -加群ですから、一般に、一つの元 $u \in U$ は色々な U の元 u^i と V の元 v^j の積の形の和 $u = \sum v_n^i u^i$ としても表示できるわけであり、その表示に対して上の正規積を使えば、交絡作用素 $I(u, z) = \sum u_r z^{-r-1}$ の係数 u_r の方も色々な表示を持つことになります。

例えば $v \in V$ の元の次数を保つ作用 $o(v) = v_{wtv-1}$ を v のある積表示 $v = \sum_i v_i^1 \dots v_i^k 1$ を使って正規積により分解したときに、すべての項の右側に最初に次数を下げるような作用がくる表示を持つものような v 全体で張られる空間を $O(V)$ とおくと、 $v \in O(V)$ の元の加群 U の次数最小の空間 (トップ加群) への次数を保つ作用は常に 0 となるわけです。ツリー代数 $A(V)$ というのは、 $V/O(V)$ のことで、ツリー理論は逆にこれらが作用するものは、ある加群のトップ加群となっていると主張しているのです。即ち、正規積による分解が本質的であるということです。

これを拡張して、次数を保つ作用 $o(v)$ を正規積を使って分解したときにすべての項の右側に、次数を n 下げたまま作用の積が最初にくるような元 v 全体を $O_{n-1}(V)$ とすれば、同じ論法により、 $v \in O_{n-1}(V)$ の次数を保つ作用は、加群の最初の $U(0) \oplus U(1) \oplus \dots \oplus U(n-1)$ に 0 として作用していることが分かります。それ故、

$$A_{n-1}(V) = V/O_{n-1}(V)$$

は $\bigoplus_{i=0}^{n-1} U(i)$ に作用しています。この逆が成り立つというのが、Dong, Li, Mason たちによるツリー代数の拡張です。

では、ここで、頂点作用素の部分を交絡作用素で考えてみようというのがこの講演の出発点です。例えば、 $u \in U$ をとり、タイプ $U: W \rightarrow X$ の交絡作用素 $I(u, z) = \sum_{r \in \mathbb{R}} u_r$ を考え、 W のトップ加群 $W(0)$ から X のトップ加群 $X(0)$ への

写像となる係数 u_r を考えます。加群への頂点作用素の場合とは異なり、次数を保つとは限りません。この場合にも、 $u \in U$ の元を色々な V の元と U の元の積の和表示 $u = \sum_i v_{n_i}^i u^i$ と正規積による分解を使って、 u_r を作用の積の和の形に分解します。もし、ある分解において、すべての項が右側に次数を下げる作用を持つか、最後に次数を上げる作用を持っていれば、 u_r の $W(0)$ から $X(0)$ への写像はゼロになります。このような $u \in U$ 全体が張る空間を $O(U)$ とすると、これが、ズー代数 $A(V)$ の加群 $A(U) = U/O(U)$ を定義します。

定義から容易に、 $A(U)$ は $A(V) \otimes A(V)^{\text{op}}$ -両側加群であることが分かりますが、さらに、 V が有理型の場合には、左 $A(V)$ -加群として、

$$A(U) \otimes_{A(V)} W(0) = \sum_{X \text{ 既約加群}} N_{U,W}^X X(0)$$

が成り立つことが Frenkel-Zhu と Li によって示されています。ここで、 $N_{U,W}^X$ はタイプ $U:W \rightarrow X$ の交絡作用素の張る空間の次元を表しており、形式的な積の分解式（またはその係数）

$$U \times W = \sum N_{U,W}^X X$$

をフージョン規則と呼んでいます。頂点作用素代数が有理型（任意の加群が既約加群の直和）の場合には、 $\sum N_{U,W}^X X$ で一意的な加群 $\oplus_X N_{U,W}^X X$ を表すので、この加群の事をタイトルに出てくるテンソル積加群と呼んでいます。

今日の話の最初の結果は、この論法をトップ加群だけではなく、加群全体に対して適用し、加群としてのベクトル空間および、頂点作用素をすべて実際に求めることができるということです。

$a \in V, u \in U$ とすると、正規積

$$(a_n b)_m = a_n b_m + n a_{n-1} b_{m+1} + \dots \\ - (-1)^n b_{m+n} a_0 - (-1)^n n b_{n+m-1} a_1 + \dots$$

の右式の後半部分の成分をみると、最初の項の右には a_0 が必ず出てくるので、次数をいったんは $wt a - 1$ あげています。ではこの項を消去することを考えてみましょう。

$$\text{Res}_w(w+1)^p Y(a, w) b$$

と定義すると、後半部分から $b_{n+m-i} a_i$ ($i = 0, 1, \dots, p-1$) の項が消えます。例えば

$$\text{Res}_w(w+1)^{wt a + p} Y(a, w) b$$

を計算すると、右式の後半部分の項の右側は $a_{wt a - 1 + p + i}$ ($i = 1, \dots$) なので、次数をまず、 $p+1$ 以上上げるわけで、 $W(0) \oplus \dots \oplus W(p-1)$ から写像を出発させた場

合には右式の後半部分は 0 と考えてよいわけです。注意してほしいのは、この論法においては、 m は関係ないということです。

U の元 u で u_m を考えると、適当な正規積の展開から

($+s$ 以上次数を上げる作用) (intertwining operator)

の表示を持つような u 全体で張られる空間 $O_{s,*}(U)$ 、

(intertwining operator)(r 以上次数を下げる作用)

の表示を持つような u 全体で張られる空間 $O_{*,r}(U)$

$$O_{s,r}(U)$$

とおきます。これを使って、

$$\tilde{U}_{s,r} = (O_{s,*}(U) \cap O_{*,r}(U)) / (O_{s+1,*}(U) + O_{*,r+1}(U))$$

$$\tilde{U} = \bigoplus_{s=0, r=0}^{\infty} \tilde{U}_{s,r}$$

とおきます。

このような剰余空間を考えると言うことは、 U の相対空間

$$U^* = \text{Hom}(U, \mathbb{C})$$

の部分空間を考えるということになります。

では、 $v \in V$ の \tilde{U} への作用を定義しましょう。

$$\tilde{Y}(v, z) = \text{Res}_w \frac{1}{z} \delta\left(\frac{w+1}{z}\right) Y(v, w)$$

を考えます。

ここで、 $\delta(z) = \sum_{n \in \mathbb{Z}} z^n$ はデルタ関数で、

$$\delta(z) z^m = \delta(z)$$

という性質を持っています。

これと同じような表示ですが、次の 3 通りの定義を考えます。

$$\tilde{Y}^1(v, z) = \text{Res}_w \frac{1}{z} \delta\left(\frac{w+1}{z}\right) Y(v, w)$$

$$\tilde{Y}^2(v, z) = \text{Res}_w \frac{1}{z} \delta\left(\frac{w+1}{z}\right) \left\{ \left(\frac{w+1}{z}\right)^{wtv} Y(v, w) \right\}$$

$$\tilde{Y}^3(v, z) = \text{Res}_w \frac{1}{z} \delta\left(\frac{w+1}{z}\right) \left\{ \left(\frac{w+1}{z}\right)^N Y(v, w) \right\} \text{ for } N \gg 0.$$

ここで最後の式の N というのは、 $u \in O_{r,k}(U)$ に対しては

$$\tilde{Y}^3(v, z)u = \text{Res}_w \frac{1}{z} \delta\left(\frac{w+1}{z}\right) \left\{ \left(\frac{w+1}{z}\right)^N Y(v, w)u \right\} \quad \text{for } N > wv + k$$

ということです。 $\delta(z)z = \delta(z)$ ですが、 $\delta(z)$ を含む積は結合律が成り立つわけではないので、 \tilde{Y}^1, \tilde{Y}^2 と \tilde{Y}^3 はすべて異なります。

まず、もっとも重要な結果として、次の補題を得ます。

補題 1 \tilde{U} 上への頂点作用素 $\tilde{Y}^m(v, z)$ はすべて結合律を満たし、互いに局所可換である。

さらに、

$$\tilde{Y}^0(v, z) = \text{Res}_w \frac{1}{z} \delta\left(\frac{1+w}{z}\right) Y(v, w)$$

とおくと、これは交換律

$$[v_n, u_r] = \sum_{i=0}^{\infty} \binom{n}{i} (v_i u)_{n+r-i}$$

から出てくる作用素

$$\sum_{n \in \mathbb{Z}} \left(\sum_{i=0}^{\infty} \binom{n}{i} v_i \right) z^{-n-1}$$

に対応しており、次数を保つ作用の部分にはツーの変形作用素

$$Y[v, z] = \sum v[n] z^{-n-1}$$

の $v[0]$ と一致します。

定理 2 \tilde{U} 上に 2 つの頂点作用素:

$$\begin{aligned} Y^{left}(v, z) &= \tilde{Y}^3(v, z) \\ Y^{right}(v, z) &= \tilde{Y}^3(v, z) - Y^0(v, z) \end{aligned}$$

を定義すると、 \tilde{U} は $V \otimes V^{op}$ -加群となる。

一応、 V^{op} -加群の説明をしておきましょう。これは加群への頂点作用素は通常に加群への作用に似ていますが、作用の次数の増減は逆であり、正規積の順序が逆に

なるものです。例えば、 $(U, Y^U(*, z))$ を V -加群として、 U^* を制限相対加群とします。即ち、

$$U^* = \bigoplus_{n=0}^{\infty} (\text{Hom}(U(n), \mathbb{C}))$$

です。このとき、 $u^* \in U^*, u \in U$ に対して、

$$\langle Y^1(v, z)u^*, u \rangle = \langle u^*, Y^U(v, z)u \rangle$$

によって $Y^1(v, z)$ を定義すると、これが V^{op} -加群 (U^*, Y^1) を与えています。

$V \otimes V^{op}$ を考えるのは非常に自然なことです。元々、頂点作用素代数は 2次元共形場理論に対応する厳密な数学的対象と考えられるのですが、実際には 2次元共形場理論の左カイラル代数にすぎません。2次元共形場理論においては同時に左カイラル代数の作用と可換な右カイラル代数が出てくるのですが、ムーンシャイン頂点作用素代数の場合には、右カイラル代数は

$$(V^1)^{op}$$

です。しかも、 $V^1 \otimes (V^1)^{op}$ の全自己同型群は神秘的な関係で与えられるパイモンスタール群 $M \wr \mathbb{Z}_2$ になります。

定理 3 簡単のために、 V を有理型頂点作用素代数とし、フュージョン規則を

$$U \times W = \sum_T N_{U,W}^T T$$

とする。この時、 \tilde{U} は $V \otimes V^{op}$ -加群として、

$$\sum_{W,T} N_{U,W}^T T \otimes_{\mathbb{C}} W^{op}$$

と同型となる。特に、 $\tilde{V}^1 \cong V^1 \otimes (V^1)^{op}$ である。

$\tilde{Y}^2(v, z)$ の性質については述べていませんが、同じような論法により、 V -加群 $(U, Y^U), (W, Y^W)$ に対して、 U の変形した加群上に、 V -加群 $\bigoplus_X N_{U,W}^X X$ の構造を持つことが証明できます。

2 モジュラー群と加群の変形

前節のテンソル積加群への頂点作用素の定義において、 $\delta(\frac{w+1}{z})$ が中心的な役割を果たしています。この変形を k 回繰返すと

$$\text{Res}_w \frac{1}{z} \delta\left(\frac{w+k}{z}\right) Y(v, w)$$

となります。作用するベクトル空間は非常に複雑になっているので、ここでは説明を省きます。

この形は $w \rightarrow w+k (k=0,1,2,\dots)$ の変換に対応してと考えることが出来ます。それで、 $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} (k \in \mathbb{Z})$ に対して

$$Y^{w+k}(v, z) = \frac{1}{z} \delta\left(\frac{w+k}{z}\right) Y(v, w)$$

と定義しておきます。

次に、 $w \rightarrow \frac{1}{w}$ の変換に対応する頂点作用素の変換があることを示しましょう。

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (k \in \mathbb{Z})$ に対して

$$Y^{1/w}(v, z) = \text{Res}_w \frac{1}{z} \frac{1}{w} e^{L(1)/w} (-w^2)^{L(0)} \delta\left(\frac{1}{wz}\right) Y(v, w)$$

と定義する。この変換は頂点作用素代数の加群 (U, Y) の制限相対空間

$$U^* = \bigoplus_{n=0}^{\infty} (\text{Hom}(U(n), \mathbb{C}))$$

に対して定義される頂点作用素 $Y^*(v, z)$ を定義するのに使われます。即ち、 $\langle, \rangle: U^* \otimes U \rightarrow \mathbb{C}$ を自然な2次形式とすると、 $\langle Y^*(v, z)u^*, u \rangle = \langle u^*, Y^{1/w}(v, z)u \rangle$ です。

変形 $Y^{w+k}(v, z) (k \in \mathbb{Z})$ と $Y^{1/w}(v, z)$ を繰り返して、

定理 4 $A \in GL(2, \mathbb{Z})$ の各元 A に対して、 $Y^A(v, z)$ を上の2つの変形を繰り返すことによって定義できる。これは、

$$(Y^A)^B(v, z) = Y^{BA}(v, z) \quad \forall A, B \in GL(2, \mathbb{Z})$$

を満たし、もし、 $A \in SL(2, \mathbb{Z})$ なら $Y^A(v, z)$ は結合法則を満たし、 $|A| = -1$ なら、 $Y^A(v, z)$ は逆結合法則を満たしている。

単純群のシロ－2部分群

原田耕一郎 (M.L.Lang との共同研究)

[1]. 位数 12 の群を全部決定したという結果が発表されたのは、すでに 19 世紀も終わり頃となっていた。その結果そのものには誤りがあったようで、3 年後の 1889 年にケーレーが正しく分類した。位数 12 の群は同型を除いて全部で 5 個ある。たった 5 個であるが、全部を構造まで含めて正しく数え上げるためには 実用群論 に対する 慣れ が必要であろう。百年を経るといのは大したものので紀元 2000 年には位数 2000 以下の群の構造がすべて決まっている [Beshe, Eick, O'Brien].

彼らの結果から位数が $2^{10} = 1024$ の群が 49,487,365,422 個あり、その他は全部で 423,164,062 個であることがわかる。言い換えれば、位数が $2^{10} = 1024$ の群は位数 2000 以下の群の 99.16% を占めているのである。位数 521, 128 などの群も加えると少ししではあるがその割合はさらに大きくなることはいうまでもない。

「漸近的にはほとんどすべての有限群は 2 群である」といってもウソにはならない。しかし、タイトルにあるように有限単純群のシロ－2部分群になり得るような位数が 2^{10} の群はたったの 11 個しかないのである。言い換えれば、ひとつの 2 群を無作為に選んだとすればそれが有限単純群のシロ－2部分群になっている可能性はほとんど 0 なのである。

ここに我々の研究の出発点がある。少ないのであれば特徴づけることが可能ではないかと思えるのである。

[2]. もう少し大きい 2 群を見てみよう。G.Higman と C.Sims の仕事を合わせると、位数 p^n の群の個数の漸近式が求められる。それは

$$p^{a(n,p)n^3}, \quad a(n,p) = \frac{2}{27} + O(n^{-1/3})$$

という式で表される。

この式を位数が 2^{46} の群に応用してみよう。なお、 2^{46} はモンスターのシロ－2部分群の位数である。位数が 2^{10} 以下であればそれを位数として持つ 2 群の個数は正確に分かっているのであるから、漸近式の $O(n^{-1/3})$ を $kn^{-1/3}$ で置き換えると k の値がわかる。実際、それらは $n = 6, 7, 8, 9, 10$ に応じて $k = -0.0668, -0.0793, -0.0865, -0.0875, -0.0830$ である。それゆえ、 k の値がほぼそのような領域に入っているとの仮定のもとに、 n が大きい場合は $k = -0.08$ と決めよう。

この $k = -0.08$ を用いると位数 2^{46} の群の個数がほぼ 10^{1500} と計算される。我々の現宇宙のすべての粒子の個数は 10^{83} 程度と同僚の数理論物理学者が言ってくれた。モンスターも 10^{1500} 個もある位数 2^{46} の中の 1 つを用いて

単純群となっているのである。考えてみればずいぶん神秘的な話である。しかもモンスターと同じシロー 2 部分群を持つ単純群はモンスターが唯一のものである。神秘さがさらに増す。

[3]. 定義. 2 群 S はそれが有限単純群のシロー 2 群になっているとき 実現可能 と呼ぶ。

この言葉を用いれば、位数 2^{10} の実現可能な群は全部で 11 個ある。そのほかの小さい位数の実現可能なものの個数は表 1 として後で示す。

[4]. 問題. 2 群が実現可能であるための必要十分条件を求めよ。

[5]. 仮定 I. ベキ零指数 3 以上の 2 群だけを考えればよい。

ベキ零指数 3 以下の 2 群をシロー 2 部分群として持つ単純群は単純群分類の初期に完成されている [Gorenstein-Gilman]. 重要なことはそれが独立に完成されていることである。その後の多くの分類定理は [すべての単純群は知られているものにかぎる] との仮定のもとに証明されているがこれは違う。現れるべき単純群の系列も $PSL_2(2^n), PSL_3(2^n), PSU_3(2^n)$ などと少なくとも一度現代的手法でやりなおすとしても大して手間はかからないと思われる。

しかし、仮定 I をおく主たる理由は別のところにもある。観察：ほとんどすべての 2 群はベキ零指数が 2 以下である。信用しがたいと思う人もあるだろうから証明を付けよう。

G.Higman の結果を用いるのである。彼は、中心も中心による剰余群も初等可換群であるような p 群の個数を決めた。そのような群のベキ零指数はもちろん 2 以下である。そのような群の個数は

$$p^{b(n,p)n^3}, \quad b(n,p) = \frac{2}{27} + O(n^{-1})$$

であるというのが彼が結果である。証明も易しいので述べておこう。

$n = r + s$ とする。ここで $r, s > 0$ である。また $0 \leq b(i, k) \leq p - 1, 0 \leq c(i, j, k) \leq p - 1$ とする。さらに $1 \leq i < j \leq r, 1 \leq k \leq s$ である。

元 g_1, g_2, \dots, g_r で生成され、次の生成関係式をもつ群を P とおく。

- (1). $[g_i, g_j] = \prod_{k=1}^s h_k^{c(i,j,k)},$
- (2). $[g_i, h_k] = 1,$
- (3). $[h_k, h_{k'}] = 1,$
- (4). $g_i^p = \prod_{k=1}^s h_k^{b(i,k)},$
- (5). $h_k^p = 1.$

$b(i, k)$ は全部で p^{rs} 通りの選び方があり、一方 $c(i, j, k)$ には $\frac{(r-1)r}{2}s$ 通りの選び方がある。それゆえ、群 P の同型類の個数は高々

$$p^{\frac{(r-1)r}{2}s + rs}$$

である。

$t = \frac{(r-1)r}{2}s + rs$ とおき、この値の最大値を調べよう。 $s = n - r$ だから、 $t = t(r) = \frac{1}{2}(n-r)r(r+1)$ と r の関数の形に書ける。 $t(r)$ の極大値を与える $t = \alpha$ は $\frac{2n-2}{3} < \alpha < \frac{2n+1}{3}$ と分かる (極小値を与える α' は $t(r)$ のグラフから明らかに区間 $(-1, 0)$ の中にある。 それを使うと α の存在領域もわかる)。そこで $\beta = \lceil \frac{2n}{3} \rceil$ とおけば、 $t(\beta)$ は $t(r)$ のとり得る最大整数である。 もちろん $r > 0$ は考慮に入れてある。 ここで $\lceil \cdot \rceil$ はガウスの記号である。 $r = \lceil \frac{2n}{3} \rceil$ と選んで、

$$t = \frac{(r-1)r}{2}s + rs = \frac{2}{27}n^3 + O(n^2) = \left(\frac{2}{27} + O(n^{-1}) \right) n^3$$

を得る。これが G.Higman の式である。 もう一言加えると、同型な P を与える異なった $b(i, k)$ と $c(i, j, k)$ の個数が $O(n^2)$ であることも言っておかねばならない。 $\frac{2}{27}$ という当初はあまり意味がなさそうだった数字がここに現れている。

これより、 $n \rightarrow \infty$ のとき

$$\frac{p \text{ groups of order } p^n \text{ of class } \leq 2}{\text{all } p \text{ groups of order } p^n} \rightarrow 1$$

であることが分かる。

実際にその現象で目で見たいという気もする。 そのために次の表 1 を用意した。

2^n	16	32	64	128	256	512	1024	2^{46}
number	14	51	267	2328	56092	10494213	49487365422	$\sim 10^{1500}$
realizable	3	4	8	7	7	12	11	< 30
class ≤ 2	79%	65%	48%	41%	56%	84%	???	???

表から分かるように、ベキ零指数が 2 以下の群の割合が急速に大きくなっている。 漸近的にほとんどの 2 群はベキ零指数が 2 以下である。 しかも、その事実は $n \leq 46$ でも十分に成立していそうである。 これが仮定 1 をおいた主たる理由である。

[6]. 定義. 2つの群 G_1 と G_2 は、それらのシロー 2 群が同型のとき、2 同型 であるという。 $G_1 \stackrel{2}{\sim} G_2$ と書く。 また、2つの 単純群 が 2-同型のときは、 G_1 と G_2 は同じ属に属するという。(通常 genus は種と訳されるが、我々の genus は生物学の分類論の属 (genus) である。)

例を少しあげよう。

- (1). $A_8 \stackrel{2}{\sim} PSp_4(3)$,
- (2). $A_{10} \stackrel{2}{\sim} PSL_4(3)$,
- (3). $Mathieu_3 \stackrel{2}{\sim} PSU_4(3)$,

- (4). $A_{12} \cong PSp_6(2)$,
 (5). $Mathieu_5 \cong GL_5(2) \cong Held$.

ここで, *Monster* はそれがそれが属する属の唯一の単純群であることを注意しておく.

[7]. 定義. 群 G が2つの自明でない群の直積として表わすことができないとき G は直既約であるという.

例. よく知られているように, 次数 $4n$ の対称群 S_{4n} のシロー2部分群は次数 $4n+2$ の交代群 A_{4n+2} のシロー2部分群に同型である. また n 次の対称群のシロー2部分群が $S_{2^{e_i}}$ のシロー2部分群の直積であることもよいであろう. ここで $n = 2^{e_1} + 2^{e_2} + \dots + 2^{e_t}$, $e_1 > e_2 > \dots > e_t \geq 0$ は n の2進法による展開である. これらのことより

$$A_{50} \cong S_{48} \cong S_{32} \times S_{16} \cong A_{34} \times A_{18}$$

となり, それゆえ T を A_{50} のシロー2部分群とするすればそれは直既約ではない. ところが, T を分解すると各成分はそれ自身実現可能な2群となっている. 一般につきのことが成立している.

定理. 単純群のシロー2群を直既約な成分の直積に分解するとその各々の成分も実現可能である.

それゆえ:

[8]. 仮定 II. 直既約な2群だけを考えればよい.

さて, 実現可能な2群の極小集合を探したためにもう1つの還元 (reduction) を行う. $PSL_2(q)$ という無限系列を考えよ. ここで q は奇素数のべきとする. この系列に属している単純群のシロー2部分群はすべて2面体群 D_{2^n} である. ここで, 2^n は $\frac{(q-1)(q+1)}{2}$ 割り切る最大の2のべきである.

2面体群 D_{2^n} をシロー2群に持つ単純群の分類方法は n には依らない. A_7 のような例外がないわけではないが, すべていっぺんにできる. ゆえに D_8 の場合に分類ができれば, その他の場合もできるとしてよい. 一般にこのような問題は, シロー2群は2面体群 (環積, その他) と構造は変えなければ, n が大きいほど問題は易しくなってくると思ってよい. 例外的な構造が少なくなるからである. なお D_4 はクラインの4群と呼ばれるもので可換である, それは可換なシロー2群を持つ単純群の仲間に入れる方がよい.

[9]. 定義. 実現可能な2群 S はそれが2個, 3個, または4個の元からなる体 (F_2, F_3, F_4) の上のシュヴァレー群または散在型単純群のシロー2部分群のとき *stem type* (幹型?と呼んでおく) 呼ぶ. ただし, F_4 は $PSL_3(4), PSU_3(4)$ のような特別な場合だけ必要であろう. また, 交代群のシロー2部分群は直

交群のそれに等しくなる。以上の考察により：

[10]. 仮定 III. *stem type* の 2 群だけを考えればよい。

[11]. 定義. 実現可能な 2 群は、幹型であり、ベキ零指数が 3 以上、さらに直既約であるとき 基本型 と呼ぶ。

基本型の実現可能な 2 群をすべて分類したいのである。表 1 で位数 2^{46} の実現可能な群は全部で 30 個あるといったが、基本型に限るとたったの 3 個になってしまう。それらは *Monster*, PSL_{20} , と $O_{26}^-(3)$ のシロー 2 群である。全部でほぼ 10^{1500} 個ある位数 2^{46} の 2 群がまず 30 個の実現可能なものになり、そして最後には 3 個の基本型まで落ちてきたのである。

[12]. 目標, 行程.

- (1). 有限単純群の分類を用いて、すべての基本型の実現可能な 2 群を決定せよ。ただし、いまのところ考慮にいれるのは、位数が最大で 2^{46} とする。
 - (2). (1) で得られた群に対して共通な性質を数え上げよ。
 - (3). (2) で得られた性質を満たす 2 群をすべて決定せよ。この段階 (3) では計算器を用いることもあり得る。
 - (4). (3) で得られた群の個数が (1) で得られた数に比べて大きすぎるときは (2) に帰り、共通な性質をさらに探す。
 - (5). (1) = (3) となれば、実現可能な 2-群の特徴付けができたことになる。
 - (6). 有限単純群の分類の結果を用いずに (2) で得られた性質を実現可能な 2 群に対して証明せよ。
- (6) ができれば単純群の分類への新しい道も開けてこよう。

[13]. これは 2001 年 6 月 25 日から 30 日まで台南市で開かれた国際代数学会の報告集の原稿を日本語に訳したものにほぼ等しい。そこでは文献なども揃えたがここでは省略する。

Department of Mathematics, The Ohio State University, Columbus, Ohio
43210, USA
haradako@math.ohio-state.edu

Department of Mathematics, National University of Singapore, Singapore, 117543
matlml@math.nus.edu.sg

Highest weight vectors in lattice vertex operator algebras

Hirofumi Yamada

Department of Mathematics
Hitotsubashi University
Kunitachi, Tokyo 186-8601, Japan
yamada@math.hit-u.ac.jp

1 Introduction

We shall report recent developments in the study of the decomposition of vertex operator algebras associated with $\sqrt{2}$ times the root lattice of type A_l , D_l , or E_l as a module for a tensor product of Virasoro vertex operator algebras.

Let $L = \sqrt{2}A_l$, $\sqrt{2}D_l$, or $\sqrt{2}E_l$ be $\sqrt{2}$ times the root lattice of type A_l , D_l , or E_l and V_L be the vertex operator algebra associated with L (see Frenkel, Lepowsky, and Meurman [8] for the definition of V_L). It was shown by Dong, Li, Mason, and Norton [4] that there exist $l + 1$ mutually orthogonal conformal vectors in V_L . Then, the vertex operator subalgebra T generated by those $l + 1$ mutually orthogonal conformal vectors is isomorphic to a tensor product of $l + 1$ Virasoro vertex operator algebras. As a module for T , V_L is completely reducible. That is, the vertex operator algebra V_L is decomposed into a direct sum of irreducible T -modules. It is natural to ask which irreducible T -modules appear in V as direct summands. We collect known examples of such decompositions in Section 3. Then in Section 4 we shall discuss some applications of these decompositions.

2 Highest weight vectors

We shall quickly review some notations concerning a vertex operator algebra $(V_L, Y, \mathbf{1}, \omega)$ associated with a positive definite even lattice L and introduce their highest weight vectors. We refer the reader to Chapter 8 of [8] for the exact definition of vertex operator algebras and the detailed construction of V_L . First of all, recall the notion of a vertex operator algebra. Roughly speaking, a vertex operator algebra $(V, Y, \mathbf{1}, \omega)$ is an infinite dimensional vector space V over \mathbb{C} and for each $u \in V$, a vertex operator

$$Y(u, z) = \sum_{n \in \mathbb{Z}} u_n z^{-n-1}, \quad u_n \in \text{End } V$$

is defined, which satisfies a certain axiom. Here z is a formal variable. The coefficient $u_n \in \text{End } V$ of z^{-n-1} is called a component operator.

A Virasoro algebra Vir is an infinite dimensional Lie algebra with basis $\{L(n), n \in \mathbb{Z}\} \cup \{1\}$ over \mathbb{C} and commutator relations

$$[L(m), L(n)] = (m - n)L(m + n) + \frac{m^3 - m}{12}\delta_{m+n,0}c, \quad (2.1)$$

where c is a constant called the central charge.

A Vir -module W is a vector space over \mathbb{C} equipped with $L(n) \in \text{End } W$ which satisfy the above relations with $[L(m), L(n)] = L(m)L(n) - L(n)L(m)$ in $\text{End } W$. In this article we always assume that the operator $L(0)$ is semisimple on W . Thus W is a direct sum of eigenspaces

$$W_\lambda = \{w \in W \mid L(0)w = \lambda w\}$$

for $L(0)$. The eigenvalue λ is called a weight. We shall write $\text{wt } w = \lambda$ if $L(0)w = \lambda w$.

Definition 2.1 A vector v in a Vir -module is called a highest weight vector with highest weight h if

- (1) $L(0)v = hv$, and
- (2) $L(n)v = 0$ for all $n > 0$.

A highest weight module W is a Vir -module which is generated by a highest weight vector. The parameters c and h are said to be the central charge and the highest weight of W respectively. Note that if v is a highest weight vector and W is generated by v , then

$$W = \text{span}\{L(-n_1) \cdots L(-n_k)v \mid 0 < n_k \leq \cdots \leq n_1, k = 0, 1, 2, \dots\}.$$

If the vectors

$$L(-n_1) \cdots L(-n_k)v, \quad 0 < n_k \leq \cdots \leq n_1, \quad k = 0, 1, 2, \dots$$

are linearly independent, then W is called the Verma module. It is uniquely determined by c and h and is denoted by $M(c, h)$. Every highest weight module for Vir with central charge c and highest weight h is a homomorphic image of $M(c, h)$. Moreover, there is a unique maximal submodule $J(c, h)$ in $M(c, h)$ and the quotient module $L(c, h) = M(c, h)/J(c, h)$ is a unique irreducible highest weight module with central charge c and highest weight h . In case of $h = 0$, $L(c, 0)$ has a vertex operator algebra structure. It is called a Virasoro vertex operator algebra or a minimal model. For any h , $L(c, h)$ is a module for the vertex operator algebra $L(c, 0)$.

A Vir -module is said to be unitary if it possesses a nondegenerate contravariant hermitian form. Not all $L(c, h)$ are unitary. It is well known (see for example [14, Proposition 3.1]) that

Theorem 2.2 If $L(c, h)$ is unitary, then c and h satisfy one of the following conditions.

- (1) $c \geq 1$ and $h \geq 0$.
- (2) $c = 1 - \frac{6}{(m+2)(m+3)}$ and $h = h_{r,s} = \frac{((m+3)r - (m+2)s)^2 - 1}{4(m+2)(m+3)}$ for some integers m, r, s such that $m \geq 0$ and $1 \leq s \leq r \leq m+1$.

Case (2) is so called the discrete series.

We now turn to vertex operator algebras associated with positive definite even lattices. Let L be $\sqrt{2}$ times an ordinary root lattice of type A_l , D_l , or E_l with inner product $\langle \cdot, \cdot \rangle$. Denote by Π the set of simple roots of type A_l , D_l , or E_l . Let V_L be the vertex operator algebra associated with the lattice L defined by Frenkel, Lepowsky, and Meurman [8]. Then

$$V_L = M(1) \otimes \mathbb{C}[L]$$

as a vector space, where $M(1)$ is the symmetric algebra of

$$\text{span}\{\alpha(-n) \mid \alpha \in \Pi, 0 < n \in \mathbb{Z}\}$$

and $\alpha(m)$, $m \in \mathbb{Z}$ are operators which satisfy the commutator relations

$$[\alpha(m), \beta(n)] = \langle \alpha, \beta \rangle m \delta_{m+n, 0}.$$

Moreover, $\mathbb{C}[L] = \text{span}\{e^\beta \mid \beta \in L\}$ is the group algebra of the additive group L with multiplication $e^\alpha e^\beta = e^{\alpha+\beta}$.

For $v = \alpha_1(-n_1) \cdots \alpha_k(-n_k) \otimes e^\beta \in V_L$, the weight $\text{wt } v$ of v is given by

$$\text{wt } v = n_1 + \cdots + n_k + \frac{1}{2} \langle \beta, \beta \rangle.$$

By convention, the weight of the zero vector is considered to be an arbitrary number. Then the set of all vectors of weight m forms a subspace, which is called the homogeneous subspace of weight m , and V_L is a direct sum of those homogeneous subspaces.

The vertex operator algebra V_L possesses a special element ω called the Virasoro element. Let $L(n) = \omega_{n+1}$, the coefficient of z^{-n-2} in the vertex operator $Y(\omega, v)$. Then these operators $L(n)$ satisfy the Virasoro relations (2.1) with central charge l . Furthermore, the homogeneous subspace of weight m is the eigenspace for $L(0)$ with eigenvalue m . Thus the weight of a vector in V_L is nothing but the eigenvalue for $L(0)$.

Definition 2.3 *A vector v of weight 2 in V_L is said to be a conformal vector with central charge c if the component operators $L_v(n) = v_{n+1} \in \text{End } V_L$ satisfy the Virasoro relations*

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

Theorem 2.4 ([4]) *In the vertex operator algebra V_L associated with a lattice $L = \sqrt{2}A_l$, $\sqrt{2}D_l$, or $\sqrt{2}E_l$, there exist $l + 1$ mutually orthogonal conformal vectors $\omega^1, \dots, \omega^{l+1}$ such that $\omega^1 + \cdots + \omega^{l+1} = \omega$.*

Let c_i be the central charge of a conformal vector ω^i and $\text{Vir}(\omega^i)$ be the vertex operator subalgebra generated by ω^i . Recall that two conformal vectors ω^i and ω^j are said to be orthogonal if the component operators $(\omega^i)_m$ and $(\omega^j)_n$ commute, that is, $(\omega^i)_m (\omega^j)_n = (\omega^j)_n (\omega^i)_m$ for all $m, n \in \mathbb{Z}$. Since those conformal vectors are mutually orthogonal, the

vertex operator subalgebra T generated by $\omega^i, i = 1, 2, \dots, l+1$ is isomorphic to a tensor product of $\text{Vir}(\omega^i)$'s:

$$T \cong \text{Vir}(\omega^1) \otimes \cdots \otimes \text{Vir}(\omega^{l+1}).$$

It is known that the vertex operator algebra associated with a positive definite even lattice possesses a nondegenerate invariant form. In our case this means that

- (a) $\text{Vir}(\omega^i) \cong L(c_i, 0)$,
- (b) V_L is completely reducible as a T -module.

Now, any irreducible T -module is of the form (see [7])

$$L(c_1, h_1) \otimes \cdots \otimes L(c_{l+1}, h_{l+1}) \tag{2.2}$$

and it is generated by a highest weight vector $v = v(h_1, \dots, h_{l+1})$ for T . Here highest weight vectors for T are defined as follows.

Definition 2.5 *A highest weight vector $v = v(h_1, \dots, h_{l+1})$ for T is a vector which satisfies the two conditions:*

- (1) $(\omega^i)_1 v = h_i v$ for $1 \leq i \leq l+1$,
- (2) $(\omega^i)_n v = 0$ for $n \geq 2$ and $1 \leq i \leq l+1$.

Note that the weight of v is $h_1 + \dots + h_{l+1}$ since $\omega^1 + \dots + \omega^{l+1} = \omega$. Such a highest weight vector is unique up to scalar multiple in each irreducible T -module of the form (2.2).

We want to know the decomposition of V_L into a direct sum of irreducible T -modules. For this purpose it is enough to determine all highest weight vectors for T in V_L . In the next section we shall present some known examples.

3 Known examples

EXAMPLE 1. $L = \sqrt{2}A_1$. This is the smallest case. In this case $l = 1$ and $c_1 = c_2 = \frac{1}{2}$. As a T -module, $V_{\sqrt{2}A_1}$ is a direct sum of two irreducible modules:

$$V_{\sqrt{2}A_1} = (L(\frac{1}{2}, 0) \otimes L(\frac{1}{2}, 0)) \oplus (L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{1}{2}, \frac{1}{2})).$$

EXAMPLE 2 ([13]). $L = \sqrt{2}A_2$. In this case $c_1 = \frac{1}{2}, c_2 = \frac{7}{10}, c_3 = \frac{4}{5}$ and $V_{\sqrt{2}A_2}$ is a direct sum of 8 irreducible T -modules. The list of (h_1, h_2, h_3) for the highest weight vectors $v(h_1, h_2, h_3)$ are

$$\begin{aligned} (0, 0, 0), & \quad (0, \frac{3}{5}, \frac{2}{5}), & \quad (\frac{1}{2}, \frac{1}{10}, \frac{2}{5}), & \quad (0, \frac{3}{5}, \frac{7}{5}), \\ (\frac{1}{2}, \frac{1}{10}, \frac{7}{5}), & \quad (\frac{1}{2}, \frac{3}{2}, 0), & \quad (0, 0, 3), & \quad (\frac{1}{2}, \frac{3}{2}, 3). \end{aligned}$$

EXAMPLE 3 ([5]). $L = \sqrt{2}A_3$. In this case $c_1 = \frac{1}{2}$, $c_2 = \frac{7}{10}$, $c_3 = \frac{4}{5}$, $c_4 = 1$ and $V_{\sqrt{2}A_3}$ is a direct sum of infinitely many irreducible T -modules. All of the irreducible direct summands are known.

EXAMPLE 4 ([20]). $L = \sqrt{2}A_l$, $l \geq 4$. In this case

$$c_i = 1 - \frac{6}{(i+2)(i+3)}, \quad 1 \leq i \leq l,$$

$$c_{l+1} = \frac{2l}{l+3}.$$

Only highest weight vectors of weight at most 2 are known in this case. We note that $V_{\sqrt{2}A_l}$ is generated by T and the highest weight vectors of weight at most 2 as a vertex operator algebra.

The conformal vectors $\omega^1, \dots, \omega^{l+1}$ discovered by Dong, Li, Mason, and Norton [4] are not unique. In fact, they depend on a sequence of sublattices of L . In case of type D_l or E_l , there are some possible choices of such sequences.

EXAMPLE 5. $L = \sqrt{2}D_l$, $l \geq 4$.

Case 1 ([6]). If we take sublattices $A_1 \subset A_2 \subset A_3 \subset A_4 \subset \dots \subset D_l$ of $L/\sqrt{2} = D_l$, then the central charges of the corresponding conformal vectors are

$$c_1 = \frac{1}{2}, \quad c_2 = \frac{7}{10}, \quad c_3 = \frac{4}{5}, \quad c_i = 1, \quad 4 \leq i \leq l+1.$$

In this case the decomposition of $V_{\sqrt{2}D_l}$ into a direct sum of irreducible T -modules is known.

Case 2 ([21]). If we take sublattices $A_1 \subset A_2 \subset \dots \subset A_{l-1} \subset D_l$ of $L/\sqrt{2} = D_l$, then the central charges of the corresponding conformal vectors are

$$c_i = \begin{cases} 1 - \frac{6}{(i+2)(i+3)} & \text{if } 1 \leq i \leq l-1, \\ \frac{2(l-1)}{l+2} & \text{if } i = l, \\ 1 & \text{if } i = l+1. \end{cases}$$

In this case only highest weight vectors of weight at most 2 are known.

EXAMPLE 6. $L = \sqrt{2}E_6$. There are two typical sequences of sublattices of $L/\sqrt{2} = E_6$, namely

(a) $A_1 \subset A_2 \subset A_3 \subset A_4 \subset A_5 \subset E_6$,

(b) $A_1 \subset A_2 \subset A_3 \subset A_4 \subset D_5 \subset E_6$.

In case (a) the central charges are

$$c_1 = \frac{1}{2}, \quad c_2 = \frac{7}{10}, \quad c_3 = \frac{4}{5}, \quad c_4 = \frac{6}{7}, \quad c_5 = \frac{25}{28}, \quad c_6 = \frac{39}{28}, \quad c_7 = \frac{6}{7},$$

and in case (b) they are

$$c_1 = \frac{1}{2}, \quad c_2 = \frac{7}{10}, \quad c_3 = \frac{4}{5}, \quad c_4 = \frac{6}{7}, \quad c_5 = \frac{8}{7}, \quad c_6 = \frac{8}{7}, \quad c_7 = \frac{6}{7}.$$

In case (a) all highest weight vectors of weight at most 2 are known. The list of $(h_1, h_2, h_3, h_4, h_5, h_6, h_7)$ for the highest weight vectors of weight 1 and 2 in $V_{\sqrt{2}E_6}$ are as follows.

There are 6 highest weight vectors of weight 1. They are

$$\begin{aligned} & (0, 0, 0, 0, 0, 6/7, 1/7) \\ & (0, 0, 0, 0, 3/4, 3/28, 1/7) \\ & (0, 0, 0, 5/7, 1/28, 3/28, 1/7) \\ & (0, 0, 2/3, 1/21, 1/28, 3/28, 1/7) \\ & (0, 3/5, 1/15, 1/21, 1/28, 3/28, 1/7) \\ & (1/2, 1/10, 1/15, 1/21, 1/28, 3/28, 1/7) \end{aligned}$$

There are 15 highest weight vectors of weight 2 in $V_{\sqrt{2}E_6}^-$. They are

$$\begin{aligned} & (0, 0, 0, 0, 0, 13/7, 1/7) \\ & (0, 0, 0, 5/7, 15/28, 17/28, 1/7) \\ & (0, 0, 2/3, 1/21, 15/28, 17/28, 1/7) \\ & (0, 3/5, 1/15, 1/21, 15/28, 17/28, 1/7) \\ & (1/2, 1/10, 1/15, 1/21, 15/28, 17/28, 1/7) \\ & (0, 0, 2/3, 10/21, 3/28, 17/28, 1/7) \\ & (0, 3/5, 1/15, 10/21, 3/28, 17/28, 1/7) \\ & (1/2, 1/10, 1/15, 10/21, 3/28, 17/28, 1/7) \\ & (0, 3/5, 2/5, 1/7, 3/28, 17/28, 1/7) \\ & (1/2, 1/10, 2/5, 1/7, 3/28, 17/28, 1/7) \\ & (0, 0, 2/3, 10/21, 5/14, 5/14, 1/7) \\ & (0, 3/5, 1/15, 10/21, 5/14, 5/14, 1/7) \\ & (1/2, 1/10, 1/15, 10/21, 5/14, 5/14, 1/7) \\ & (0, 3/5, 2/5, 1/7, 5/14, 5/14, 1/7) \\ & (1/2, 1/10, 2/5, 1/7, 5/14, 5/14, 1/7) \end{aligned}$$

There are 50 linearly independent highest weight vectors of weight 2 in $V_{\sqrt{2}E_6}^+$. They

are

(1/2, 3/2, 0, 0, 0, 0, 0)
(0, 3/5, 7/5, 0, 0, 0, 0)
(1/2, 1/10, 7/5, 0, 0, 0, 0)
(0, 0, 2/3, 4/3, 0, 0, 0)
(0, 3/5, 1/15, 4/3, 0, 0, 0)
(1/2, 1/10, 1/15, 4/3, 0, 0, 0)
(0, 0, 0, 5/7, 9/7, 0, 0)
(0, 0, 2/3, 1/21, 9/7, 0, 0)
(0, 3/5, 1/15, 1/21, 9/7, 0, 0)
(1/2, 1/10, 1/15, 1/21, 9/7, 0, 0)
(0, 0, 0, 0, 0, 2, 0)
(0, 0, 0, 0, 3/4, 5/4, 0)
(0, 0, 0, 5/7, 1/28, 5/4, 0)
(0, 0, 2/3, 1/21, 1/28, 5/4, 0)
(0, 3/5, 1/15, 1/21, 1/28, 5/4, 0)
(1/2, 1/10, 1/15, 1/21, 1/28, 5/4, 0)
(0, 0, 0, 5/7, 15/28, 3/4, 0)
(0, 0, 2/3, 1/21, 15/28, 3/4, 0)
(0, 3/5, 1/15, 1/21, 15/28, 3/4, 0)
(1/2, 1/10, 1/15, 1/21, 15/28, 3/4, 0)
(0, 0, 2/3, 10/21, 3/28, 3/4, 0)
(0, 3/5, 1/15, 10/21, 3/28, 3/4, 0)
(1/2, 1/10, 1/15, 10/21, 3/28, 3/4, 0)
(0, 3/5, 2/5, 1/7, 3/28, 3/4, 0)
(1/2, 1/10, 2/5, 1/7, 3/28, 3/4, 0)
(0, 0, 2/3, 10/21, 5/14, 1/2, 0)
(0, 3/5, 1/15, 10/21, 5/14, 1/2, 0)
(1/2, 1/10, 1/15, 10/21, 5/14, 1/2, 0)
(0, 3/5, 2/5, 1/7, 5/14, 1/2, 0)
(1/2, 1/10, 2/5, 1/7, 5/14, 1/2, 0)

and

$$\begin{array}{l}
 (0, 0, 0, 0, 0, 9/7, 5/7) \\
 (0, 0, 0, 0, 3/4, 15/28, 5/7) \\
 (0, 0, 0, 0, 3/4, 15/28, 5/7) \\
 (0, 0, 0, 5/7, 1/28, 15/28, 5/7) \\
 (0, 0, 0, 5/7, 1/28, 15/28, 5/7) \\
 (0, 0, 2/3, 1/21, 1/28, 15/28, 5/7) \\
 (0, 0, 2/3, 1/21, 1/28, 15/28, 5/7) \\
 (0, 3/5, 1/15, 1/21, 1/28, 15/28, 5/7) \\
 (0, 3/5, 1/15, 1/21, 1/28, 15/28, 5/7) \\
 (1/2, 1/10, 1/15, 1/21, 1/28, 15/28, 5/7) \\
 (1/2, 1/10, 1/15, 1/21, 1/28, 15/28, 5/7) \\
 (0, 0, 0, 5/7, 15/28, 1/28, 5/7) \\
 (0, 0, 2/3, 1/21, 15/28, 1/28, 5/7) \\
 (0, 3/5, 1/15, 1/21, 15/28, 1/28, 5/7) \\
 (1/2, 1/10, 1/15, 1/21, 15/28, 1/28, 5/7) \\
 (0, 0, 2/3, 10/21, 3/28, 1/28, 5/7) \\
 (0, 3/5, 1/15, 10/21, 3/28, 1/28, 5/7) \\
 (1/2, 1/10, 1/15, 10/21, 3/28, 1/28, 5/7) \\
 (0, 3/5, 2/5, 1/7, 3/28, 1/28, 5/7) \\
 (1/2, 1/10, 2/5, 1/7, 3/28, 1/28, 5/7)
 \end{array}$$

Note that

$$\begin{array}{l}
 (0, 0, 0, 0, 3/4, 15/28, 5/7) \\
 (0, 0, 0, 5/7, 1/28, 15/28, 5/7) \\
 (0, 0, 2/3, 1/21, 1/28, 15/28, 5/7) \\
 (0, 3/5, 1/15, 1/21, 1/28, 15/28, 5/7) \\
 (1/2, 1/10, 1/15, 1/21, 1/28, 15/28, 5/7)
 \end{array}$$

are of multiplicity 2.

4 Some remarks

The study of vertex operator algebras as modules for their subalgebras isomorphic to tensor products of Virasoro vertex operator algebras was initiated by Dong, Mason, and Zhu [7]. In [7] it is shown that the Monster module V^h contains a subalgebra isomorphic to a tensor product $L(\frac{1}{2}, 0)^{\otimes 48}$ of 48 copies of the smallest nontrivial Virasoro vertex operator algebra $L(\frac{1}{2}, 0)$ in the discrete series. The Monster module V^h has a nondegenerate invariant form and so V^h is completely reducible as a module for this subalgebra. The decomposition of V^h is also studied in [7]. Such a decomposition, especially together with

fusion rules among irreducible modules for the subalgebra, is very useful for the study of V^h (for example, see Dong [2], Dong, Li, and Mason [3], Huang [9], Miyamoto [16, 17]). Furthermore, Miyamoto [18] obtained a new construction of V^h as a combination of those irreducible modules.

In 1998, Dong, Li, Mason, and Norton [4] discovered other subalgebras in V^h which are similar tensor products of Virasoro vertex operator algebras. In fact, as already appeared in Section 2 they showed that the Virasoro element ω can be written as a sum of $l + 1$ mutually orthogonal conformal vectors $\omega^1, \dots, \omega^{l+1}$ in V_L , where $L = \sqrt{2}A_l, \sqrt{2}D_l$, or $\sqrt{2}E_l$. The vertex operator subalgebra T of V_L generated by these $l + 1$ conformal vectors is isomorphic to $L(c_1, 0) \otimes \dots \otimes L(c_{l+1}, 0)$, where c_i denotes the central charge of ω^i . Now, assume that l is a divisor of 24. Then the orthogonal sum $L^{\otimes 24/l}$ of $24/l$ copies of L is contained in the Leech lattice Λ . Such an embedding is not unique in general (cf. [4], see also Kitazume's recent work). This embedding implies that a tensor product of $24/l$ copies of V_L is contained in V_Λ ; $(V_L)^{\otimes 24/l} \subset V_\Lambda$, and it follows that

$$T^{\otimes 24/l} \subset V_\Lambda^+ \subset V^h.$$

Hence we can study V^h as a module for $T^{\otimes 24/l}$.

If $l = 1$, then $T = L(\frac{1}{2}, 0) \otimes L(\frac{1}{2}, 0)$ as in EXAMPLE 1 in Section 3. This case is treated in [7]. The cases $l = 2$ and 3 are studied in [10] and [12] respectively.

Recently, Shimakura [19] studied another kind of tensor products. Let $L = \mathbb{Z}\alpha$ be a rank one lattice spanned by α with $\langle \alpha, \alpha \rangle = 2k$, where k is a positive integer. In [19] it is shown that V^h contains a subalgebra isomorphic to a tensor product $(V_L^+)^{\otimes 24}$ of 24 copies of V_L^+ and that the decomposition of V^h as a module for $(V_L^+)^{\otimes 24}$ can be described in terms of an extremal Type II code of length 24 over \mathbb{Z}_{2k} . Using this decomposition and the fusion rules for V_L^+ (see Abe [1]), Shimakura also obtains 4A element or 2B element of the Monster according as k is odd or even respectively.

Some other applications of the decompositions can be found in [11, 13, 15].

References

- [1] T. Abe, Fusion rules for the charge conjugation orbifold, preprint.
- [2] C. Dong, Representations of the moonshine module vertex operator algebra, in: Mathematical aspects of conformal and topological field theories and quantum groups, P. J. Sally et al. Ed., *Contemporary Math.* **175** (1994), 27-36.
- [3] C. Dong, H. Li, and G. Mason, Some twisted modules for the moonshine vertex operator algebras, in: Moonshine, the monster, and related topics, C. Dong and G. Mason Ed., *Contemporary Math.* **193** (1996), 25-43.
- [4] C. Dong, H. Li, G. Mason, and S. P. Norton, Associative subalgebras of the Griess algebra and related topics, in: *The Monster and Lie Algebras*, ed. by J. Ferrar and K. Harada, Walter de Gruyter, 1998, 27-42.
- [5] C. Dong, C. H. Lam, and H. Yamada, Decomposition of the vertex operator algebra $V_{\sqrt{2}A_3}$, *J. Algebra* **222** (1999), 500-510.

- [6] C. Dong, C. H. Lam, and H. Yamada, Decomposition of the vertex operator algebra $V_{\sqrt{2}D_1}$, *Comm. in Contemporary Math.* **3** (2001), 137-151.
- [7] C. Dong, G. Mason, and Y. Zhu, Discrete series of the Virasoro algebra and the Moonshine module, *Proc. Symp. Pure Math., Amer. Math. Soc.* **56** II (1994), 295-316.
- [8] I. B. Frenkel, J. Lepowsky, and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. **134**, Academic Press, 1988.
- [9] Y. Huang, A non-meromorphic extension of the moonshine module vertex operator algebra, in: Moonshine, the monster, and related topics, C. Dong and G. Mason Ed., *Contemporary Math.* **193** (1996), 123-148.
- [10] M. Kitazume, C. H. Lam, and H. Yamada, Decomposition of the moonshine vertex operator algebra as Virasoro modules, *J. Algebra* **226** (2000), 893-919.
- [11] M. Kitazume, C. H. Lam, and H. Yamada, A class of vertex operator algebras constructed from \mathbb{Z}_8 codes, *J. Algebra* **242** (2001), 338-359.
- [12] M. Kitazume, C. H. Lam, and H. Yamada, Moonshine vertex operator algebra as $L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \otimes L(\frac{4}{5}, 0) \otimes L(1, 0)$ -module, to appear in *J. Pure and Applied Algebra*.
- [13] M. Kitazume, M. Miyamoto, and H. Yamada, Ternary codes and vertex operator algebras, *J. Algebra* **223** (2000), 379-395.
- [14] V. G. Kac and M. Wakimoto, Modular and conformal invariance constraints in representation theory of affine algebras, *Advances in Math.* **70** (1988), 156-236.
- [15] C. H. Lam and H. Yamada, $\mathbb{Z}_2 \times \mathbb{Z}_2$ codes and vertex operator algebras, *J. Algebra* **224** (2000), 268-291.
- [16] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* **179** (1996), 523-548.
- [17] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra* **181** (1996), 207-222.
- [18] M. Miyamoto, A new construction of the Moonshine vertex operator algebra over the real number field, preprint.
- [19] H. Shimakura, Decomposition of the Moonshine module with respect to a code over \mathbb{Z}_{2^k} , preprint.
- [20] H. Yamada, Highest weight vectors with small weights in the vertex operator algebra associated with a lattice of type $\sqrt{2}A_l$, *Comm. in Algebra* **29** (2001), 1311-1324.
- [21] H. Yamada, Highest weight vectors in the vertex operator algebra associated with a lattice of type $\sqrt{2}D_l$, preprint.

Intertwining operators in orbifold theory

山内 博

(Hiroshi Yamauchi)

筑波大学数学研究科

Graduate School of Mathematics

University of Tsukuba

e-mail: hirocci@math.tsukuba.ac.jp

1 概要

今回の話では VOA の表現論における Zhu の理論をオービフォルド理論に応用し、[DLM2] と [M] で得られている結果を拡張する。有理型 VOA の既約表現から得られる次数付きトレース関数が収束し、それらで張られる空間がモジュラー群 $SL_2(\mathbb{Z})$ の作用で不変になることは [Z] において体系的に示された。その拡張として自己同型で不変な加群から得られる無限次元リー代数の表現論では twining character として知られている次数付きトレース関数の保型性が [DLM2] で示された。さらに [DLM2] ではオービフォルド VOA の表現論も展開され、ツイストセクターにおける次数付きトレース関数の保型性も同時に調べられている。一方、[M] では頂点作用素を一般化したものである交絡作用素 (intertwining operator) を用いて得られるトレース関数の保型性が証明された。これらの結果は [Z] の一般化であると考えられる。即ち、[DLM2] では自己同型を主眼において [Z] の結果を拡張しており、[M] では作用素を一般化して新しい結果を得ている。今回、自己同型と交絡作用素を同時に考えることによりこれらの結果をさらに一般化できたのでそれを報告したい。理論の基本的方針は [DLM2], [M] とともに [Z] のものと本質的に同じであるが、これらを同時に考えるときには大きな違いが現れる。[Z], [DLM2] そして [M] の中ではみなそれぞれの既約表現を独立に考察しているが、自己同型と交絡作用素を同時に扱うときには、自己同型で共役な既約表現を同時に扱わなければならない。これは頂点作用素と交絡作用素の違いを反映している。共役な既約表現をひとまとめにして扱う手法は [DY] にも見られており、オービフォルド VOA の表現論の一つの特徴にもなっている。

2 ツイスト交絡作用素

V を VOA とする。任意の N -次数付き加群が完全可約であるとき、 V を有理型という。本稿ではツイスト、ノンツイストどちらの場合でも V は有理型であると仮定する。[DLM1] において有理型 VOA の既約加群は有限個であることが示されている。

ツイスト加群間の交絡作用素の一般的な定義は [X] で与えられているが、今回の話では自己同型との関連を明確にするために修正を加えた定義を採用する。我々の定義はツイスト加群上の頂点作用素の一般化にあたる。

$g, h \in \text{Aut}(V)$ をそれぞれ有限位数で互いに可換なものとする。 V の g -ツイスト既約加群の同型類全体からなる集合 \mathcal{M}_g とするとき、 \mathcal{M}_g 上に h の自然な作用が考えられる。 $(M, Y^M) \in \mathcal{M}_g$ とするとき、 M 上の頂点作用素 Y^M に対し

$$(Y^M \circ h)(a, z) := Y^M(ha, z)$$

と定めると $(M, Y^M \circ h)$ もまた g -既約 V -加群になる。この作用でみた V -加群 M を $(M, Y^M) \circ h$ で表す。これは \mathcal{M}_g の元のどれかと同型になっているので、 \mathcal{M}_g 上に h は置換として作用する。特に $(M, Y^M) \circ h \simeq (M, Y^M)$ となるとき (M, Y^M) を h -安定と呼ぶ。これは次の条件を満たす線形自己同型 $\phi_h \in GL(M)$ が存在することを意味する:

$$Y^M(ha, z) = \phi_h Y^M(a, z) \phi_h^{-1} \quad \text{for } \forall a \in V. \quad (1)$$

このような写像 ϕ_h を安定化自己同型と呼ぶことにする。定義から定数倍は許されるので安定化自己同型は一意には定まらないが、Schur の補題からスカラー倍を除いて一意に定まる。

$(U = \bigoplus_{n=0}^{\infty} U_{n+h_0}, Y^0)$ を g -安定な既約 V -加群とし、 $\phi_g \in GL(U)$ を (1) を満たすものとする。そして $(W_g^i = \bigoplus_{n=0}^{\infty} (W_g^i)_{n/|g|+h_i}, Y^i)$ ($i = 1, 2$) を既約 g -ツイスト V -加群とする。最初に安定化自己同型 ϕ_g を正規化する。Schur の補題から $\phi_g^{|g|} \in \mathbb{C}$ であることが分かる。条件 (1) ではスカラー倍は許されているので、適当にスカラー倍することにより $\phi_g^{|g|} = 1$ としてよい。このとき ϕ_g は U 上に半単純に作用し、次のように U は固有空間分解をする;

$$U = U^0 \oplus U^1 \oplus \cdots \oplus U^{|g|-1}, \quad U^r = \{u \in U \mid \phi_g \cdot u = e^{2\pi i r / |g|} u\}.$$

この分解は先程行った ϕ_g の正規化の仕方に依存することに注意する。この分解を基に $U \times W_g^1 \rightarrow W_g^2$ 型の ϕ_g -ツイスト交絡作用素を次の様に定義する。

定義 1. $U \times W_g^1 \rightarrow W_g^2$ 型の交絡作用素であるとは、線形写像

$$I: U \otimes W_g^1 \rightarrow W_g^2\{z\}$$

$$u \otimes w^1 \mapsto I(u, z)w^1 = \sum_{s \in \mathbb{C}} (u, w^1) z^{-s-1}$$

であって、以下の公理を満たすものである;

1° $u \in U^r, w^1 \in W_g^1$ に対して

$$I(u, z)w^1 \in W_g^2((z))z^{-r/|g|-h_0-h_1+h_2};$$

2° $I(L(-1)u, z) = \frac{d}{dz} I(u, z)$;

3° $a \in V, ga = e^{2\pi ir/|g|}a$ に対して次の *twisted Jacobi identity* が成り立つ;

$$z_0^{-1} \delta \left(\frac{z_1 - z_2}{z_0} \right) Y^2(a, z_1) I(u, z_2) - z_0^{-1} \delta \left(\frac{-z_2 + z_1}{z_0} \right) I(u, z_2) Y^1(a, z_1)$$

$$= z_2^{-1} \delta \left(\frac{z_1 - z_0}{z_2} \right) \left(\frac{z_1 - z_0}{z_2} \right)^{-r/|g|} I(Y^0(a, z_0)u, z_2).$$

定義から上の交絡作用素は U の分解の仕方に依存しており、これは安定化自己同型 ϕ_g の正規化に依っている。やや天下り的に定義してきたが、 V の g による固有値分解を

$$V = V^0 \oplus V^1 \oplus \dots \oplus V^{|g|-1}$$

とすると、先程の正規化は V^0 -加群として V と U の間には次のフュージョン規則

$$V^r \times U^s = U^{r+s}$$

が成り立つことを要請していることと同値である。この関係を明示するために安定化自己同型を用いた。

定義より I は各ツイスト加群上の頂点作用素と局所可換性

$$(z-w)^N Y^2(a, z) I(u, w) = (z-w)^N I(u, w) Y^1(a, z) \quad \text{for } N \gg 0$$

を満たすことが確認できる。以後、 $U \times W_g^1 \rightarrow W_g^2$ 型のツイスト交絡作用素全体のなす線形空間を $I_\phi \left(\begin{smallmatrix} W_g^2 \\ U \ W_g^1 \end{smallmatrix} \right)$ で表す。

3 両側加群 $A_{\phi_g}(U)$ とツイスト交絡作用素

[Z]において、与えられたVOA V からその商空間として結合代数 $A(V)$ が構成された。そして既約 $A(V)$ -加群と既約 V -加群の間には一対一対応があることが示された。 V から $A(V)$ を構成する手続きを V -加群 W においても同様に行うことができ、 $A(V)$ -両側加群 $A(W)$ が構成される (cf. [FZ])。先程の対応定理は $I\left(\begin{smallmatrix} X \\ V \end{smallmatrix}\right)$ 型の交絡作用素を構成することに他ならず、 $A(W)$ を用いることによりその一般化あたる次の定理が Li によって示されている [L];

定理 1. (Li) V が有理型であるとき線形空間として次の同型が成り立つ;

$$I\left(\begin{smallmatrix} W^2 \\ W^0 \ W^1 \end{smallmatrix}\right) \simeq \text{Hom}_{A(V)}\left(A(W^0) \otimes_{A(V)} W^1(0), W^2(0)\right).$$

ここで $W^i(0)$ は W^i のトップレベルを表す。

この定理を先程定義したツイスト加群上のツイスト交絡作用素の場合にまで拡張する。それにはまず $A(V)$, $A(W)$ に対応するものを定義する必要がある。 $A(V)$ のツイスト版 $A_g(V)$ は既に [DLM1] において構成されており、既約 g -ツイスト V -加群と既約 $A_g(V)$ -加群の間には一対一対応があることが示されている。そこで V -加群から $A_g(V)$ -加群を構成する。

(U, ϕ_g) を g -安定 V -加群とする。このとき U は ϕ_g の作用で固有空間分解する。即ち $U^r := \{u \in U \mid gu = e^{2\pi ir/|g|}u\}$ として

$$U = U^0 \oplus U^1 \oplus \dots \oplus U^{|g|-1}$$

と分解する。同様に g の作用で V も固有空間分解をする;

$$V = V^0 \oplus V^1 \oplus \dots \oplus V^{|g|-1}.$$

$a \in V^r, u \in U$ として V の U への作用を以下のように定義する。

$$a \circ_g u := \text{Res}_z \frac{(1+z)^{wt_a-1 + \frac{r}{|g|} + \delta_{r,0}}}{z^{1+\delta_{r,0}}} Y^U(a, z)u.$$

そして $a \in V^0, u \in U^0$ について

$$\begin{aligned} a *_g u &:= \text{Res}_z \frac{(1+z)^{wt_a}}{z} Y^U(a, z)u \\ u *_g a &:= \text{Res}_z \frac{(1+z)^{wt_a-1}}{z} Y^U(a, z)u \end{aligned}$$

と定義する。ここで Res_z は形式的留数を意味し、 z^{-1} の係数をとることとする。そして積 \circ_g を用いて U の部分空間を

$$O_g(U) := \langle a \circ_g u \mid a \in V, u \in U \rangle$$

とおくとき、 $g = 1$ のときの拡張として次の定理が成り立つことを示した。

定理 2. 商空間 $A_g(U) := U^0/O_g(U) \cap U^0$ は上で定義した作用 $*_g$ で $A_g(V)$ -両側加群となる。

$A_g(U)$ を用いてツイスト加群間のフュージョン規則が決定できる。 $W_g^i = \bigoplus_{n \in \frac{1}{|g|}\mathbb{Z}} (W_g^i)_{n+h_i}$ を既約 g -ツイスト V -加群とする。これらのトップレベル $(W_g^i)_{h_i}$ を $W_g^i(0)$ で表す。 I が $U \times W_g^1 \rightarrow W_g^2$ 型の交絡作用素であるとき、 U の I による次数を保つ作用 (ゼロモード) o^I を考える。 o^I をトップレベルに制限して考えると、これは $W_g^1(0)$ から $W_g^2(0)$ への写像になっている。このとき $a \in V^0, u \in U^0$ として

$$o^I(a *_g u)|_{W_g^1(0)} = o^V(a)|_{W_g^2(0)} o^I(u)|_{W_g^1(0)}$$

$$o^I(u *_g a)|_{W_g^1(0)} = o^I(u)|_{W_g^1(0)} o^V(a)|_{W_g^2(0)}$$

$$o^I(O_g(U))|_{W_g^1(0)} = 0$$

が成り立つ。即ち、この関係式から次の命題が成立する。

命題 1. (Li) $I \mapsto o^I$ は線形写像

$$I_\phi \left(\begin{array}{c} W_g^2 \\ U \\ W_g^1 \end{array} \right) \rightarrow \text{Hom}_{A_g(V)} \left(A_g(U) \otimes_{A_g(V)} W_g^1(0), W_g^2(0) \right)$$

を与える。さらにこの写像は単射である。

上の対応は V が有理型るときには同型を与えることが示せる。これは Li の定理 ([L]) のツイスト交絡作用素への拡張になっている。

定理 3. V を g -rational VOA、 W_g^1, W_g^2 が既約 g -twisted V -module とするとき、対応 $I \mapsto o^I$ により次の同型が成り立つ：

$$I_\phi \left(\begin{array}{c} W_g^2 \\ U \\ W_g^1 \end{array} \right) \simeq \text{Hom}_{A_g(V)} \left(A_g(U) \otimes_{A_g(V)} W_g^1(0), W_g^2(0) \right)$$

4 トレース関数

G を $\text{Aut}(V)$ の有限部分群、 W を既約 V -加群とする。任意の $g \in G$ に対して $W \circ g \simeq W$ であるとき、 W を G -安定であるという。このとき各 $g \in G$ に対して

$$Y^W(ga, z) = \phi(g) Y^W(a, z) \phi(g)^{-1}$$

が任意の $a \in V$ について成り立つ $\phi_g \in GL(W)$ が存在する。各 $g \in G$ に対して $\phi(g)$ を決めて固定しておく。このとき W の既約性から $\phi(gh) = \lambda(g, h)\phi(g)\phi(h)$ となる $\lambda(g, h) \in \mathbb{C}$ が G の 2 元 g, h をとる毎に定まる。この $\lambda(g, h)$ は G 上の 2-コサイクルになっており、 $\phi(g)$ はスカラー倍を除いて一意に定まることから λ の定めるコホモロジーの同値類は一意に定まる。この射影表現に関して [DY] において V の G -invariants V^G と λ による G のツイスト群環は W 上 dual pair をなしており、 V^G -加群として W は完全可約になることなどが示されている。このように G -安定な加群はオービフォールド VOA の表現として特に興味深いものである。今回、 G として互いに可換な 2 元 g, h を $\text{Aut}(V)$ からとり、これらが生成する可換群 $\langle g, h \rangle$ の場合を考える。 U を G -安定な既約 V -加群とし、(1) を満たす G の U 上の自己同型写像を $\phi: G \rightarrow GL(U)$ とする。一般に $\langle \phi_g, \phi_h \rangle$ は $\langle g, h \rangle$ の U 上の射影表現を与えるが、ここではコサイクルが自明になる場合、即ち適当にスカラー倍を施すことにより ϕ は群準同型 $\phi: \langle g, h \rangle \rightarrow GL(U)$ を与えるものと仮定する。 W を g -ツイスト h -安定 V -加群、 ψ_h をその h -安定化自己同型として $I_\phi(U, W)$ 型のツイスト交絡作用素で次の条件を満たしているもの考える。

$$\psi_h I(u, z) = I(\phi_h u, z) \psi_h. \tag{2}$$

このような交絡作用素 I を用いて次で定義される \bar{W} 上のトレース関数を考える:

$$S^I(u, \tau) := z^{\text{wt}u} \text{tr}_{|W} I(u, z) \psi_h^{-1} q^{L_0 - c/24}.$$

上のトレース関数はこの段階では q を不定元としての形式的巾級数であるが、 U がある有限条件を満たすときには τ を複素上半平面の点として $q = e^{2\pi i \tau}$ と代入することで正則関数に収束することが示せる。そのためのいくつかの定義を示しておく。

定義 2. $(V, Y(-, z), \mathbb{1}, \omega)$ を VOA とする。このとき変数変換された頂点作用素

$$Y[a, z] = Y(a, e^z - 1) e^{\text{wt}(a)z} = \sum_{n \in \mathbb{Z}} a_{[n]} z^{-n-1}$$

に関して $(V, Y[-, z], \mathbb{1}, \hat{\omega} = \omega - \frac{c}{24} \mathbb{1})$ もまた VOA となる。これを指数変形 VOA と呼ぶ。

U が g -安定な V -加群であるとき、これは指数変形された V -加群でもある。新しいヴィラソロ元 $\hat{\omega}$ の頂点作用素 $Y[\hat{\omega}, z] = \sum_{n \in \mathbb{Z}} L[n] z^{-n-1}$ の $L[0]$ に関する次数分解を四角括弧で $U = \bigoplus_{n=0}^{\infty} U_{[n+h]}$ と表すことにする。ここで h は U のトップレベルの (L_0) ウェイトである。

次の有限条件は [M] で導入された。

定義 3. U が $C_{[2,0]}$ -条件を満たしているとは $C_{[2,0]}(U) := \langle a_{[-2]}u, b_{[0]}u \mid a \in V, b \in V^{(g,h)}, u \in U \rangle$ とおくと、 $\dim(U/C_{[2,0]}(U)) < \infty$ であることとする。

この条件は通常仮定される C_2 -条件より弱い条件である。この有限条件から次が従う。

定理 4. U が $C_{[2,0]}$ -条件を満たしているとき $S^I(u, \tau)$ は複素上半平面上の正則関数に収束する。

トレース関数の保型性を考えるにはそれらが持つ性質を調べなければならない。ポイントは各トレース関数 S^I が抽象的に定義されるある関数空間 $C_1(g, h)$ の元になることを示すところであるが、詳細は複雑な記号の準備などが必要なためここでは省略する。詳しくは [DLM2], [Y] を参照して頂きたい。

定理 5. U を (g, h) -安定な既約 V -加群とし、 $C_{[2,0]}$ -条件を満たしていると仮定する。 W を h -安定 g -ツイスト V -加群としたとき、 $U \times W \rightarrow W$ 型のツイスト交絡作用素 I で条件 (2) を満たしているとき、 I から得られるトレース関数 S^I は $C_1(g, h)$ の元になる。

重要なのは関数空間 $C_1(g, h)$ の持つ次の性質である。

定理 6. $S \in C_1(g, h)$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $u \in U_{[k]}$ に対して

$$S|\gamma(u, \tau) := S|_k\gamma(u, \tau) = (c\tau + d)^{-k}S(u, \gamma\tau)$$

と定めるとき、 $S|\gamma \in C_1(g^a h^c, g^b h^d)$ である。

この定理から $a, b, c, d \in \mathbb{Z}$ を $a \equiv d \equiv 1 \pmod{\text{lcm}(|g|, |h|)}$, $b \equiv 0 \pmod{|g|}$, $c \equiv 0 \pmod{|h|}$ として行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ らのなす $SL_2(\mathbb{Z})$ の部分群を $\Gamma(g, h)$ とするとき $C_1(g, h)$ は $\Gamma(g, h)$ で不変であることが分かる。それゆえ、もしトレース関数が $C_1(g, h)$ を張っていればトレース関数の張る空間の保型性が示される。

5 保型性

トレース関数の張る空間の保型性を示すには S^l が $C_1(g, h)$ を張っていることを示せばよいことは前節で示した。 $C_1(g, h)$ の各元はある微分方程式を満たしており、Frobenius-Fuchs の理論からその解はある程度具体的に書き下すことができる (cf. [DLM2],[AM])。そこで逆にこの解を調べることで $C_1(g, h)$ の元はすべてトレース関数の和で表されることを示すというのが Zhu の行った論法である。ここでは簡単にその説明を行う。先程の微分方程式の解は

$$T(u, \tau) = q^\lambda \sum_{n=0}^{\infty} \alpha_n(u) q^{n/|g|} \cdot (\log q)^n$$

という形の関数の線形和で表される。このトップの係数 $\alpha_0 : U \rightarrow \mathbb{C}$ が $A_g(U)$ と関係している。

補題 1. 上に書いた α_0 は次の性質を満たす:

(i) $ga = a, ha = \xi a, a \in V, \phi_g a = a, \phi_h a = \zeta a, u \in U, \xi, \zeta \in \mathbb{C}$ に対して $\alpha_0(a *_g u) = \xi^{-1} \delta_{\zeta, 1} \alpha_0(u *_g a)$;

(ii) $u \in O_g(U)$ に対して $\alpha_0(u) = 0$;

(iii) $\exists N > 0$ s.t. 任意の $u \in U$ に対して $\alpha_0((\omega *_g - c/24 - \lambda)^N u) = 0$.

この補題から α_0 は $A_g(U)$ から \mathbb{C} への線形写像であることが分かる。さらに上の補題 (i), (iii) から次の補題を示すことができる。

補題 2. 線形写像 α_0 は、(2) を満たす主 h -安定な g -ツイスト加群 $(\bar{W}_i, \psi_h^{(i)})$ 上の交絡作用素 $I_i \in I_\phi(U, \bar{W}_i)$ を用いて

$$\alpha_0(u) = \sum_i c_i \text{tr}_{\bar{W}_i(0)} o^h(u) \psi_h^{(i)}$$

と表される。

この補題によって α_0 は $\text{Hom}_{A_g(V)}(A_g(U) \otimes_{A_g(V)} \bar{W}(0), \bar{W}(0))$ の元によるトレース関数で表される。よって対応定理 3 を用いることにより T のトップの係数から先程のトレース関数を作れる。 T とこのトレース関数の差を取ったものを T' と置くと、このトップ項もまた T と同じく補題 1 を満たしており、作り方から $\lambda' > \lambda$ となっている。よってこのトップ項を考えることにより、 T' は別の h -安定 g -ツイスト加群上のトレース関数を含んでいることが分かる。今、 V は g -有理

型であるから、 h -安定 g -ツイスト加群の数は有限である。そのため、この操作も有限回で止まらなければならない。即ち T はトレース関数の和で表されるのである。それゆえ、次の主定理が得られる。

定理 7. U を既約 (g, h) -安定 V -加群とし、 $C_{[2,0]}$ -条件を満たしているとする。 $\{(\bar{W}_g^i, \psi_h)\}_{i=1, \dots, m}$ を h -安定 g -ツイスト V -加群全体とし、 $I \in I_\phi(U, \bar{W}_g^i)$ を (2) を満たす ϕ_g -ツイスト交絡作用素とすると、このような I から得られるトレース関数

$$S^I(u, \tau) = z^{wtu} \text{tr}_{\Gamma_{UV}} I(u, z) \psi_h^{-1} q^{L_0 - c/24}$$

は $q = e^{2\pi i \tau}$ として $\tau \in \mathcal{H}$ において収束し、このトレース関数で張られる空間 $\langle S^I \rangle$ は $\Gamma(g, h)$ の作用で不変である。

この結果により [DLM2] および [M] で得られている結果が一つの定理として述べられる。[M] では具体的に例を挙げてトレース関数から得られる保型形式を与えているが、我々の結果を応用できる具体例は分かっていない。ツイスト加群の具体的な構成がより一般に出来れば具体例も調べることができる。

参考文献

- [AM] G. Anderson and G. Moore, Rationality in conformal field theory, *Comm. Math. Phys.* 117 (1988), 441-450.
- [DLM1] C. Dong, H. Li, G. Mason, Twisted representations of vertex operator algebras, *Math. Ann.* 310 (1998) 571-600.
- [DLM2] C. Dong, H. Li, G. Mason, Modular-invariance of trace functions in orbifold theory, *Comm. Math. Phys.* 214, 1-56.
- [DY] C. Dong, G. Yamskulna, Vertex operator algebras, generalized doubles and dual pairs, *q-alg/0006005*.
- [FZ] I. Frenkel and Y. C. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, *Duke Math. J.* 66 (1992), 123-168.
- [L] H. Li, Determining Fusion Rules by $A(V)$ -Modules and Bimodules, *J. Algebra* 212, 515-556

- [M] M. Miyamoto, Intertwining operators and modular invariance, q-alg/0010180.
- [X] X. Xu, Intertwining operators for twisted modules of a colored vertex operator superalgebra, J. Algebra 175, 241-273.
- [Y] H. Yamauchi, Orbifold Zhu's theory associated with intertwining operators, preprint.
- [Z] Y.Zhu, Modular invariance of characters of vertex operator algebras, J. Amer. Math. Soc. 9 (1996), 237-302.

Cosets of extremal doubly-even codes of length $24n + 16$ and 1-designs

田辺顕一朗
筑波大学数学系

tanabe@math.tsukuba.ac.jp

1 イントロダクション

C を二元体 \mathbb{F}_2 上の長さ $N = 24n + 16$ の extremal doubly-even self-dual code とします。この講演では次の定理が証明できたことを報告します。

定理 1 U をウェイト $4n + 2$ の C のコセットで、ウェイト $4n + 4$ の元を持たないものとする。この時、 $\{u \in U \mid \text{wt}(u) = i\}$ ($\forall i$) は 1-デザインをなす。

以下、定理に使われている用語とこの問題を考えた動機を紹介していきます。 \mathbb{F}_2^N の部分空間 C を線形符号といいます。 $u := (u_i), v := (v_i) \in \mathbb{F}_2^N$ に対して u のウェイト $\text{wt}(u) = |\{i \mid u_i \neq 0\}|$ と、 u と v との内積 $(u, v) := \sum_{i=1}^N u_i v_i$ を定義します。 $C^\perp := \{v \in \mathbb{F}_2^N \mid (u, v) = 0, \forall u \in C\}$ を C の双対符号といいます。 $C = C^\perp$ となる符号は self-dual であると呼ばれます。また任意の $u \in C$ に対して $\text{wt}(u)$ が 4 の倍数となっている符号 C は doubly-even であると呼ばれます。

符号 C に対してその最小距離 $d(C) := \min\{\text{wt}(u) \mid 0 \neq u \in C\}$ を定義します。 C が doubly-even self-dual である場合には $d(C)$ に対して上限:

$$d(C) \leq 4 \lfloor \frac{N}{24} \rfloor + 4.$$

が知られています (cf. [5])。 $d(C)$ が上の式で上限に達する符号は extremal であると呼ばれます。

符号 C には最小距離とは別に被覆半径と呼ばれる値 $\rho(C)$ が定義されます。 $\rho(C)$ は次を満たす整数 r の最小値として定義されます:

$$\mathbb{F}_2^N = \cup_{c \in C} \{a \in \mathbb{F}_2^N \mid \text{wt}(a - c) \leq r\}.$$

$\rho(C)$ には次の上限が知られていて Delsarte bound と呼ばれています。

定理 2 [2]

$$\rho(C) \leq \lfloor \frac{\text{wt}(u)}{4} \rfloor \text{ for } 0 \neq u \in C^\perp.$$

被覆半径 $\rho(C)$ に対して

$$\rho(C) = \max_{a \in \mathbb{F}_2^N} \min_{c \in C} \text{wt}(a + c).$$

が成立することが簡単に確かめられます。この式から剰余類 \mathbb{F}_2^N/C の全ての元 $a + C$ (コセットと呼ばれる) に対してウェイト分布 $\{\text{wt}(u) \mid u \in a + C\}$ が計算できれば、 $\rho(C)$ が決定できることが分かります。

被覆半径の定義から、その値が小さい符号に興味があるわけです。Extremal double-even self-dual code の範囲では、被覆半径が Delsarte bound より真に小さくなる例が、2000年に山形大学の原田と小関 [4] によって初めて構成されました。この符号 C_{40} の長さは 40 で、この場合の Delsarte bound は 8 ですが $\rho(C_{40}) = 7$ となっています。

同時に彼らによって、その符号のコセットに対して興味深い観察がなされました。

定理 3 [4] C_{40} には、ウェイト 6 のコセットでウェイト 8 の元を持たないものが 6 個ある。 U をそのようなコセットの一つとすると、 $\{u \in U \mid \text{wt}(u) = i\}$ ($\forall i$) は 1-デザインをなす。

ここでコセット U のウェイトは $\text{wt}(U) := \min\{\text{wt}(u) \mid u \in U\}$ で定義しています。符号とデザインの関係については次の定理 4 がよく知られています。コセットに対して定理 4 の類似を与え、上記の観察の説明をコセット重み分布の方から与えたいと思ったのが研究の動機です。

定理 4 (cf. [5]) C を長さ N の extremal double-even self-dual code とする。この時、任意の i に対して $\{u \in C \mid \text{wt}(u) = i\}$ は t -デザインをなす。ここで

$$t = \begin{cases} 5, & \text{if } N \equiv 0 \pmod{24}, \\ 3, & \text{if } N \equiv 8 \pmod{24}, \\ 1, & \text{if } N \equiv 16 \pmod{24}. \end{cases}$$

である。

定理 1 を得た当時は、被覆半径が小さくなると定理の条件を満たすコセットが存在するのだろうか？ もしそうなら被覆半径が小さな符号の研究に役立たないかとも考えていました。しかし、最近、山形大学の原田と九州大学の宗政によって被覆半径が 7 の符号で、そのようなコセットを持たない例が構成されてしまい、結局被覆半径とは関係のない現象であることが分かりました。

最後にデザインの定義を一応紹介しておきます。 V を $\{1, 2, \dots, N\}$ の部分集合の全体からなる集合とし、 $X_i := \{A \subset \{1, 2, \dots, N\} \mid |A| = i\}$ とおきます。以下 V と \mathbb{F}_2^N を自然に同一視しておきます。

定義 1 t, i, λ を $t \leq i$ を満たす正の整数とする。 $B \subset X_i$ とする。任意の $T \in X_t$ に対して $|\{U \in B \mid T \subset U\}| = \lambda$ が成り立つとき、 B は t -デザインと呼ばれる。

2 定理1の証明のスケッチ

X_k, V の元を基底とする \mathbb{R} 上のベクトル空間 $\mathbb{R}X_k, \mathbb{R}V$ をそれぞれ考えます。 $f = \sum_{a \in X_k} f(a)a \in \mathbb{R}X_k$ に対して $\tilde{f} = \sum_{u \in X} \tilde{f}(u)u \in \mathbb{R}V$ を

$$\tilde{f}(u) := \sum_{\substack{a \in X_k \\ a \subset u}} f(a),$$

で定義します。微分 $\gamma: X_k \rightarrow X_{k-1}, (k = 0, 1, \dots, n)$ を $z \in X_k$ に対して

$$\gamma(z) = \sum_{y \in X_{k-1}, y \subset z} y.$$

で定義します。また $\text{Harm}_k = \text{Ker}(\gamma|_{\mathbb{R}X_k})$ を定義します。以上の準備の下で以下の結果が知られています。

補題 5 [3] i, t を $0 \leq t \leq i \leq n$ を満たす整数とする。 $B \subset X_i$ とする。この時、

$$\begin{aligned} & B \text{ は } t\text{-デザイン} \\ \Leftrightarrow & \sum_{b \in B} \tilde{f}(a) = 0, \forall f \in \text{Harm}_k, 1 \leq \forall k \leq t. \end{aligned}$$

Bachoc[1] によって導入された harmonic weight enumerator を紹介します。

定義 2 U を \mathbb{F}_2^N の部分集合とする。 $f \in \text{Harm}_k$ とする。 U と f の harmonic weight enumerator を

$$W_{U,f}(x, y) := \sum_{u \in U} \tilde{f}(u) x^{N-\text{wt}(u)} y^{\text{wt}(u)}.$$

で定義する。

Harmonic weight enumerator に対して次の MacWilliams 型の等式が成立します。

補題 6 C を長さ N の符号とし、 $a \in V$ とする。 $f \in \text{Harm}_k$ とする。この時、次の等式が成り立つ:

$$\begin{aligned} & \sum_{v \in C^\perp} (-1)^{va} \tilde{f}(v) x^{N-\text{wt}(v)-k} y^{\text{wt}(v)-k} \\ &= \frac{(-2)^k}{|C|} \sum_{u \in a+C} \tilde{f}(u) (x+y)^{N-\text{wt}(u)-k} (x-y)^{\text{wt}(u)-k}. \end{aligned}$$

定理 1 の証明の概略を与えます。 C を長さ $N = 24n + 16$ の extremal doubly-even self-dual code とし、 $U = a + C$ を定理 1 の条件を満たすコセットとします。 $\text{Harm}_1 = \text{Span}_{\mathbb{R}}\{2b - 2b' \mid b, b' \in X_1\}$ に注意します。 U と全ての $f = 2(b - b'), (b, b' \in X_1)$ に対して補題 6 の式の右辺が 0 に等しいことが示されれば、補題 5 から定理が証明されます。ここで $\tilde{f}(v) = (-1)^{bv} - (-1)^{b'v}$ より、

$$\begin{aligned} (-1)^{av} \tilde{f}(u) &= (-1)^{av} ((-1)^{bv} - (-1)^{b'v}) \\ &= (-1)^{(a+b)v} - (-1)^{(a+b')v}. \end{aligned}$$

となります。また補題 6 を $1 \in \text{Harm}_0$ に適用すると、

$$\begin{aligned} & \sum_{v \in C} (-1)^{v(a+b)} x^{N-\text{wt}(v)} y^{\text{wt}(v)} \\ &= \frac{1}{|C|} \sum_{u \in a+b+C} (x+y)^{N-\text{wt}(u)} (x-y)^{\text{wt}(u)}. \end{aligned}$$

を得ます。これらを用いて $f = 2(b-b')$, $(b, b' \in X_1)$ と U に関する補題 6 の式の右辺を計算していきます。

$$\begin{aligned} (*) & \frac{-2}{|C|} \sum_{u \in a+C} \tilde{f}(u) (x+y)^{N-\text{wt}(u)-1} (x-y)^{\text{wt}(u)-1} \\ &= \sum_{v \in C} (-1)^{va} \tilde{f}(v) x^{N-\text{wt}(v)-1} y^{\text{wt}(v)-1} \\ &= \sum_{v \in C} (-1)^{v(a+b)} x^{N-\text{wt}(v)-1} y^{\text{wt}(v)-1} \\ &\quad - \sum_{v \in C} (-1)^{v(a+b')} x^{N-\text{wt}(v)-1} y^{\text{wt}(v)-1} \\ &= \frac{x^{-1}y^{-1}}{|C|} \left(\sum_{u \in a+b+C} (x+y)^{N-\text{wt}(u)} (x-y)^{\text{wt}(u)} \right. \\ &\quad \left. - \sum_{u \in a+b'+C} (x+y)^{N-\text{wt}(u)} (x-y)^{\text{wt}(u)} \right). \end{aligned}$$

を得ます。実は $\text{wt}(U) = 4n+2$ と U がウェイト $4n+4$ の元を持たないことから

$$\sum_{u \in a+b+C} (x+y)^{N-\text{wt}(u)} (x-y)^{\text{wt}(u)} = \sum_{u \in a+b'+C} (x+y)^{N-\text{wt}(u)} (x-y)^{\text{wt}(u)}.$$

が示されるので、式 (*) は 0 に等しいことが分かります。したがって補題 5 から定理は示されました。

References

- [1] C. Bachoc, On harmonic weight enumerators of binary codes, *Designs, Codes and Cryptography*, Vol. 18 (1999), 11-28.
- [2] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Information and Control* **23** (1973), 407-438.
- [3] P. Delsarte, Hahn polynomials, discrete harmonics, and t -designs, *SIAM J. Appl. Math.* Vol. 34 (1978) 157-166.
- [4] M. Harada and M. Ozeki, Extremal self-dual codes with the smallest covering radius, *Discrete Math.* **215** (2000), 271-281.

- [5] C. L. Mallows and N. J. A. Sloane, *The theory of error-correcting codes*. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

On Frames of the Niemeier Lattices

Masaaki Harada

Department of Mathematical Sciences
Yamagata University

and

Masaaki Kitazume

Department of Mathematics and Informatics
Chiba University

Abstract

In this manuscript, it is shown that every Niemeier lattice contains a $(4k^2 + 2k + 6)$ -frame for every integer k .

1 Introduction

The 24 even unimodular lattices in dimension 24 are called the Niemeier lattices, which are remarkable lattices. It is a fundamental problem to determine if a fixed even unimodular lattice is constructed from some self-dual code by Construction A. An even unimodular lattice L is constructed from some code over \mathbb{Z}_{2k} if and only if L contains a $2k$ -frame. Hence the above problem can be reworded as follows: determine if a fixed even unimodular lattice contains a $2k$ -frame.

Problem. For a fixed k , does every Niemeier lattice contain a $2k$ -frame?

Since there are only nine inequivalent binary doubly-even self-dual codes of length 24, the answer in the case $k = 1$ is negative. Recently, the problem in the case $k = 2$ have been settled in [3] (see also [8]). In this manuscript, we have the following:

Theorem 1. *Every Niemeier lattice N contains a $(4k^2 + 2k + 6)$ -frame for every integer k . In other words, every Niemeier lattice is constructed from some Type II code over \mathbb{Z}_{4k^2+2k+6} .*

This is a partial answer of the above problem.

2 Preliminaries

Let \mathbb{Z}_{2k} ($= \{0, 1, 2, \dots, 2k - 1\}$) be the ring of integers modulo $2k$. A code C of length n over \mathbb{Z}_{2k} (or a \mathbb{Z}_{2k} -code of length n) is a \mathbb{Z}_{2k} -submodule of \mathbb{Z}_{2k}^n . An element of C is called a codeword. We define the inner product on \mathbb{Z}_{2k}^n by $x \cdot y = x_1 y_1 + \dots + x_n y_n$, where $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$. The dual code C^\perp of C is defined as $C^\perp = \{x \in \mathbb{Z}_{2k}^n \mid x \cdot y = 0 \text{ for all } y \in C\}$. A code C is *self-dual* if $C = C^\perp$. The Hamming weight of a codeword is the number of non-zero components in the codeword. The Euclidean weight of a codeword x is $\sum_{i=1}^n \min\{x_i^2, (2k - x_i)^2\}$. The minimum Euclidean weight d_E of C is the smallest Euclidean weight among all nonzero codewords of C . A Type II code over \mathbb{Z}_{2k} is a self-dual code with all codewords having Euclidean weight divisible by $4k$. It is known [2] that there is a Type II code of length n if and only if $n \equiv 0 \pmod{8}$.

A (Euclidean) lattice Λ is *integral* if $\Lambda \subseteq \Lambda^*$ where Λ^* is the dual lattice under the standard inner product $\langle x, y \rangle$. An integral lattice with $\Lambda = \Lambda^*$ is called *unimodular*. A lattice with even norms is said to be *even*. An n -dimensional even unimodular lattice exists if and only if $n \equiv 0 \pmod{8}$. The minimum norm of Λ is the smallest norm among all nonzero vectors of Λ . Up to equivalence, there are 24 even unimodular lattices in dimension 24 (called the Niemeier lattices) and one of them has minimum norm 4 (called the Leech lattice).

We now introduce Construction A to construct even unimodular lattices from Type II codes over \mathbb{Z}_{2k} . Construction A was first defined for binary codes (cf. [5, Chap. 7]), and was generalized to codes over \mathbb{Z}_{2k} (cf. [2]). Let C be a \mathbb{Z}_{2k} -code C and let e_1, \dots, e_n be an orthogonal basis of an n -dimensional Euclidean space satisfying $\langle e_i, e_j \rangle = 2k\delta_{ij}$ where δ_{ij} is the Kronecker delta. Then we define the lattice $A_{2k}(C)$ obtained from C by Construction A as

$$A_{2k}(C) = \left\{ \frac{1}{2k} \sum_{i=1}^n x_i e_i \mid x_i \in \mathbb{Z}, (x_i \pmod{2k}) \in C \right\}.$$

In general, the set of vectors f_1, \dots, f_n in an n -dimensional lattice L with $\langle f_i, f_j \rangle = 2k\delta_{ij}$ is called a $2k$ -frame of L . Clearly $A_{2k}(C)$ has a $2k$ -frame e_1, \dots, e_n . Conversely if the lattice L has a $2k$ -frame f_1, \dots, f_n , then L is obtained by Construction A from some \mathbb{Z}_{2k} -code C' which is defined as

$$C' = \{(c_1, \dots, c_n) \in \mathbb{Z}_{2k}^n \mid c_i = \langle v, f_i \rangle \pmod{2k}, v \in L\}.$$

If C is a Type II \mathbb{Z}_{2k} -code with minimum Euclidean weight d_E then $A_{2k}(C)$ is an even unimodular lattice with minimum norm $\min\{d_E/2k, 2k\}$ [2].

3 Proof

The aim of this section is to give a proof of Theorem 1. We want to emphasize that our proof is unified by using the result (1) of Dong, Li, Mason and Norton.

Let H be a Hadamard matrix of order n , that is, an n by n matrix of ± 1 's with $H \cdot H^T = nI$ where H^T denotes the transpose of H . A Hadamard matrix H is called skew-symmetric if $(H - I)^T = -(H - I)$.

Lemma 2. *Let H be a skew-symmetric Hadamard matrix of order 24. Let h_i denote the i -th row of H . If N contains $h_1/2, \dots, h_{24}/2$ and the 4-frame*

$$\{e_1 = (2, 0, \dots, 0), e_2 = (0, 2, 0, \dots, 0), \dots, e_{24} = (0, \dots, 0, 2)\},$$

then N has a $(4k^2 + 2k + 6)$ -frame for any integer k .

Proof. Let k be any integer. We will show that $\{h_1/2 + ke_1, \dots, h_{24}/2 + ke_{24}\}$ is a $(4k^2 + 2k + 6)$ -frame in N . For any i, j ,

$$\langle h_i/2 + ke_i, h_j/2 + ke_j \rangle = \begin{cases} k(h_{ij} + h_{ji}) & \text{if } i \neq j, \\ 4k^2 + 2k + 6 & \text{if } i = j, \end{cases}$$

where h_{ij} denotes the j -th coordinate in h_i . Since H is skew-symmetric, $h_{ij} + h_{ji} = 0$ if $i \neq j$. The result follows. \square

Recall that the torsion part $C^{(2)}$ of a \mathbb{Z}_4 -code C is defined as

$$C^{(2)} = \left\{ \frac{1}{2}c \mid c \in C, c_i \equiv 0 \pmod{2} \right\}$$

where $C^{(2)}$ is regarded as a binary code.

Lemma 3. *Let C be a Type II \mathbb{Z}_4 -code of length 24. If $C^{(2)}$ contains some code equivalent to the extended Golay code G_{24} then C contains a skew-symmetric Hadamard matrix of order 24*

Proof. Let H be a Hadamard matrix with the i -th row h_i . Then the binary code generated by $(1/2)(h_1 - h_i)$ ($2 \leq i \leq 24$) is classified in [1, Table 7.1] and is equivalent to one of the six Type II codes $A_{24}, C_{24}, D_{24}, E_{24}, F_{24}, G_{24}$. In particular, if H is the Paley skew-symmetric Hadamard matrix P (see e.g., [1] for the definition), then this binary code is equivalent to G_{24} . We denote by p_i the i -th row of P . Then we may assume that p_1 is the all-one vector.

Suppose that $C^{(2)}$ contains some code equivalent to G_{24} . Then C contains some codewords obtained from $p_1 - p_i$ ($2 \leq i \leq 24$) by some suitable permutation. Here we regard the vectors p_i as codewords of a \mathbb{Z}_4 -code. Moreover it is known that any Type II \mathbb{Z}_4 -code contains some codeword whose entries are ± 1 . Hence C contains all the rows of $P \cdot M$ for some monomial matrix M . The matrix $M^T \cdot P \cdot M$ is a skew-symmetric Hadamard matrix whose row vectors are contained in C . \square

We now are in a position to describe a result by Dong, Li, Mason and Norton [6], which is an important key of our proof. They showed that there exists an embedding

$$(1) \quad \Lambda_{24} \supseteq \sqrt{2}N \supseteq 2\Lambda_{24}$$

of each Niemeier lattice N into the Leech lattice Λ_{24} . The following lemma is obtained as a consequence of (1).

Lemma 4 (Bonnecaze et al. [3]). *Every Niemeier lattice N contains a 4-frame.*

Indeed by using (1), it is proved that $\sqrt{2}N$ contains a *coordinate frame* (in the sense of [5, Chap. 10]) $\{g_1, \dots, g_{24}\}$ of Λ_{24} , which is an 8-frame of Λ_{24} . Hence $\{g_1/\sqrt{2}, \dots, g_{24}/\sqrt{2}\}$ becomes a 4-frame of N , and thus N is written as

$$N = A_4(C) = \left\{ \frac{1}{4} \sum_{i=1}^{24} x_i \frac{g_i}{\sqrt{2}} \mid x_i \in \mathbb{Z}, (x_i \pmod{4}) \in C \right\},$$

from some Type II \mathbb{Z}_4 -code C by Construction A.

We will show $C^{(2)} \supset G_{24}$. The construction of the Leech lattice Λ_{24} from the binary extended Golay code G_{24} and the coordinate frame is well known (cf. [5]). From the construction, Λ_{24} contains a sublattice

$$L_B(G_{24}) = \left\{ \frac{1}{2} \sum_{i=1}^{24} x_i \frac{g_i}{2} \mid x_i \in \mathbb{Z}, (x_i \pmod{2}) \in G_{24}, \sum_{i=1}^{24} x_i \in 4\mathbb{Z} \right\}$$

constructed from G_{24} by Construction B. It follows from (1) that N contains the sublattice

$$\sqrt{2}L_B(G_{24}) = \left\{ \frac{1}{4} \sum_{i=1}^{24} 2x_i \frac{g_i}{\sqrt{2}} \mid x_i \in \mathbb{Z}, (x_i \pmod{2}) \in G_{24}, \sum_{i=1}^{24} 2x_i \in 8\mathbb{Z} \right\}.$$

This together with the 4-frame $\{g_1/\sqrt{2}, \dots, g_{24}/\sqrt{2}\}$ generates the sublattice $A_4(2G_{24})$ where $2G_{24}$ is regarded as a \mathbb{Z}_4 -code. Hence C contains $2G_{24}$ and thus we have proved the following:

Lemma 5. *For any Niemeier lattice N , there is a Type II \mathbb{Z}_4 -code C with $A_4(C) = N$ such that $C^{(2)}$ contains G_{24} .*

The above lemma together with Lemmas 2 and 3 shows that every Niemeier lattice N contains a $(4k^2 + 2k + 6)$ -frame for every integer k . Therefore the proof of Theorem 1 is completed. It is worthwhile noting that the authors [8] have constructed a Type II \mathbb{Z}_4 -code C satisfying the condition in Lemma 5 by giving explicit generator matrices.

We end this manuscript with giving the following remarks:

- (1) Recently it is shown that there is a $2k$ -frame in the Leech lattice for every positive integer $k \geq 2$ [4] and [7]. By (1), every Niemeier lattice contains a $4k$ -frame for every positive integer k .
- (2) Montague [9] found ternary self-dual codes such that all the Niemeier lattices are obtained by two construction methods which are called the straight construction and the twisted constructions in his paper. By his construction (Section 4 in [9]), every Niemeier lattice N contains the sublattice equivalent to $\sqrt{3}$ times the root lattice of type D_n generated by $e_i \pm e_j$ ($1 \leq i, j \leq 24$) satisfying $\langle e_i, e_j \rangle = 3\delta_{ij}$. Hence N contains a 6-frame

$$\{f_1 = e_1 + e_2, f_2 = e_1 - e_2, f_3 = e_3 + e_4, \dots, f_{24} = e_{23} - e_{24}\}.$$

- (3) It follows from [4, Lemma 5.1] that if N contains an n -frame then it also contains an mn -frame for each positive integer m . Therefore every Niemeier lattice N contains an $m(4k^2 + 2k + 6)$ -frame for an integer k and a positive integer m .

References

- [1] E.F. Assmus, Jr. and J.D. Key, *Designs and Their Codes*, Cambridge Univ. Press, Cambridge, 1992.
- [2] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 257–269.
- [3] A. Bonnecaze, P. Gaborit, M. Harada, M. Kitazume and P. Solé, Niemeier lattices and Type II codes over \mathbb{Z}_4 , *Discrete Math.* **205** (1999), 1–21.
- [4] R. Chapman, Double circulant constructions of the Leech lattice, *J. Aust. Math. Soc. Ser. A* **69** (2000), 287–297.
- [5] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups* (3rd ed.), Springer-Verlag, New York, 1999.
- [6] C. Dong, H. Li, G. Mason and S.P. Norton, Associative subalgebras of the Griess algebra and related topics, *The Monster and Lie Algebras*, Ohio State Univ. Math. Res. Inst. Publ., 7, de Gruyter, Berlin, 1998, 27–42.
- [7] T.A. Gulliver and M. Harada, Orthogonal frames in the Leech lattice and a Type II code over \mathbb{Z}_{22} , *J. Combin. Theory Ser. A*, **95** (2001), 185–188.
- [8] M. Harada and M. Kitazume, \mathbb{Z}_4 -code constructions for the Niemeier lattices and their embeddings in the Leech lattice, *Eurp. J. Combin.* **21** (2000), 473–485.
- [9] P.S. Montague, A new construction of lattices from codes over $\text{GF}(3)$, *Discrete Math.* **135** (1994), 193–223.

A combinatorial problem in $SL(2, q)$

Sachiyo Terada

Abstract

For a power q of 2 greater than 2 and each natural number λ not divisible by $q - 1$, it is shown that the subset \mathcal{U} of involutions does not divide $\lambda SL(2, q)$. Moreover, it is conjectured that, for an orbit X of an involution by the conjugation of a Singer cycle of $SL(2, q)$, X does not divide $\lambda SL(2, q)$ if λ is not divisible by $q + 1$ and $q \neq 2$.

1 Preliminaries.

For a finite group G and its non-empty subset Ω , the Cayley graph $\Gamma(G, \Omega)$ is the graph with the vertex set $V\Gamma = G$ and the edge set $E\Gamma = \{(g, h) \mid gh^{-1} \in \Omega\}$. A subset C of the vertex set $V\Gamma$ of a graph Γ is called a *perfect e -code* if, for any vertex v of Γ , there is a unique codeword c in C such that $d(c, v) \leq e$. Perfect e -codes in the Cayley graph $\Gamma(G, \Omega)$ are perfect 1-codes in the Cayley graph $\Gamma(G, X)$, where X is the set of vertices x with $d(x, 1) \leq e$ in $\Gamma(G, \Omega)$. So when we consider perfect e -codes in a Cayley graph, we may assume $e = 1$.

For a subset X of a group G , we say X *divides* G (with a code Y) and write $X \cdot Y = G$ if there is a subset Y of G such that each element of G is uniquely described as xy with $x \in X$ and $y \in Y$.

Note that X divides G with a code Y if and only if G is covered by the disjoint sets $\{Xy \mid y \in Y\}$ in the metric space $\Gamma(G, X)$. If X contains the identity, Xy ($y \in Y$) is a sphere of radius 1 and so Y is a perfect 1-code in $\Gamma(G, X)$.

Examples. (1) (Symmetric group S_3) Let X_1 be the set of transpositions and X_2 be the alternating subgroup A_3 :

$$\begin{aligned} X_1 &:= \{(1\ 2), (2\ 3), (1\ 3)\}, \\ X_2 &:= \{\text{id}, (1\ 2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

Each of X_1 and X_2 divides S_3 with a code $Y = \{\text{id}, (1\ 2)\}$.

(2) (Dihedral groups D_{4n}) Take generators a and b of D_{4n} such that $a^2 = b^{2n} = 1$ and $aba^{-1} = b^{-1}$. Let X_j ($j = 1, 2$) be the conjugacy classes of involutions of size n :

$$X_j = \{ab^{2i+j} \mid i = 0, 1, \dots, n-1\}.$$

Then each of X_1 and X_2 divides D_{4n} with a code $Y = \{1, a, b, ab\}$.

Rothaus and Thompson [RT] give a necessary condition for a perfect 1-code to exist in a Cayley graph $\Gamma(S_n, T)$ for the union T of transpositions and the identity in the symmetric group S_n .

In general, for a subset X of G and a natural number λ , we say X divides λG (with a code Y) and write $X \cdot Y = \lambda G$ if there is a subset Y of G such that each element g of G has just λ descriptions as $xy = g$ with $x \in X$ and $y \in Y$. We say X trivially divides λG (with a code Y) if X divides λG with a code $Y = G$ or $Y = \{y\}$ for some $y \in G$.

Proposition 1 (An analogue of [RT]). *Let G be a finite group, X a non-empty subset of G and λ a natural number. Assume that G contains a subgroup H with property that*

- (1) *the order $|X|$ of X does not divide $\lambda|H|$, and*
- (2) *the matrix $P(\dot{X})$ is non-singular, where P is the permutation representation of G acting on the cosets $H \backslash G$ and \dot{X} is the sum of elements of X in the group algebra $\mathbb{C}[G]$ over the complex field \mathbb{C} .*

Then X does not divide λG .

Proof. Assume that X divides λG , that is, there is a subset Y of G such that $X \cdot Y = \lambda G$. Then $P(\dot{X})P(\dot{Y}) = P(\lambda \dot{G})$. By the assumption (2), there exists the inverse matrix $P(\dot{X})^{-1}$, which can be described as a polynomial of $P(\dot{X})$. Since $P(\dot{G}) = P(x)P(\dot{G})$ for any x in G , we have $P(\dot{Y}) = P(\dot{X})^{-1}P(\lambda \dot{G}) = aP(\lambda \dot{G})$ for some complex number a . Then, by multiplying the last equation by $P(\dot{X})$ from left, we have $a = |X|^{-1}$. Hence we have

$$P(\dot{Y}) = \frac{1}{|X|}P(\lambda \dot{G}) = \frac{\lambda}{|X|}P(\dot{G}) = \frac{\lambda|H|}{|X|}J,$$

where J is the matrix with all entries 1. This equation contradicts the fact that the matrix $P(\dot{Y})$ has integral entries. \square

Lemma 2. *If a subset X divides λG with a code $Y \neq G$, then the Cayley graph $\Gamma(G, X)$ has an eigenvalue 0.*

2 The case where the subset X is closed under conjugation.

Let us assume the subset X is closed under conjugation. Then, for an irreducible representation R of a finite group G , $R(\dot{X})$ is a scalar by Schur's lemma and the condition of Proposition 1(2) can be checked easily.

2.1 Symmetric groups S_n and transpositions.

Theorem 3 ([RT]). *Let T_0 be the set of transpositions of S_n .*

- (1) *If $1 + n(n-1)/2$ is divisible by a prime exceeding $\sqrt{n} + 2$, then $T := T_0 \cup \{\text{id}\}$ does not divide S_n .*
- (2) *If a prime exceeding $\sqrt{n} + 2$ divides $n(n-1)/2$, then T_0 does not divide S_n .*

Remark ([RT]). The numbers $n = 1, 2, 3, 6, 91, 137, 733$ and 907 are the only integers less than $1,000$ which do not have any prime satisfying the assumption of Theorem 3 (1), that is, n is one of the above if T divides S_n ($n \leq 1000$).

Note that the symmetric group S_3 is not divided by T since the sphere packing condition fails with $|T| = 4$ and $|S_3| = 6$. Moreover, we can prove that T does not divide S_6 , using a combinatorial argument or the fact that the graph $\Gamma(S_6, T)$ does not have eigenvalue 0 , that is, the graph $\Gamma(S_6, T_0)$ does not have eigenvalue -1 .

2.2 Symmetric groups S_n and three-cycles.

Theorem 4 ([Ta]). For a natural number n , let X be the union of three-cycles and the identity in the symmetric group S_n and let $n_0 := \max\{i \mid n \geq (3i - 1)i\}$. If a prime exceeding $1 + n/n_0$ divides $1 + n(n - 1)(n - 2)/3$, then the set X does not divide S_n .

Remark ([Ta]). The numbers $n = 2, 3, 4, 14$ and $4,065$ are the only integers less than $40,000$ which do not have any prime satisfying the assumption of Theorem 4, that is, n is one of the above if X divides S_n ($n \leq 40000$). For $n = 4$ and 14 , however, X does not divide S_n by the sphere packing condition. For $n = 3$, X divides S_3 as in the example of Section 1.

2.3 Special linear groups $SL(2, q)$ (q even, $q \neq 2$) and involutions.

In this section, let q be even and $q \neq 2$.

Theorem 5 (Te). For a natural number λ not divisible by $q - 1$, the set \mathcal{U} of involutions does not divide $\lambda SL(2, q)$.

The character table of $SL(2, q)$ is given in Table 1, where δ (resp. ε) is a primitive $(q - 1)$ -st (resp. $(q + 1)$ -st) root of unity in the complex number field \mathbb{C} .

Table 1: The irreducible characters of $SL(2, q)$

Class name	1	\mathcal{U}	\mathcal{T}_i ($i=1,2,\dots,(q-2)/2$)	\mathcal{S}_j ($j=1,2,\dots,q/2$)
Size	1	$q^2 - 1$	$q(q + 1)$	$q(q - 1)$
χ_0	1	1	1	1
χ_1	q	0	1	-1
ψ_m ($m=1,2,\dots,(q-2)/2$)	$q + 1$	1	$\delta^{mi} + \delta^{-mi}$	0
φ_n ($n=1,2,\dots,q/2$)	$q - 1$	-1	0	$-(\varepsilon^{nj} + \varepsilon^{-nj})$

Take a matrix representation $R(\vartheta)$ affording ϑ for an irreducible character ϑ and set

$$\mathcal{R} := \{R(\chi_0), R(\psi_m), R(\varphi_n) \mid m = 1, 2, \dots, (q - 2)/2, n = 1, 2, \dots, q/2\}.$$

Lemma 6. Take a Singer cycle S of $SL(2, q)$ (that is, S is a cyclic subgroup of order $q + 1$). The set \mathcal{R} coincides with the irreducible constituents of the permutation representation P of $SL(2, q)$ acting on the cosets $S \backslash SL(2, q)$. Each representation in \mathcal{R} is contained in P with multiplicity one: $P = \bigoplus_{R \in \mathcal{R}} R$.

Proof of Theorem 5. For each irreducible representation R of $SL(2, q)$, we have $R(\bar{U}) = cI$ for some $c \in \mathbb{C}$ by Schur's lemma. From the character table, $R(\bar{U})$ is non-singular if and only if \mathcal{R} contains R since $\text{tr}R(\bar{U}) = c \cdot \text{deg } R$ and c is nonzero. This implies that the matrix $P(\bar{U})$ is non-singular for the permutation representation P of $SL(2, q)$ acting on the cosets $S \backslash SL(2, q)$. Since $|\mathcal{U}| = (q + 1)(q - 1)$ and $|S| = q + 1$, the theorem holds by Proposition 1. \square

Suppose X is a non-trivial closed subset under conjugation and divides $\lambda SL(2, q)$ ($q = 2^f \geq 4$). Then X is one of the below with λ divisible by λ' in the table.

Subsets X	λ'
\mathcal{U}	$q - 1$
$G \setminus \mathcal{U}$	$(q - 1)^2$
$\bigcup_{j \in \mathcal{J}'} \mathcal{S}_j$	$ \mathcal{J}' $
$(\bigcup_{i \in \mathcal{I}_0} \mathcal{T}_i) \cup (\bigcup_{j \in \mathcal{J}'} \mathcal{S}_j)$	$ X /(p_0q)$
$1 \cup \mathcal{U} \cup (\bigcup_{i \in \mathcal{I}_1} \mathcal{T}_i) \cup (\bigcup_{j \in \mathcal{J}'} \mathcal{S}_j)$	$ X /(r_1q)$
$\bigcup_{i \in \mathcal{I}'} \mathcal{T}_i$	$ X /(p'q)$
$(\bigcup_{i \in \mathcal{I}'} \mathcal{T}_i) \cup (\bigcup_{j \in \mathcal{J}_0} \mathcal{S}_j)$	$ X /(p'q)$
$1 \cup \mathcal{U} \cup (\bigcup_{i \in \mathcal{I}'} \mathcal{T}_i) \cup (\bigcup_{j \in \mathcal{J}_1} \mathcal{S}_j)$	$ X /(r'q)$

where \mathcal{I}_k (resp. \mathcal{J}_k) ($k = 0, 1$) is a subset of the index set $\mathcal{I} := \{1, 2, \dots, (q - 2)/2\}$ (resp. $\mathcal{J} := \{1, 2, \dots, q/2\}$) such that

$$\sum_{i \in \mathcal{I}_k} (\delta^{mi} + \delta^{-mi}) = -k \quad (\text{resp.} \quad \sum_{j \in \mathcal{J}_k} (\varepsilon^{nj} + \varepsilon^{-nj}) = -k)$$

for some $m \in \mathcal{I}$ (resp. $n \in \mathcal{J}$), \mathcal{I}' (resp. \mathcal{J}') is a subset (possibly empty) of \mathcal{I} (resp. \mathcal{J}),

$$\begin{aligned} p_0 &:= \gcd(|\mathcal{I}_0|, q - 1), & p' &:= \gcd(|\mathcal{I}'|, q - 1), \\ r_1 &:= \gcd(1 + |\mathcal{I}_1|(q + 1), q - 1) \quad \text{and} \\ r' &:= \gcd(1 + |\mathcal{I}'|(q + 1), q - 1). \end{aligned}$$

Problem For each X in the table, determine whether X divides $\lambda SL(2, q)$ or not.

Note that if a subset $X \neq 1$ divides a group G with a code Y , then $|Y|$ is even. This fact and the list above settle the perfect 1-code problem in $SL(2, q)$ with $\lambda = 1$, that is, for a subset X closed under conjugation and a power q of 2, the special linear group $SL(2, q)$ is divided by X non-trivially if and only if $q = 2$.

3 The case where the subset X is not closed under conjugation.

Let λ be a natural number and let q be a power of 2. Take an orbit X of an involution by the conjugation of a Singer cycle of $SL(2, q)$. When does X divide $\lambda SL(2, q)$?

Conjecture. For $q \geq 4$, X does not divide $\lambda SL(2, q)$ if λ is not divisible by $q + 1$, that is, X does not divide $\lambda SL(2, q)$ non-trivially.

Remark. Let λ is a natural number which is not divisible by $q + 1$. Using Proposition 1, we have checked that X does not divide $\lambda SL(2, q)$ for $q = 4, 8$ and 16 .

References

- [RT] O. Rothaus and J. G. Thompson, A combinatorial problem in the symmetric group, *Pacific J. Math.*, 18(1966), 175–178.
- [Ta] T. Takematsu, in preparation.

Sachiyo Terada
Division of Mathematics and Computational Science,
Kanazawa University,
Kakuma-machi, Kanazawa, 920-1192
e-mail: terada@kappa.s.kanazawa-u.ac.jp

有限群の指標とその複素共役との積

千葉大学大学院自然科学研究科

波多野 順

1 Introduction

有限群 G の通常指標の全体は \mathbb{Z} -多元環を形成し, 特に既約指標全体が \mathbb{Z} -基底を成していることはよく知られた基本的な性質である. そして指標環の構造を調べるために, 指標の積の既約指標への分解の様子が自然と考えられてきた. その一つとして, 既約指標の積でその既約成分の個数が少ない場合について, G の構造を考察する.

以下 G を有限群とし, $\text{Irr}G$ で G の既約指標全体を, $\text{Irr}\theta$ によって, 指標 θ の既約成分全体を表わすものとする. また, 指標の内積は $\langle \cdot, \cdot \rangle$ と書くことにし, $\bar{\theta}$ で指標 θ の複素共役な指標とする.

2 Character products with few irreducible constituents

G の既約指標 χ に対し, $\#\text{Irr}\chi$ が十分に小さいときはある程度 G の構造が決まることが分かっている [1],[7].

Theorem 1 (Isaacs and Zisser) 有限群 G の忠実な既約指標 χ で

$$\#\text{Irr}\chi^2 = 1$$

を満たすものが存在するとき, G は *cyclic 2-群* と奇数位数の *central type* の群の直積と同型.

Remark 1 群 H が *central type* とは, H の既約指標 ψ で $\psi^2(1) = |H : Z(H)|$ を満たすものが存在することとする.

Theorem 2 (Isaacs and Zisser) 有限群 G の忠実な既約指標 χ で

$$\#\text{Irr}\chi^2 = 2, \quad \text{Irr}\chi^2 = \text{Irr}\bar{\chi}^2$$

を満たすものが存在するとき, G は 高々位数 4 の *cyclic 2-群* と奇数位数の群の直積で表される.

さらに $\text{Irr}G$ を類別することで、拡張と精密化が出来ることが分かった [8]. $\text{Irr}G$ の類別をするために、以下の記号を使う.

指標 θ に対して \mathcal{G}_θ で \mathbb{Q} に θ のとる値を添加した体の \mathbb{Q} の代数閉包への体拡大 $\bar{\mathbb{Q}}/\mathbb{Q}(\theta)$ のガロア群を表す.

G の既約指標 χ に対して,

$$\hat{\chi} := \begin{cases} \chi & (\chi = \bar{\chi}) \\ \chi + \bar{\chi} & (\text{otherwise}) \end{cases}$$

で定義し,

$$\text{RIrr}G = \{\hat{\chi} | \chi \in \text{Irr}G\}$$

とおく.

Theorem 3 (Kiyota and Suzuki) χ を有限群 G の忠実な既約指標とする. このとき χ が

$$\begin{aligned} \hat{\chi}^2 &= b \cdot 1_G + a\hat{\chi} + c \sum_{i=1}^r \hat{\psi}_i, \\ \hat{\psi}_1^{\hat{\chi}} &= \{\hat{\psi}_1, \hat{\psi}_2, \dots, \hat{\psi}_r\} \quad (a, b, c \in \mathbb{Z}, \hat{\psi}_1, \hat{\psi}_2, \dots, \hat{\psi}_r \in \text{RIrr}G) \end{aligned}$$

を満たすならば, G は次のうちいずれかを満たす.

1. 巡回群と同型.
2. Frobenius 群でその補群は素数位数 p で $p = \chi(1) = 2r + 1$ を満たす.
3. 3次対称群と同型.
4. binary polyhedral group と同型.
5. 5次交代群と同型.

3 Representation diagram and \mathbb{Q} -polynomial association scheme

次に association scheme との関連性について述べる. $\mathcal{X} = \mathcal{X}(X, \{R_i\}_{0 \leq i \leq d})$ を commutative association scheme とする.

Definition 1 \mathcal{X} が \mathbb{Q} -polynomial であるとは, \mathcal{X} の Bose-Mesner algebra の primitive idempotent に番号を付けて, i 番目の idempotent が 次数 i の \mathbb{C} 係数多項式に 1 番目の idempotent を代入して得られることとする. ただし, 多項式に代入したときの行列の積は Hadamard 積とする.

q_{hi}^j を Krein parameter とするとき, $\mathcal{D}^*(\mathcal{X}, h)$, ($1 \leq h \leq d$) を $\{0, 1, \dots, d\}$ を点集合とし $q_{hi}^j \neq 0$ を満たす (i, j) を辺とする有向グラフとする. この $\mathcal{D}^*(\mathcal{X}, h)$ を h による \mathcal{X} の表現グラフと呼ぶ.

Proposition 4 \mathcal{X} が Q -polynomial であることと, ある $1 \leq h \leq d$ による \mathcal{X} の表現グラフが *path* であることは同値.

さて group association scheme が Q -polynomial となる場合が Theorem 3 と結びつくことを簡単に述べる.

G の group association scheme を $\mathcal{X}(G)$ とおき, 表現グラフ $\mathcal{D}^*(\mathcal{X}(G), h)$ を共役類 K_h に対応する χ_h による G の表現グラフと呼び $\mathcal{D}^*(G, \chi_h)$ で表す. 群の表現グラフは relation と共役類と既約指標の番号が対応しているため, 点集合を $\text{Irr}G$ で考えることができ, (χ_i, χ_j) が辺となるのは $\langle \chi_h, \chi_i \chi_j \rangle \neq 0$ のときとしてよい.

Theorem 3 では, $\text{Irr}G$ を類別しているため表現グラフもそれに対応させる. $\mathcal{X}(G) = \mathcal{X}(G, \{R_i\}_{0 \leq i \leq d})$ に対して,

$$\widetilde{R}_i = R_i \cup {}'R_i$$

と定義し $\widetilde{\mathcal{X}}(G) = \mathcal{X}(G, \{\widetilde{R}_i\})$ とおくと $\widetilde{\mathcal{X}}(G)$ は symmetric association scheme となる. そして $\hat{\chi} \in \text{RIrr}G$ を固定して $\text{RIrr}G$ を点集合, $\langle \hat{\chi} \hat{\chi}_i, \hat{\chi}_j \rangle \neq 0$ のとき $(\hat{\chi}_i, \hat{\chi}_j)$ を辺とするグラフを $\widetilde{\mathcal{D}}^*(G, \hat{\chi})$ と書くことにすると, $\widetilde{\mathcal{X}}(G)$ が Q -polynomial であることは, Proposition 4 から $\widetilde{\mathcal{D}}^*(G, \hat{\chi})$ が *path* となることであり, さらに表現グラフが

$$1_G \text{---} \hat{\chi} \text{---} \hat{\psi} \text{---} \bigcirc \text{---} \dots \text{---} \bigcirc$$

となるのだから,

$$\hat{\chi}^2 = b \cdot 1_G + a\hat{\chi} + c\hat{\psi}, \quad (a, b, c \in \mathbb{Z}, \hat{\chi}, \hat{\psi} \in \text{RIrr}G)$$

を満たすことが分かる.

Theorem 5 (Kiyota and Suzuki) G を有限群とするととき, $\widetilde{\mathcal{X}}(G)$ が Q -polynomial ならば, G は次のいずれかと同型.

1. 巡回群
2. 3次対称群
3. 4次交代群
4. 3元体上2次元特殊線形群
5. 位数21の Frobenius 群

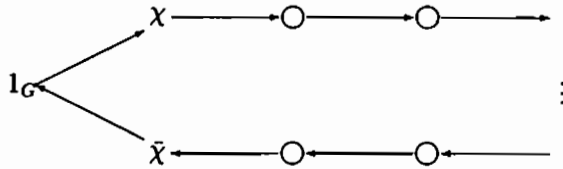
さらに, *path* とは別の特別な形状の表現グラフとある特別な指標を持つ群が対応する例をあげておく.

Theorem 6 (Suzuki) G を有限群とする. このとき, G が $\{0, 1\}$ -sharp 指標を持つことと既約指標 χ で $\mathcal{D}^*(G, \chi)$ が *star* (i.e. 1点を除いて辺でつながっている点の個数はちょうど1個で連結) となるものが存在することが同値.

4 Examples of Representation diagram

まず簡単な表現グラフの例を見てみると (二重丸は nonreal valued character を意味する.)

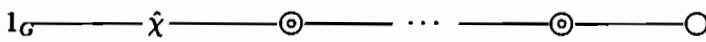
$$\mathcal{D}^*(\mathbb{Z}/n\mathbb{Z}, \chi) \quad \chi(1) = 1$$



$$\widetilde{\mathcal{D}}^*(\mathbb{Z}/n\mathbb{Z}, \hat{\chi}) \quad \chi(1) = 1$$

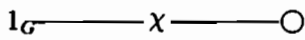


or

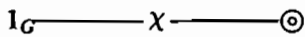


Theorem 3 などに出てきた群について実際に計算してみると

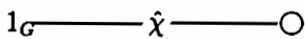
$$\widetilde{\mathcal{D}}^*(S_3, \hat{\chi}) \quad \chi(1) = 2$$



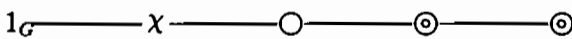
$$\widetilde{\mathcal{D}}^*(A_4, \hat{\chi}) \quad \chi(1) = 3$$



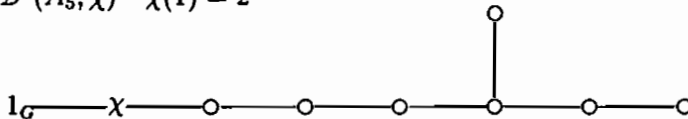
$$\widetilde{\mathcal{D}}^*(F_{21}, \hat{\chi}) \quad \chi(1) = 3 \quad (F_{21} \text{ は位数 } 21 \text{ の Frobenius 群})$$



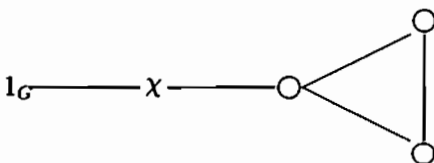
$$\widetilde{\mathcal{D}}^*(SL(2, 3), \hat{\chi}) \quad \chi(1) = 2$$



$$\widetilde{\mathcal{D}}^*(A_5, \hat{\chi}) \quad \chi(1) = 2$$

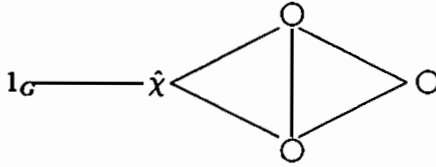


$$\widetilde{\mathcal{D}}^*(SL(2, 5), \hat{\chi}) \quad \chi(1) = 2$$



ここまでに出ていない sharp 指標を持つ群として $L_2(7)$ を計算した.

$$\widetilde{D}(L_2(7), \chi) \quad \chi(1) = 3$$



5 Complex conjugacy character

詳しい証明は参考文献を参照していただくとして, Theorem 3 において G が分類できた要因として $\text{Irr}\chi^2$ と $\text{Irr}\chi\bar{\chi}$ をそれぞれ類別したときの類の個数が非常に小さいことがあげられる. 特に $\#\text{Irr}\chi\bar{\chi}$ が小さいことが, Frobenius 核の存在を与えていると思われる. そこで $\#\text{Irr}\chi\bar{\chi}$ が十分小さくなる G について調べてみた.

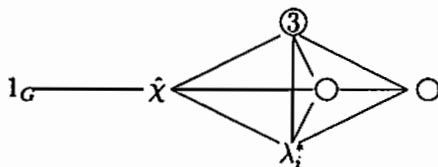
Proposition 7 χ を有限群 G の忠実な既約指標とする. $\#\text{Irr}\chi\bar{\chi} = 1$ ならば G は巡回群.

Theorem 8 χ を有限群 G の忠実な既約指標とする. $\#\text{Irr}\chi\bar{\chi} = 2$ で $\langle \chi^2, \bar{\chi} \rangle \neq 0$ かつ $Z(G) = 1$ ならば G は $L_2(7)$ と同型.

略証 $\#\text{Irr}\chi\bar{\chi} = 2$ と $\langle \chi^2, \bar{\chi} \rangle \neq 0$ から χ の交代積 $\text{Alt}\chi$ が χ で表されることが計算できるので, $\chi(1) = 3$ を得る. そして, 素数次数の既約指標と $Z(G) = 1$ より, Sylow 3-部分群とその中心化群および正規化群が決定できる. さらに 3-元と Sylow 2-部分群の central involution での値が計算でき, それによって次数 7 の既約指標 θ の存在がわかる. 再び素数次数の既約指標と $Z(G) = 1$ より, Sylow 7-部分群とその中心化群, 正規化群および $|G|$ が決定できる. そして $\#\text{Irr}G$ が判明し, $1_G + \theta$ が G の Sylow 7-部分群全体への共役による作用の置換指標となることがわかり, $G \simeq L_2(7)$ が示される.

ここで G を決定できたのは Zassenhaus 群となることを導いたことによるが, では他の Zassenhaus 群に $\#\text{Irr}\chi\bar{\chi} = 2$ となるような群があるだろうか? 実は S_8 による類別をすれば, 8 元体上の Suzuki 群が満たしていることが分かった.

$$\chi \in \text{Irr}S(8) \quad \chi\bar{\chi} = 1_G + (\lambda_1 + \lambda_2 + \lambda_3)$$



上の図は $\widetilde{\mathcal{D}}^*(S(8), \hat{\chi})$ の点集合 $\text{RIrr}S(8)$ を \mathcal{S}_χ で類別して同じ類に属する点同士の間の辺を無視したものである。丸の数字はその点に含まれる既約指標の個数である。

なお $\#\text{Irr}\chi\bar{\chi} = 2$ を満たす群は先に述べたもの以外にも存在することが分かっている。

参考文献

- [1] H.L.Blau and D.Chillag: *On powers of characters and powers of conjugacy classes of finite groups*, Proc. Amer. Math. Soc. **98**, 7-10 (1986).
- [2] E.Bannai and T.Ito: *Algebraic Combinatorics I Association Scheme*, Benjamin, California (1984)
- [3] P.J.Cameron and M.Kiyota: *Sharp characters of finite groups*, J.Algebra **115** (1988), 125-143.
- [4] W.Feit: *Characters of finite groups*, Benjamin, New York (1967).
- [5] D.Gorenstein: *Finite groups(2nd. edition)*, Chelsea Publishing Company, New York (1980).
- [6] I.M.Isaacs: *Characters of finite groups*, Academic Press, New York (1976).
- [7] I.M.Isaacs and I.Zisser: *Squares of characters with few irreducible constituents in finite groups*, Arch. Math. **63** (1994), 197-207.
- [8] M.Kiyota and H.Suzuki: *Character Products and Q-polynomial Group Association Schemes*, J. Algebra **226** (2000), 533-546

1870-1871. The first year of the war. The first year of the war. The first year of the war.

1871-1872. The second year of the war. The second year of the war. The second year of the war.

1872-1873. The third year of the war. The third year of the war. The third year of the war.

1873-1874. The fourth year of the war. The fourth year of the war. The fourth year of the war.

1874-1875. The fifth year of the war. The fifth year of the war. The fifth year of the war.

1875-1876. The sixth year of the war. The sixth year of the war. The sixth year of the war.

1876-1877. The seventh year of the war. The seventh year of the war. The seventh year of the war.

1877-1878. The eighth year of the war. The eighth year of the war. The eighth year of the war.

1878-1879. The ninth year of the war. The ninth year of the war. The ninth year of the war.

1879-1880. The tenth year of the war. The tenth year of the war. The tenth year of the war.

1880-1881. The eleventh year of the war. The eleventh year of the war. The eleventh year of the war.

1881-1882. The twelfth year of the war. The twelfth year of the war. The twelfth year of the war.

1882-1883. The thirteenth year of the war. The thirteenth year of the war. The thirteenth year of the war.

1883-1884. The fourteenth year of the war. The fourteenth year of the war. The fourteenth year of the war.

1884-1885. The fifteenth year of the war. The fifteenth year of the war. The fifteenth year of the war.

1885-1886. The sixteenth year of the war. The sixteenth year of the war. The sixteenth year of the war.

1886-1887. The seventeenth year of the war. The seventeenth year of the war. The seventeenth year of the war.

1887-1888. The eighteenth year of the war. The eighteenth year of the war. The eighteenth year of the war.

1888-1889. The nineteenth year of the war. The nineteenth year of the war. The nineteenth year of the war.

1889-1890. The twentieth year of the war. The twentieth year of the war. The twentieth year of the war.