第16回代数的組合せ論シンポジウム報告集

1999年6月24日～25日

於　九州大学　国際ホール

平成11年度文部省科学研究費基盤研究(A)

研究代表者　坂内 英一

まえがき

この報告集は、１９９９年６月２４日と６月２５日の２日間、九州大学国際ホールにおいておこなわれた「第１６回代数的組合せ論シンポジウム」の講演記録です。プログラムは代数的組合せ論とその関連分野の、第一線の研究者による講演を集めて作成しました。

この集会に先立って、「代数的組合せ論夏の学校１９９９」を福岡市東区の休暇村志賀島で開催した関係で、シンポジウムの日程は例年より短い２日間となりましたが、周辺の分野の講演を多く入れたため８０名の参加者があり、盛会でした。

この集会に関わる講演者の旅費、並びに、この報告集の印刷費について、科学研究費基盤（Ａ）（研究代表者：坂内英一・九州大学教授）の援助をいただきましたことを御礼申し上げます。

最後になりましたが、講演者の方々、会場の準備を手伝ってくださった九州大学大学院数理学研究科の大学院生有志の方々に感謝します。

１９９９年１２月

宗政 昭弘

原田 昌晃

「第１６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 九州大学 宗政 昭弘
山形大学 原田 昌晃

記

日程：1999 年 6 月 24 日 (木) - 25 日 (金)
場所：九州大学国際ホール (箱崎キャンパス)
福岡市営地下鉄箱崎九大前下車徒歩５分

プログラム

６月２４日 (木)

10:00–10:50　本間 正明 (神奈川大)
代数曲線上の２点についての gap 集合とそれらの点を支持台に持つ代数曲線符号
11:00–11:30　田邊 顕一朗 (九州大 数理)
$\mathbb{Z}_4$ 上のコードにおける Assmus-Mattson の定理
11:40–12:10　城本 啓介 (熊本大 自然科学)・堀本 博 (熊本大 自然科学)
MDS codes over quasi-Frobenius rings

13:30–14:20　関口 次郎 (姫路工大 理)
正２０面体方程式とモジュラ形式
14:30–15:00　大野 泰生 (大阪大 理)
多重ゼータ値と荒川-金子のゼータ関数の特殊値について
15:20–15:50　平坂 貢 (九州大 数理)
Quasithin association scheme と置換群との関係について
16:00–16:30　坂内 悦子 (九州大 数理)
Four-weight spin model について
16:40–17:10　土山 泰史 (九州大 数理)・鈴木　寛 (国際基督教大)
サイズ 6, 7 のスピンモデルについて

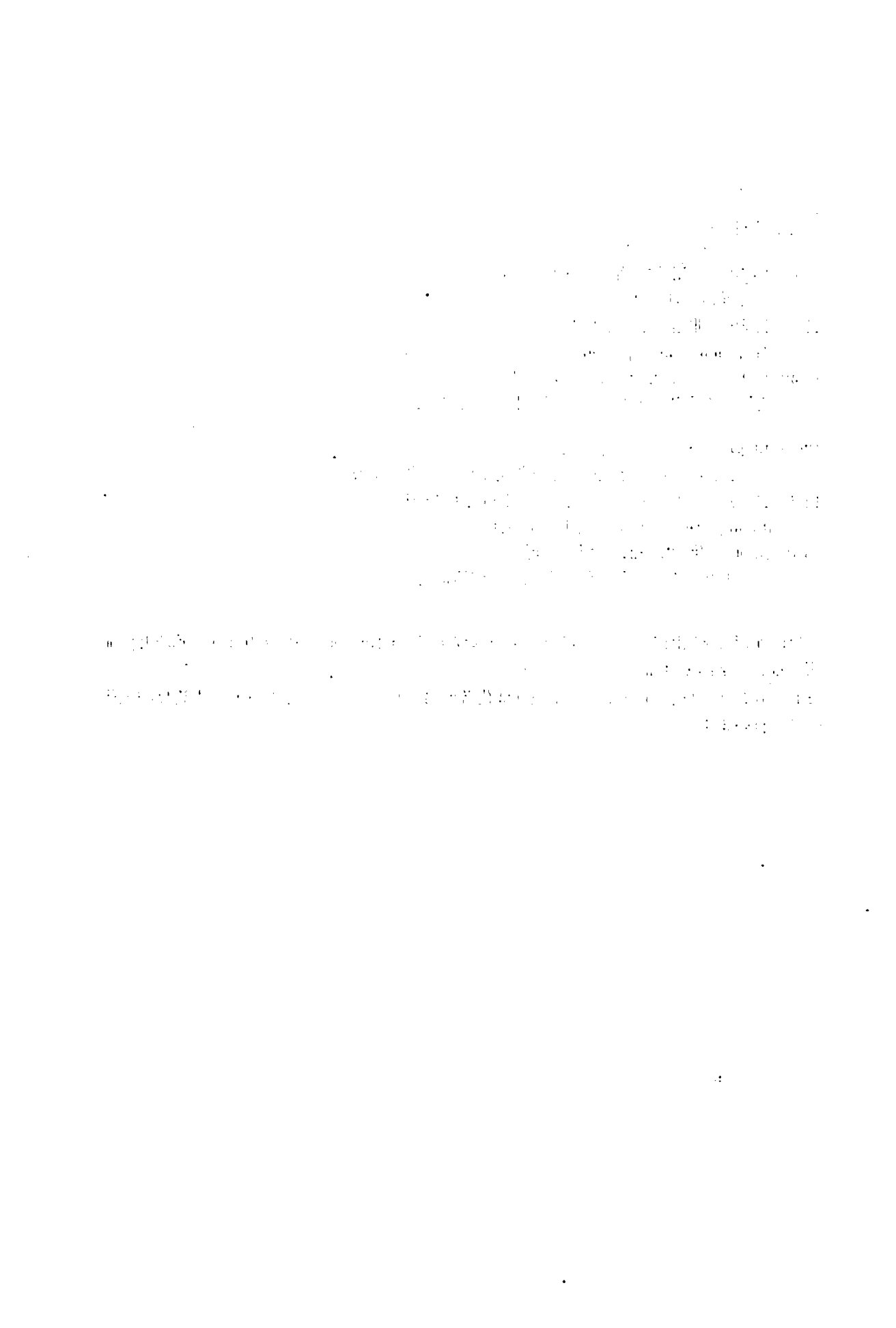
6月25日(金)

10:00–10:50　原田 耕一郎 (オハイオ州立大)
　　単純群のシロー 2-群を切る
11:00–11:30　北詰 正顕 (千葉大 理)
　　27-dimensional representations of $3.O(7,3), 3.F_{22}, 3.^2E_6(2)$
11:40–12:10　丹原 大介 (弘前大学 理工)
　　有限体の乗法群と加法群の半直積の表現の圏の変形

13:30–14:20　松尾 厚 (東京大 数理)
　　Hamming 符号に附随した頂点作用素代数の自己同型群
14:30–15:00　石川 雅雄 (鳥取大)・田川 裕之 (和歌山大)
　　d-complete posets に関連した母関数について
15:10–16:00　伊吹山 知義 (大阪大 理)
　　重さ半整数のジーゲル保型形式の具体的構造

会場の九州大学国際ホールは箱崎キャンパス理学部三号館の向かいにあります。箱崎九大前駅から、理学部を目標においでください。

なお、6月20日(日)から23日(木)は代数的組合せ論夏の学校１９９９を志賀島国民休暇村で行います。



目次

代数曲線上の2点についての gap 集合とそれらの点を支持台に持つ代数曲線符号

本 間 正 明*

神奈川大学工学部

homma@cc.kanagawa-u.ac.jp

1 代数曲線符号

有限体 $\mathbb{F}_q$ の上で定義された代数曲線 X 上の Goppa 符号は，その曲線上の相異なる $\mathbb{F}_q$-有理点 $P_1,\ldots,P_n$ からなる正因子 $D=\sum_{i=1}^{n}P_i$ とこれらの点をその support には含まない $\mathbb{F}_q$-有理な因子 F とから構成される．さらに，理論的には必要はないが，煩雑さを避けるために，F は正因子であると仮定する．

この D と F から線形符号をつくる標準的方法として X の関数加群を用いる方法と，微分加群を用いる方法とがある．前者は L-構成法，後者は Ω-構成法とよばれる．

ここで，この小論を通して用いるいくつかの記号を用意するが，概ね Stichtenoth [9] に従う．$\mathbb{F}$ を完全体とし[1]，X を $\mathbb{F}$ 上定義された絶対既約な完備非特異代数曲線[2]とし，X の $\mathbb{F}$- 有理関数全体を $\mathbb{F}(X)$ で表す．また$\mathbb{F}$- 有理微分全体のなす $\mathbb{F}(X)$ ベクトル空間を $\Omega_{\mathbb{F}(X)}$ で表す．またこの曲線 X の $\mathbb{F}$- 有理点全体を $X(\mathbb{F})$ で表す．この曲線の種数を g で表す．

---

*ここで述べる事柄は，Seon Jeong Kim (Gyeongsang National University) との共同研究の一部分である．証明を含めた完全版は，遠くない将来，どこかに発表する予定である．

[1]符号について考えるときは，当然 $\mathbb{F}$ は有限体 $\mathbb{F}_q$ とする．

[2]以下，これを単に $\mathbb{F}$ 上の代数曲線 (あるいは，単に，曲線) とよぶことにする．

$f \in \mathbb{F}$ について，$(f)_0$ で f の零点のなす因子を，$(f)_\infty$ で f の極のなす因子を表し，さらに，$(f) := (f)_0 - (f)_\infty$ と記す．$\Omega_{\mathbb{F}(X)}$ の元についても同様な記法を用いる．$(f)_0, (f)_\infty, (f)$ 等は $\mathbb{F}$ 上定義された因子である[3].$\mathbb{F}$ 上定義された因子のことを$\mathbb{F}$- 有理因子とよぶことにする．

$\mathbb{F}$- 有理因子 E について，

$$\mathcal{L}(E) := \{f \in \mathbb{F}(X) \setminus \{0\} \mid (f) + E \succ 0\} \cup \{0\},$$

$$\Omega(E) := \{\omega \in \Omega_{\mathbb{F}(X)} \setminus \{0\} \mid (\omega) \succ E\} \cup \{0\},$$

として，これらの $\mathbb{F}$ ベクトル空間としての次元を $\ell(E) := \dim_{\mathbb{F}} \mathcal{L}(E)$, $i(E) := \dim_{\mathbb{F}} \Omega(E)$ で表す．

さて，冒頭のパラグラフの状況に戻ろう．

L-構成法　$\mathbb{F}_q$-線形写像

$$\mathcal{L}(F) \ni f \longmapsto (f(P_1), \ldots, f(P_n)) \in {\mathbb{F}_q}^n$$

を考え，この像である符号を $C_L(D, F)$で表す．明らかに $\dim C_L(D, F) = \ell(F) - \ell(F - D)$ である．

Ω-構成法　$\mathbb{F}_q$-線形写像

$$\Omega(F - D) \ni \eta \longmapsto (\mathrm{res}_{P_1}\eta, \ldots, \mathrm{res}_{P_n}\eta) \in {\mathbb{F}_q}^n,$$

を考え，この像である符号を $C_\Omega(D, F)$で表す．明らかに，$\dim C_\Omega(D, F) = i(F - D) - i(F)$ である．

Riemann-Roch の定理と留数定理より，容易にわかるように，$C_L(D, F)$ と $C_\Omega(D, F)$は互いに双対符号の関係にある．

また，Pellikaan - Shen - van Wee [8] によって，全ての線形符号は適当な曲線 X とその上の因子の組 (D, F) から L-構成法によって得られることが証明されている．従って，全ての線形符号は Ω-構成法によって得られると言っても良い．

以下，小論では Ω-構成法で得られた符号について考察する．符号 $C_\Omega(D, F)$ の設計距離は F, D に何の制限も設けなければ Riemann - Roch の定理により，

(1)　$$\deg F - (2g - 2)$$

[3]これは，その因子にあらわれる点自身が $X(\mathbb{F})$ の点であることを意味しない．

で与えられる.

われわれは，$C_\Omega(D,F)$ の最小距離について議論したいので，それを $d_\Omega(D,F)$ なる記号で表す.

2 Garcia - Lax および Garcia - Kim - Lax による評価

Garcia と Lax は 1991 年に で，F が$\mathbb{F}_q$-有理点 Q の何倍かになっている状況では，ある場合に (1) より良い評価が得られることを示した．すなわち，α, β が Q での空隙[4]であるとき，$F=(\alpha+\beta-1)Q$ とすれば，

$$d_\Omega(D,F) \geq \deg F-(2g-2)+1; \tag{2}$$

である.

翌年，Garcia - Kim - Lax の 3 人によって，以下のような場合には評価 (2) が改良されることが示された．この状況はエルミート曲線[5]の場合に良く適合する[6].

t を自然数として，$\alpha+t\leq\beta$ とする．さらに，$\alpha,\alpha+1,\ldots,\alpha+t$ をひき続く $t+1$ 個の Q での空隙の列，$\beta-(t-1),\ldots,\beta-1,\beta$ をひき続く t 個の Q での空隙の列とするとき，$F=(\alpha+\beta-1)Q$ とすれば，

$$d_\Omega(D,F) \geq \deg F-(2g-2)+t+1. \tag{3}$$

なる評価を得る.

上に述べたような，代数曲線符号の支持因子 F の台が 1 点からなる，いわゆる 1 点符号は比較的取り扱い易いため，好まれているが，理論上は支持因子の台[7]が例えば，2 点であるような符号も興味があると思われる.

---

[4]関数 $f\in\mathbb{F}_q(X)$ で f の極因子 $(f)_\infty$ がちょうど αQ となるものが存在するとき，α を Q での非空隙 (nongap) といい，そうでないとき，空隙 (gap) という．与えられた点での空隙の個数は曲線の種数 g に一致する.

[5]平面非特異曲線 $y^q+y=x^{q+1}$ を $\mathbb{F}_{q^2}$ 上で考えた曲線.

[6]エルミート曲線上で $\mathbb{F}_{q^2}$-有理点 Q について $F=mQ$ とし，D として残余の有理点すべてとした符号 $C_L(D,F)$, $C_\Omega(D,F)$ の真の最小距離は Yang-Kumar [11] によって知られている.

[7]この言葉を省略して，支持台と呼ぶことにする.

実際，G. L. Matthews [7] は，特にエルミート曲線上の，2点を支持台とする曲線を調べ，パラメータの意味で1点を支持台とするものより良い符号が存在することを具体的構成によって明らかにした．

われわれは，2点を支持台とする代数曲線符号を，彼女の取り扱いよりは少しばかり理論的に，扱う．

3　曲線上の2点についての空隙集合

前節の Garcia-Lax および Garcia-Kim-Lax のような定理を2点を支持台に持つような符号について定式化しようとすれば，1点の場合の空隙列に相当する事柄について調べる必要がある．

これについては Kim [6] および著者 [5] によって基本的事柄が調べられている．ここでは，それらの中から必要となる部分を復習し，さらに，われわれの定理を定式化するために必要な概念について述べる．この節では基礎体 $\mathbb{F}$ は，単に完全体であるとする．さらに曲線 X の種数 g は2以上とする．

Q_1, Q_2 を相異なる X の $\mathbb{F}$-有理点とする．点の組 (Q_1, Q_2) についてのワイエルシュトラス (Weierstrass) 半群 $H(Q_1, Q_2)$ とは

$$\{(\nu_1, \nu_2) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid \text{ there exists } f \in \mathbb{F}(X) \text{ with } (f)_\infty = \nu_1 Q_1 + \nu_2 Q_2\},$$

によって定義される半群を意味する．ただし $\mathbb{N}_0$ は非負整数全体のなす半群である．さらに，この補集合

$$G(Q_1, Q_2) := \mathbb{N}_0 \times \mathbb{N}_0 \setminus H(Q_1, Q_2)$$

を，この2点組についての空隙集合とよぶ．

1点の場合の空隙列との大きな相違点は空隙集合は種数 g を固定してもこの位数は一定ではないことである．空隙集合を調べるために，以下の観察は重要である．

$m_1 < m_2 < \cdots < m_g$ と $n_1 < n_2 < \cdots < n_g$ とを，それぞれ Q_1, Q_2 での空隙列とする．Q_1 の各空隙 m_i に対し，

$$\min\{\beta \mid (m_i, \beta) \in H(Q_1, Q_2)\}$$

は Q_2 での空隙の1つとなる．これを $n_{\sigma(i)}$ と表すことにしよう．このとき，対応 $m_i \mapsto n_{\sigma(i)}$ は Q_1 での空隙列 $G(Q_1)$ と Q_2 での空隙列 $G(Q_2)$

の間の1対1対応を与える．従って σ は

$$\mathbb{N}_{\leq g} := \{1, 2, \ldots, g\}.$$

の上の置換となる．

さらに，この置換によって大小の順が反転されるような組の全体，すなわち

$$R(\sigma) := \{(i,j) \in \mathbb{N}_{\leq g} \times \mathbb{N}_{\leq g} \mid i < j \text{ and } \sigma(i) > \sigma(j)\}$$

を考え，$r(\sigma) := {}^{\#}R(\sigma)$ とする[8]．以上の記法の下で，空隙集合の個数は

$${}^{\#}G(Q_1, Q_2) = \sum_{i=1}^{g} m_i + \sum_{i=1}^{g} n_i - r(\sigma).$$

で与えられる．

さて，われわれの定理を定式化するため，2点組に対する「純な空隙」という概念を定義する．

定義 非負整数 (α_1, α_2) と $(Q_1, Q_2) \in X \times X$ について

$$\begin{aligned} \ell(\alpha_1 Q_1 + \alpha_2 Q_2) &= \ell((\alpha_1 - 1)Q_1 + \alpha_2 Q_2) \\ &= \ell(\alpha_1 Q_1 + (\alpha_2 - 1)Q_2). \end{aligned}$$

が成立するとき，(α_1, α_2) は (Q_1, Q_2) における純な空隙であるという．

2点組 (Q_1, Q_2) における純な空隙全体を $G_0(Q_1, Q_2)$ で表す．明らかに，$G_0(Q_1, Q_2)$ は $G(Q_1, Q_2)$ の部分集合である．

定理 3.1 上で説明した記法の下で，

$$G_0(Q_1, Q_2) = \{(m_i, n_j) \mid (i, \sigma^{-1}(j)) \in R(\sigma)\}.$$

である．特に，${}^{\#}G_0(Q_1, Q_2) = r(\sigma)$ である．

この定理の系として，

系 3.2 純な空隙の個数は

$${}^{\#}G_0(Q_1, Q_2) \leq \frac{1}{2} g(g-1),$$

で与えられる．従って $G_0(Q_1, Q_2) = \emptyset$ である為の必要十分条件は曲線 X から射影直線 $\mathbb{P}^1$ への2次の被覆があって，因子 $Q_1 + Q_2$ がその1点の逆像となることである．

[8]浅野啓三，永尾汎著「群論」岩波書店 (1965) ではこの数を転位の数とよんでいる．

証明. 最初の主張は定理と $0 \leq r(\sigma) \leq \frac{1}{2}g(g-1)$. から明らか. 後半の主張は [5, Proposition 4] による $r(\sigma) = 0$ の場合の 2 点組の特徴づけより明らか. □

4 2点を支持台に持つ符号の最小距離の評価

以下, 再び基礎体 $\mathbb{F}$ は有限体 $\mathbb{F}_q$ であるとし, X の種数は $g \geq 2$ とする.

状況設定を確認しておく. 相異なる X の $\mathbb{F}_q$-有理点 Q_1, Q_2 を固定する. さらに, $X(\mathbb{F}_q) \setminus \{Q_1, Q_2\}$ から n 個の点 $P_1, \ldots, P_n$ を選び, $D = P_1 + \cdots + P_n$ とする.

F を Q_1, Q_2 を台に持つ正因子, 符号 $C_\Omega(D, F)$ の最小距離を $d_\Omega(D, F)$ で表す.

最初の主要な結果は次のとおり.

定理 4.1 自然数の組 $(\alpha_1, \alpha_2), (\beta_1, \beta_2) \in \mathbb{N} \times \mathbb{N}$, について, $t_i := \beta_i - \alpha_i$ $(i = 1, 2)$ とおき, $t_i \geq 0$ $(i = 1, 2)$ であると仮定する. さらに,

$$\{(k_1, k_2) \mid \alpha_1 \leq k_1 \leq \beta_1,\ \alpha_2 \leq k_2 \leq \beta_2\} \subseteq G_0(Q_1, Q_2) \tag{4}$$

であれば,

$$F = (\alpha_1 + \beta_1 - 1)Q_1 + (\alpha_2 + \beta_2 - 1)Q_2$$

なる F について,

$$d_\Omega(D, F) \geq \deg F - (2g - 2) + t_1 + t_2 + 2.$$

が成り立つ.

定理 4.1 で "$t_1 = t_2 = 0$" の場合は, 以下の方向へ一般化できる. これは Garcia-Lax の評価式 (2) の支持台が 2 点の場合での類似である.

定理 4.2 (α_1, α_2) と (β_1, β_2) とを (Q_1, Q_2) における純な空隙とする.

$$F = (\alpha_1 + \beta_1 - 1)Q_1 + (\alpha_2 + \beta_2 - 1)Q_2,$$

とすれば,

$$d_\Omega(D, F) \geq \deg F - (2g - 2) + 2$$

である.

参考文献

[1] A. Garcia and R. F. Lax, Goppa codes and Weierstrass gaps. in: Coding Theory and Algebraic Geometry, Lecture Note in Mathematics **1518**, 33–42, Springer, Berlin - Heidelberg 1992

[2] A. Garcia, S. J. Kim and R. F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes. J. Pure Appl. Algebra **84**, 199–207 (1993)

[3] A. Garcia and P. Viana, Weierstrass points on certain non-classical curves. Arch. Math. **46**, 315–322 (1986)

[4] V. D. Goppa, Codes on algebraic curve. Soviet Math. Dokl. **24**, 170–172 (1981)

[5] M. Homma, The Weierstrass semigroup of a pair of points on a curve. Arch. Math. **67**, 337–348 (1996)

[6] S. J. Kim, On the index of the Weierstrass semigroup of a pair of points on a curve. Arch. Math. **62**, 73–82 (1994)

[7] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes. Preprint, Louisiana State University 1999

[8] R. Pellikaan, B. Z. Shen and G. J. M. van Wee, Which linear codes are algebraic-geometric ? IEEE Trans. Inform. Theory **37**, 583–602 (1991)

[9] H. Stichtenoth, Algebraic Function Fields and Codes. Springer, Berlin - Heidelberg 1992

[10] M. A. Tsfasman and S. G. Vlăduţ, Algebraic-Geometric Codes. Kluwer Academic Publishers, Dordrecht, 1991

[11] K. Yang and P. V. Kumar, On the true minimum distance of Hermitian curves. Lecture Note in Mathematics **1518**, 99–107, Springer, Berlin - Heidelberg 1992

An Assmus–Mattson theorem for $\mathbf{Z}_4$-codes

田辺顕一朗 tanabe@math.kyushu-u.ac.jp
九州大学大学院数理学研究科

1969 年に Assmus と Mattson[1] は有限体上の線形符号からデザインを構成する強力な手法を与えました。ここで彼らは群の軌道からこない 5-デザインを構成することに初めて成功しました。Calderbank 達 (cf. [6], [10]) の $\mathbf{Z}_4$-コードを用いた二元体上の非線形符号の研究の成功以来、$\mathbf{Z}_4$-コードの研究が活発になされています ($\mathbf{Z}_4$:=$\mathbf{Z}/(4\mathbf{Z})$)。二元体上の符号における結果の類似が $\mathbf{Z}_4$-コードにおいて成立するかどうかは非常に興味ある問題です。Gulliver と原田 ([8], [9]) は計算機を用いて、$\mathbf{Z}_4$ 上の lifted Golay code から新しい 5-デザインをいくつか構成しました。この講演では $\mathbf{Z}_4$-コードに対する Assmus-Mattson の定理の類似を与え、それを用いて彼らの結果の別証を与えます。

1 準備

二元体上の線形符号、デザインの定義をした後、二元体上の線形符号に対する Assmus-Mattson の定理を紹介します。

定義 1 n を正の整数、$\mathbf{F}_2 := \{0,1\}$ を二元体とする。$\mathbf{F}_2$ 上の n 次元ベクトル空間 $\mathbf{F}_2^n$ の部分空間を長さ n の $\mathbf{F}_2$ 上の線形符号という。$u := (u_1,\ldots,u_n) \in \mathbf{F}_2^n$ に対して、$\mathrm{wt}(u) := |\{i \in \{1,2,\ldots,n\} \mid u_i \neq 0\}|$ とおく。$\mathbf{F}_2$ 上の線形符号 C に対して、$\{\mathrm{wt}(u) \mid u \in C\}$ の元を C の重みという。長さ n の $\mathbf{F}_2$ 上の線形符号 C に対して、$C^\perp := \{u \in \mathbf{F}_2^n \mid uv = 0,\ {}^\forall v \in C\}$ を C の双対符号という。ここで $u := (u_1,\ldots,u_n)$, $v := (v_1,\ldots,v_n) \in \mathbf{F}_2^n$ に対して、$uv := \sum_{i=1}^n u_i v_i$。また線形符号 C は $C = C^\perp$ を満たす時、自己双対符号であると呼ばれる。

n を正の整数とし、記号 $X_i := \{U \subset \{1,2,\ldots,n\} \mid |U| = i\}$ $(i = 0,1,\ldots,n)$ を準備します。

定義 2 (デザイン) t, k, λ を正の整数で $t < k$ を満たすものとし、$\mathcal{B} := \{B_1, B_2, \ldots, B_m\} \subset X_k$ (B_i 達は異なっていなくてもよい) とする。$\mathcal{B}$ が条件:

$$\#\{i \in \{1,2,\ldots,m\} \mid T \subset B_i\} = \lambda,\ {}^\forall T \in X_t$$

を満たす時、$\mathcal{B}$をブロックに重複を許したt-(n,k,λ)-デザイン (あるいは簡単に、ブロックに重複を許したt-デザイン) という。特にB_i達が相異なる時、$\mathcal{B}$を (単純な) t-デザインという。

次に二元体上の線形符号に関するAssmus-Mattsonの定理を紹介します。Bachoc[2]によってこの定理の非常にきれいな別証が与えられています。

定理 1 (Assmus–Mattsonの定理 [1], or see [2]) Cを長さnの二元体上の線形符号とし、$d := \min\{\mathrm{wt}(u) \in C \mid 0 \neq u \in C\}$と置く。正の整数$t < d$が条件:

$$\#\left\{\mathrm{wt}(u) \mid 0 \neq u \in C^{\perp} \text{ and } \mathrm{wt}(u) \leq n-t\right\} \leq d-t.$$

を満たしているとする。この時、任意の重み$t \leq i \leq n-t$に対して、$\{\mathrm{supp}(u) \mid u \in C \text{ (resp. } C^{\perp}) \text{ and } \mathrm{wt}(u) = i\}$は単純な$t$-デザインとなる。ここで$\mathrm{supp}(u) := \{i \in \{1,\ldots,n\} \mid u_i \neq 0\}$.

例えば二元体上の拡張Golay符号 (=: g_{24}) は$0, 8, 12, 16, 24$に重みを持つ長さ24の自己双対符号ですが、$t = 5$に対して定理の条件を満たしています。実際、$d = 8$であり、

$$\begin{aligned} &\#\{\mathrm{wt}(u) \mid 0 \neq u \in g_{24} \text{ and } \mathrm{wt}(u) \leq n-t\} \\ &= \#\{8, 12, 16\} \\ &= 3 = 8-5 = d-t \end{aligned}$$

となっています。したがって、よく知られている事実ですが、$\{\mathrm{supp}(u) \mid u \in g_{24} \text{ and } \mathrm{wt}(u) = i\}$ $(i = 8, 12, 16)$は5-デザインとなっています。

2 $\mathbf{Z}_4$-コードに対するAssmus–Mattsonの定理

$\mathbf{Z}_4 := \mathbf{Z}/4\mathbf{Z}$と表す事にします。ここでは$\mathbf{Z}_4$-コードの定義をした後、$\mathbf{Z}_4$-コードに対するAssmus-Mattsonの定理を述べます。最後に定理を$\mathbf{Z}_4$上のLifted Golay codeに適用して5-デザインを構成します。

定義 3 $\mathbf{Z}_4^n$の部分アーベル群を長さnの$\mathbf{Z}_4$-コードという。$u := (u_1, \ldots, u_n) \in \mathbf{Z}_4^n$に対して、$\mathrm{wt}(u) := |\{i \in \{1, 2, \ldots, n\} \mid u_i \neq 0\}|$おく。$\mathbf{Z}_4$-コードに対して、重み、双対符号、自己双対符号を二元体上の符号と同様に定義する。$u = (u_1, u_2, \ldots, u_n) \in \mathbf{Z}_4^n$に対して、

$$\begin{aligned} n_0(u) &:= |\{i \in \{1, 2, \ldots, n\} \mid u_i = 0\}| \\ n_1(u) &:= |\{i \in \{1, 2, \ldots, n\} \mid u_i = 1 \text{ or } 3\}| \\ n_2(u) &:= |\{i \in \{1, 2, \ldots, n\} \mid u_i = 2\}| \end{aligned}$$

とおき、$(n_0(u), n_1(u), n_2(u))$ を u の Lee composition という。また $\mathbf{Z}_4$-コード C に対して、$\sum_{u\in C} x_0^{n_0(u)} x_1^{n_1(u)} x_2^{n_2(u)}$ を C の symmetrized weight enumerator という。ここで x_0, x_1, x_2 は変数。

$\mathbf{Z}_4$-コード C から二通りの自然な方法で二元体上のコード $C^{(1)}$, $C^{(2)}$ が定義されます:

$$\begin{aligned} C^{(1)} &:\equiv C \pmod 2, \\ C^{(2)} &:= \{u/2 \mid u \in C \text{ and } u \equiv 0 \pmod 2\}. \end{aligned}$$

定理 2 ($\mathbf{Z}_4$-コードに対する Assmus-Mattson の定理) C を長さ n の $\mathbf{Z}_4$-コードで、任意の $u \in C$ に対して $n_1(u) \equiv 0 \pmod 2$ を満たしているものとする。次のものを定義する:

$$\begin{aligned} g_1 &:= n - 1 - \max\left\{n_2(v) \mid v \in C^\perp \text{ and } n_1(v) > 0\right\}, \\ g_2 &:= \min\{\mathrm{wt}(v) \mid v \in C^\perp \text{ and } v \not\equiv 0 \pmod 2\} - 1, \\ g &:= \min\{g_1, g_2\}, \\ \Lambda(h) &:= \left\{ (n_1(u), n_2(u)) \;\middle|\; \begin{array}{l} u \in C,\ h \le \mathrm{wt}(u) \le n-h \\ \text{and } n_1(u) > 0. \end{array} \right\}, \\ & \quad 1 \le h \le n. \end{aligned}$$

正の整数 $t \le g$ が次の条件を満たしているとする:

(1) $C^{(2)}$ (またはその双対符号) と $(C^\perp)^{(2)}$ (またはその双対符号) に対して t は二元体上の線形符号に対する Assmus-Mattson の定理の条件を満たしている。

(2) $1 \le {}^\forall h \le t$ に対して適当な $\sigma_h \in GL(2, \mathbf{C})$ と、集合 $\mathcal{A}_h := \{(a_i, b_j) \in \mathbf{C}^2 \mid 0 \le i + j \le g - h\}$ $(a_i \ne a_j \text{ and } b_i \ne b_j \ (i \ne j))$ が存在して、$\sigma_h(\Lambda(h)) \subset \mathcal{A}_h$ が成立している。

この時、C の任意の Lee composition (n_0, n_1, n_2) s.t. $t \le n_1 + n_2 \le n - t$ に対して $\{\mathrm{supp}(u) \mid u \in C,\ n_1(u) = n_1, \text{ and } n_2(u) = n_2\}$ は (ブロックに重複を許した)t-デザインとなる。

証明は Bachoc[2] の方法を改良して、$\mathbf{Z}_4$-コードに適用することによって得られます。つまり、Bachoc[2] が二元体上の符号に対して導入した harmonic weight enumerator を $\mathbf{Z}_4$-コードに対しても定義し、それに対して Macwilliams 型の恒等式が成り立つことを示しておきます。この恒等式と Delsarte[7] による harmonic space を用いてのデザインの特徴付けを使って定理は証明されます。

以下、定理2を $\mathbf{Z}_4$ 上の Lifted Golay code G_{24} に適用して 5-デザインを構成してみます。G_{24} は、$x^{11}+2x^{10}+3x^9+3x^7+3x^6+3x^5+2x^4+x+3$ を生成多項式に持つ $\mathbf{Z}_4$ 上の長さ 23 の巡回符号を、長さ 24 の符号に拡張することによって定義されます [3]。G_{24} は自己双対符号で、$G_{24}^{(1)}$ と $G_{24}^{(2)}$ はともに二元体上の拡張 Golay 符号になっています。Gulliver と原田 ([8], [9]) は計算機を用いて、いくつかの Lee composition (n_0, n_1, n_2) に対して、$\{\mathrm{supp}(u) \mid u \in G_{24} \text{ and } n_i(u) = n_i \ (i = 0, 1, 2)\}$ は単純な 5-デザインとなる事を示しました。その後、Bonnecaze 達 [4] によって、G_{24} と同じ symmetrized weight enumerator を持つ任意の $\mathbf{Z}_4$-コード (このような符号は Rains[12] によって分類されていて 13 個) に対して、Lee composition が一定の符号語の support 達は (ブロックに重複を許した)5-デザインをなす事が示されました。

したがって別にここで新しいデザインが構成される訳ではありませんが、上に述べた証明は、非常に複雑かつ大量の計算を必要としています。以下に見るように、G_{24} が定理2の条件を満たすことは非常に簡単に検証できます。

G_{24} の symmetrized weight enumerator は [5] で与えられています。それを Table 1 に載せておきます。

Table 1: Symmetrized weight enumerator of G_{24} [5]

Hamming weight	Lee composition		Number of words
	n_1	n_2	
0	0	0	1
8	0	8	759
10	8	2	12144
12	8	4	170016
	0	12	2576
13	12	1	61824
14	8	6	765072
15	12	3	1133440
16	16	0	24288
	8	8	1214400
	0	16	759
17	12	5	4080384
18	16	2	680064
	8	10	765072
19	12	7	4080384
20	16	4	1700160
	8	12	170016
21	12	9	1133440
22	16	6	680064
	8	14	12144
23	12	11	61824
24	24	0	4096
	16	8	24288
	0	24	1

この表を用いて定理2の条件を確かめていきます。まず、G_{24} は自己双対符号です。$G_{24}^{(2)}$ は二元体上の拡張 Golay 符号なので、条件 (1) は成立します。$\max\{n_2(u) \mid u \in G_{24} \text{ and } n_1(u) > 0\} = 14$ より、$g_1 = 24-1-14 = 9$ です、また $g_2 = 9$ より、$g = 9$ を得ます。次に各 $1 \leq h \leq 5$ に対して $\sigma_h \in GL(2, \mathbf{C})$ を $\sigma_h(i,j) = (i, i+4j)$ で定義します。すると、各 $\sigma_h(\Lambda(h))$ は次のようになります。

Table 2

h	$\sigma(\Lambda(h))$
1	(8,16), (8,24), (8,32), (8,40), (8,48), (8,56), (8,64), (12,16), (12,24), (12,32), (12,40), (12,48), (12,56), (16,16), (16,24), (16,32), (16,40)
2	(8,16), (8,24), (8,32), (8,40), (8,48), (8,56), (8,64), (12,16), (12,24), (12,32), (12,40), (12,48), (16,16), (16,24), (16,32), (16,40)
3	(8,16), (8,24), (8,32), (8,40), (8,48), (8,56), (12,16), (12,24), (12,32), (12,40), (12,48), (16,16), (16,24), (16,32)
4	(8,16), (8,24), (8,32), (8,40), (8,48), (8,56), (12,16), (12,24), (12,32), (12,40), (16,16), (16,24), (16,32)
5	(8,16), (8,24), (8,32), (8,40), (8,48), (12,16), (12,24), (12,32), (12,40), (16,16), (16,24)
6	(8,16), (8,24), (8,32), (8,40), (8,48), (12,16), (12,24), (12,32), (16,16), (16,24)

Table 2から条件 (2) も成立する事が確かめられます。したがって G_{24} から (ブロックに重複を許した)5-デザインを構成する事が出来ました。特に、以下の Lee composition ではデザインが単純になっていることが簡単に確かめられます。上から三つ目までのデザインは二元体上の拡張 Golay 符号からくるデザインです。

Table 3

Lee composition	デザイン
(16,0,8)	5-(24,8,1)
(12,0,12)	5-(24,12,48)
(8,0,16)	5-(24,16,78)
(14,8,2)	5-(24,10,36)
(12,8,4)	5-(24,12,1584)
(11,12,1)	5-(24,13,936)
(9,12,3)	5-(24,15,40040)

Remark. $\mathbf{Z}_4$-コードからデザインが構成できた今までに知られている例は、G_{24} の 5-デザイン、$\mathbf{Z}_4$ 上の QR_{32}, QR_{48}, Kerdock codes, Preparata

codes, Delsarte-Goethals codes, Goethals codes の 3-デザインです ([4],[8], [9], [13],[14])。ここで QR_n は長さ n の quadratic residue code。Shin 達 [14] はハミング重みに関する $\mathbf{Z}_4$-コードに対する Assmus–Mattson の定理を示し、それを用いて Kerdock codes, Preparata codes の 3-デザインを示しています。しかし、上に挙げたそれ以外の符号に対しては彼らの定理は適用できません。定理 2 は彼らの定理の拡張になっているので定理 2 から Kerdock codes, Preparata codes の 3-デザインは示せます。またそのままでは駄目なのですが、定理 2 を改良することによって QR_{32} の 3-デザインは示すことが出来ます [16]。現在のところ、QR_{48}, Delsarte-Goethals codes, Goethals codes の 3-デザインに対しては Assmus–Mattson の定理のような方法では示すことが出来ていません。

参考文献

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory*, Vol. 6 (1969), pp. 122–151.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, preprint.

[3] A. Bonnecaze, A. R. Calderbank, and P. Solé, Quaternary quadratic residue codes and unimodular lattices, *IEEE Trans. Inform. Theory*, Vol. 41 (1995), pp. 366–377.

[4] A. Bonnecaze, E. Rains, and P. Solé, 3-colored 5-designs and $\mathbf{Z}_4$-codes, preprint.

[5] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain, Type II codes over $\mathbf{Z}_4$, *IEEE Trans. Inform. Theory*, Vol. 43 (1997), pp. 969–976.

[6] A. R. Calderbank, A. R. Hammons Jr., P. Vijay Kumar, N. J. A. Sloane and P. Sole, A Linear Construction for Certain Kerdock and Preparata Codes, *Bulletin Amer. Math. Soc.*, Vol. 29 (1993), pp. 218–222,

[7] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, *SIAM J. Appl. Math.*, Vol. 34 (1978), pp. 157–166.

[8] T. A. Gulliver and M. Harada, Extremal double circulant Type II codes over $\mathbf{Z}_4$ and 5-$(24, 10, 36)$ designs, *Discrete Math.*, Vol. 194 (1999), pp. 129–137.

[9] M. Harada, New 5-designs constructed from the lifted Golay code over $\mathbf{Z}_4$, *J. Combin. Des.*, Vol. 6 (1998), pp. 225–229.

[10] A. R. Hammons Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The $\mathbf{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes, *IEEE Trans. Information Theory*, Vol. 40 (1994), pp. 301–319.

[11] V. Pless and Z. Qian, Cyclic Codes and Quadratic Residue Codes over $\mathbf{Z}_4$, *IEEE Trans. Inform. Theory*, Vol. 42 (1996), pp. 1594–1600.

[12] E. Rains, Optimal self-dual codes over $\mathbf{Z}_4$, *Discrete Math.*, Vol. 203 (1999), pp. 215–228.

[13] D. Shin, P. V. Kumar, and T. Helleseth, 3-designs from the $\mathbf{Z}_4$-Goethals codes via a new Kloosterman sum identity, preprint.

[14] D. Shin, P. V. Kumar, and T. Helleseth, An Assmus-Mattson-Type Approach for Identifying 3-Designs from Linear Codes over $\mathbf{Z}_4$, preprint.

[15] K. Tanabe, An Assmus–Mattson theorem for $\mathbf{Z}_4$-codes, to appear in IEEE Trans. Information Theory.

[16] K. Tanabe, A criterion for designs in $\mathbf{Z}_4$-codes on the symmetrized weight enumerator, preprint.

MDS Codes over quasi-Frobenius Rings *

Hiroshi HORIMOTO
and
Keisuke SHIROMOTO †

Department of Mathematics, Kumamoto University,
2-39-1, Kurokami, Kumamoto 860-8555, JAPAN

1 Preliminaries.

Let R be a finite ring and let R^n be the free module of rank n consisting of n-tuples of elements from R. A *right (left) linear code* C of length n over R is a right (left) R-submodule of R^n. Put $N := \{1, 2, \cdots, n\}$. Define the *support* and the (*Hamming*) *weight* of a vector $\mathbf{x} = (x_1, \cdots, x_n) \in R^n$ as follows:

$$\begin{aligned} \mathrm{supp}(\mathbf{x}) &:= \{i \in N \mid x_i \neq 0\} \\ \mathrm{wt}(\mathbf{x}) &:= |\mathrm{supp}(\mathbf{x})|. \end{aligned}$$

The *minimum* (*Hamming*) *weight* of C, denoted by $d(C)$, is

$$d(C) := \min\{\mathrm{wt}(\mathbf{x}) \mid (\mathbf{0} \neq)\mathbf{x} \in C\}.$$

On R^n, we define the *inner product* by

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^{n} x_i y_i \ (\in R),$$

for $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$. For any subset $C \subseteq R^n$, the *right* (*left*) *dual code* is that

$$\begin{aligned} \mathcal{R}(C) &:= \{\mathbf{y} \in R^n \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall \mathbf{x} \in C\} \\ \mathcal{L}(C) &:= \{\mathbf{y} \in R^n \mid \langle \mathbf{y}, \mathbf{x} \rangle = 0, \forall \mathbf{x} \in C\}. \end{aligned}$$

*This note is based on the papers [3] and [4]. So the details and proofs are in [3] and [4].

†Supported in part by the Japan Society for the Promotion of Science.

We remark that $\mathcal{R}(C)$ and $\mathcal{L}(C)$ are also right and left R-submodules of R^n, respectively.

2 A Singleton bound.

Let R be a finite quasi-Frobenius (QF) ring, that is, R is an injective module over itself (see [1], [5] and [7]). For a right R-submodule $D \subseteq R^n$ and a subset $M \subseteq N$, we define

$$\begin{aligned} D(M) &:= \{\mathbf{x} \in D \mid \mathrm{supp}(\mathbf{x}) \subseteq M\}, \\ D^* &:= \mathrm{Hom}_R(D, R), \\ \mathrm{cut} &: R^n \longrightarrow R^n(M)\ ;\ (x_i)_{i\in N} \longmapsto (x_i)_{i\in M}. \end{aligned}$$

Then the following proposition is essential.

Proposition 1 (the basic exact sequence) *Let D be a right R-submodule of R^n and $M \subseteq N$. Then there is an exact sequence of left R-modules:*

$$0 \longrightarrow \mathcal{L}(D)(N-M) \xrightarrow{\mathrm{inc}} \mathcal{L}(D) \xrightarrow{\mathrm{cut}} R^n(M) \xrightarrow{f} D(M)^* \longrightarrow 0,$$

where the map f is defined by

$$f : \mathbf{y} \longmapsto (\widehat{\mathbf{y}} : \mathbf{x} \mapsto \langle \mathbf{y}, \mathbf{x} \rangle).$$

Using the above proposition, we have a Singleton bound for linear codes over QF rings as follows:

Theorem 1 *Let C be a right (left) linear code of length n over a QF ring R. Then*

$$d(C) \leq n - k(C) + 1,$$

where

$$k(C) := \min\{m \mid \textit{mono morphism } C \to R^m\}.$$

Definition 1 C is called a **Maximum Distance Separable (MDS)** code over a QF ring if

$$d(C) = n - k(C) + 1.$$

Example. Let R be the Galois ring $GR(2^2, 2) = \mathbb{Z}_4[X]/(X^2 + X + 1)$ and let C be the linear code over R with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & \omega \\ 0 & 0 & 1 & 1 & 3\omega \\ 0 & 0 & 0 & 2 & 2 \end{pmatrix},$$

where $\omega \in R^*$ is a primitive third root of unity. Then $n = 5, k(C) = 4$ and $d(C) = 2$. So this code is a kind of MDS codes.

3 Duality for MDS codes.

In the remaining part of this note, let R be a finite local Frobenius ring. For a right R-submodule D of R^n, we denote an *injective hull* of D by $I(D)$ and the *socle* of D by $\mathrm{Soc}(D)$. We define $F_M(D)$ as a maximum free R-submodule of D.

Lemma 1 *Let C be a right linear code of length n over R. Then*

$$d(C) = d(\mathrm{Soc}(C)) = d(I(C)).$$

Theorem 2 *If C is a right linear MDS code of length n over R, then $F_M(\mathcal{L}(C))$ is also an MDS code.*

Remark 1. Theorem 2 claims that though we can take $F_M(\mathcal{L}(C))$ in the various way, if C is an MDS code, then the minimum (Hamming) weight of $F_M(\mathcal{L}(C))$ is uniquely decided by $d(C)$ for all $F_M(\mathcal{L}(C))$.

Proof. If we put $D := I(C)$, then $\mathcal{L}(D) = F_M(\mathcal{L}(C))$. Take any subset $M \subsetneq N$ such that $|M| = d(C) - 1$, then $D(M)^* = 0$ from Lemma 1. By Proposition 1,

$$0 \to \mathcal{L}(D)(N - M) \to \mathcal{L}(D) \to R^n(M) \to 0.$$

So we have the following relation:

$$\mathcal{L}(D) \cong \mathcal{L}(D)(N - M) \oplus R^n(M).$$

Thus

$$k(\mathcal{L}(D)) \geq k(R^n(M)) = |M| = d(C) - 1.$$

We assume that C is an MDS code. Since $\mathcal{L}(D)(N-M) = \{\mathbf{0}\}$ for any M,

$$|N-M| \leq d(\mathcal{L}(D)) - 1 \leq n - k(\mathcal{L}(D)) = |N-M|.$$

Thus we have the following equation:

$$d(\mathcal{L}(D)) - 1 = n - k(\mathcal{L}(D)).$$

∎

4 Weight distributions for MDS codes.

For a right (left) linear code C of length n over R, we define the (Hamming) *weight enumerator* with two indeterminates X and Y, as follows:

$$\begin{aligned} W_C(X,Y) &:= \sum_{\mathbf{x}\in C} X^{n-\mathrm{wt}(\mathbf{x})}Y^{\mathrm{wt}(\mathbf{x})} \\ &= \sum_{i=0}^{n} A_C(i)X^{n-i}Y^i, \end{aligned}$$

where $A_C(i) := |\{\mathbf{x} \in C \mid \mathrm{wt}(\mathbf{x}) = i\}|$. The following result is well-known as the MacWilliams identity for linear codes over Frobenius rings.

Lemma 2 (Wood [8]) *For a finite Frobenius ring R and a right linear code C of length n over R,*

$$W_C(X,Y) = \frac{1}{|\mathcal{L}(C)|} W_{\mathcal{L}(C)}(X + (|R|-1)Y, X - Y).$$

We denote the (Jacobson) *radical* of R by $J(R)$. Using this lemma and Theorem 2, we have the following result.

Theorem 3 *Let C be a right (left) linear code of length n over R. If C is an MDS code, then, for any i,*

$$\begin{aligned} &\binom{n}{i} \sum_{j=0}^{i-d(C)} (-1)^j \binom{i}{j} (|R/J(R)|^{i-d(C)+1-j} - 1) \\ &\qquad \leq A_C(i) \leq \\ &\binom{n}{i} \sum_{j=0}^{i-d(C)} (-1)^j \binom{i}{j} (|R|^{(i-d(C)+1-j)} - 1). \end{aligned}$$

Remark 2. The first equality holds for all i if and only if C is a semi-simple module, and the second equality holds for all i if and only if C is a free module.

Corollary 1 *Let C be an MDS code of length n over R. If $k(C) \geq 2$, then*

$$|R/J(R)| \geq n - k(C) + 1.$$

For example, if $R = \mathbb{Z}_4$, then $|R/J(R)| = 2$ and $k(C)$ means the minimum number of generators for C. The above corollary suggests that if C is an MDS code of length n over $\mathbb{Z}_4$, then $k(C) = n - 1, n$.

5 Reed-Solomon codes over QF rings.

In this section, we introduce a kind of MDS codes over a QF ring R. We define the *right (left) cyclic* code C of length n over R as a right (left) ideal of $R[X]/(X^n - 1)$ (see [2]). We put $F := R/J(R)$. We define the map Φ as follows:

$$\begin{aligned} \Phi \ &: \ \mathrm{Soc}_R(R[X]/(X^n - 1)) \longrightarrow F[X]/(X^n - 1) \\ &; \ X^i \longmapsto X^i. \end{aligned}$$

Therefore Φ is an $R[X]$-isomorphism and $\mathrm{Soc}(C)$ is also a cyclic code of length n over F. For a right cyclic code C over R, $f(X) \in R[X]$ is called the *generator polynomial* for C if $\Phi(f(X))$ is the generator polynomial for $\Phi(\mathrm{Soc}(C))$. Then we have the following lemma.

Lemma 3 *Let C be a right (left) cyclic code of length n over R with generator polynomial $f(X) \in R[X]$. Then*

$$k(C) = n - \deg(f(X)).$$

Definition 2 A right (left) cyclic code C of length n over R with generator polynomial $f(X) \in R[X]$ is called a right (left) **Reed-Solomon** code if $n = |R/J(R)| - 1$ and

$$\Phi(f(X)) = (X - \omega)(X - \omega^2) \cdots (X - \omega^{\delta - 1}),$$

where ω is a primitive n^{th} root of unity in $R/J(R)$ and $2 \leq \delta \leq n$.

Theorem 4 *Let C be a right (left) Reed-Solomon code over a local Frobenius ring R. Then C is an MDS code.*

References

[1] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, New York: Interscience Publishers, 1962.

[2] M. Greferath, Cyclic codes over finite rings, *Discrete Math.*, **177** (1997) 273–277.

[3] H. Horimoto and K. Shiromoto, A Singleton bound for linear codes over quasi-Frobenius rings, *Proceedings of the 13th Algebra, Algebraic Algorithms and Error-Correcting Codes (Hawaii, 1999)*, (to appear).

[4] H. Horimoto and K. Shiromoto, MDS codes over finite rings, (submitted).

[5] T. Y. Lam, *Lectures on modules and rings, Graduate Texts in Math.*, **189** Springer-Verlag, New York, 1998.

[6] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam 1977.

[7] B. R. McDonald, *Finite rings with identity, Pure and Applied Mathematics*, **28** Marcel Dekker, Inc., New York, 1974.

[8] J. A. Wood, Duality for modules over finite rings and applications to coding theory, *American journal of Mathematics*, **121** (1999), 555–575.

正20面体方程式とモジュラ形式[1]

関口次郎　（姫路工業大学）

1. この原稿は，昨年 (1998 年) 末から九州大学の坂内英一教授，小池正夫教授，宗政昭弘助教授との共同研究の内容の報告である．筆者はクラインの著書 Vorlesungen über das Ikosaeder [8] を翻訳した．同書の正 20 面体に関するクラインの成果を多少理解している．そういう理由によるだろうが，コード理論と正多面体群の不変式について坂内教授から質問を受けた．その質問に関連した事柄のやりとりからこの研究は始まった．当然ながら，この内容は正 20 面体群に関係する部分に重点をおいている．問題の背景あるいは理論の全体像は，坂内 [2] に詳しく述べられている．また，Ebeling [3] Chap. 5 にも関係する話題が扱われている．

2. 正 20 面体方程式とはなにか，わからなくても正 20 面体と関係するであろうことは誰にでも連想できることだが，モジュラ形式となると，正 20 面体あるいは正 20 面体方程式とどう結びつくのかすぐには見えてこない．方程式があれば解が問題になるが，この場合，正 20 面体方程式の解がある種のモジュラ形式を使って表示できる．これが題名に「モジュラ形式」が入っている理由である．この事実を出発点にして本講演のテーマを展開する．

3. 正多面体方程式はクラインによって導入された．本講演では，正 20 面体方程式に主眼をおいている関係で，正 20 面体方程式に限定してその定義と関連することを簡単に説明する．

正 20 面体 M を考える．その外接球 S^2 と複素射影直線 $\mathbf{P}^1$ を同一視する．M には 20 枚の面と 30 本の稜と 12 個の頂点がある．それぞれの面の中心，稜の中点，頂点を S^2 の中心から S^2 に投影することによって，$\mathbf{P}^1$ の点を得る．それらを次のように表す：

$$\begin{array}{ll} a_1,\dots,a_{20} & \text{面の中心に対応する } \mathbf{P}^1 \text{ の点} \\ b_1,\dots,b_{30} & \text{稜の中点に対応する } \mathbf{P}^1 \text{ の点} \\ c_1,\dots,c_{12} & \text{頂点に対応する } \mathbf{P}^1 \text{ の点} \end{array}$$

$\mathbf{C}$ を $\mathbf{P}^1$ に自然に埋め込み，z を $\mathbf{C}$ の標準的な座標変数として，

$$\begin{aligned} f_1 &= \textstyle\prod_{i=1}^{20}(z-a_i) \\ f_2 &= \textstyle\prod_{i=1}^{30}(z-b_i) \\ f_3 &= \textstyle\prod_{i=1}^{12}(z-c_i) \end{aligned}$$

とおく．これらの具体形を求める．$z=u_1/u_2$ として斉次化すると，

$$(1)\quad \begin{cases} f &= u_1u_2(u_1^{10}+11u_1^5u_2^5-u_2^{10}) \\ H &= -(u_1^{20}+u_2^{20})+228(u_1^{15}u_2^5-u_1^5u_2^{15})-494u_1^{10}u_2^{10} \\ T &= u_1^{30}+u_2^{30}+522(u_1^{25}u_2^5-u_1^5u_2^{25})-10005(u_1^{20}u_2^{10}+u_1^{10}u_2^{20}) \end{cases}$$

[1] 第 16 回代数的組み合わせ論シンポジウム，1999/6/24-6/25, 九州大学国際ホール

が得られる．(f_1, f_2, f_3 と H, T, f では定数倍の違いがあるが，後者はクライン [8] の記号．)
f, H, T の間には次の関係式が成り立つ．

(2) $T^2 + H^3 - 1728f^5 = 0.$

4. クラインはまず

(3) $$Z = \frac{H^3}{1728f^5}$$

を考えた．この式より z 空間 ($\simeq \mathbf{P}^1$) から Z 空間 ($\simeq \mathbf{P}^1$) への有理写像を定義できる．その逆関数 $z = F(Z)$ は超幾何関数が代数関数になる場合で，このことはクラインより以前にシュワルツの研究でわかっていたことである．

さて，(3) は Z をパラメータにもつ z の60次代数方程式とみなせるが，クラインはこれを「正20面体方程式」と呼んだ．この方程式を5次代数方程式の解法に応用することが [8] の後半の主要なテーマである．

クラインが次に考えたことは Z を絶対不変式 $J(\tau)$ にしたときに z はどうなるか，ということであった[2]．つまり，

(4) $$J(\tau) = \frac{H^3}{1728f^5}$$

となる τ の関数 z を求めよ，という問題である．(これも正20面体方程式と呼ぶことにする．) [8] の第I部 §5.7 ([8] の訳者による付録も参照) に次のことが述べられている．

(5) $$\Lambda(\tau) = q^{2/5}\frac{\sum_{k=-\infty}^{+\infty}(-1)^k q^{5k^2-3k}}{\sum_{k=-\infty}^{+\infty}(-1)^k q^{5k^2-k}} \quad (q = e^{\pi i \tau})$$

とおけば，$z = \Lambda(\tau)$ は

(6) $$J(\tau) = \frac{\{-(z^{20}+1) + 228(z^{15}-z^5) - 494z^{10}\}^3}{1728z^5(z^{10}+11z^5-1)^5}$$

を満たす．これは，$z = \Lambda(\tau)$ が (4) の解になることを意味する．式 (6) はラムダ関数 $\lambda(\tau)$ と $J(\tau)$ の間の関係式

$$J(\tau) = \frac{4}{27}\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$$

の類似である．

5. 昨年 (1998年) 夏に，筆者はこの周辺の話題について調べていたのだが，特に特筆するような成果を得ることはできなかった．多少興味あるかもしれない結果は Halphan 型微分

[2] $J(\tau)$ は次のように正規化したものとする：

$$J(\tau) = \frac{1}{1728q^2}\{1 + 744q^2 + 196884q^4 + O(q^6)\}$$

方程式を決定したことである．少しそれに言及しておく．$w=\Lambda(\tau)^5$ の満たす微分方程式はシュワルツ微分を用いて表すことができるが，それと同等だが Halphen の流儀による非線形微分方程式を決定できる (cf. [4], [11], [12])．[4] によれば次のようになる．まず，

$$w^2+11w-1=0$$

の 2 根を α,β とする．このとき，

$$u=\frac{1}{2}\frac{w''}{w'},v_1=\frac{1}{2}\frac{w'}{w},v_2=\frac{1}{2}\frac{w'}{w-\alpha},v_3=\frac{1}{2}\frac{w'}{w-\beta}$$

とおけば，

$$(7)\quad \begin{cases} v_1' &=& -2v_1^2+2uv_1 \\ v_2' &=& -2v_2^2+2uv_2 \\ v_3' &=& -2v_3^2+2uv_3 \\ u' &=& u^2-(v_1^2+v_2^2+v_3^2-\frac{2\sqrt{5}}{5}v_1v_2+\frac{2\sqrt{5}}{5}v_1v_3-2v_2v_3) \\ 0 &=& -\alpha v_1v_2+\beta v_1v_3+(\alpha-\beta)v_2v_3 \end{cases}$$

もちろん，ここでは w を τ の関数とみており，$w'=dw/d\tau$ etc. である．最後の式は u,v_1,v_2,v_3 の間の制約条件である．微分方程式 (7) は Halphan 型微分方程式と呼ばれるものの例になる．

6. そうこうしていた 11 月のある日，九州大学の坂内英一教授から興味深い e-mail を受け取った．その後の展開をすべて見通している内容なのでそれを再現しておく．

%%%

関口様、数学の質問です。（例によって全くの素人の質問で申し訳ありません。）この種のことは昔の Klein の仕事の中にあるのかもしれないと思い、お尋ねする次第です。

1. E_4,E_6 を通常の Eisenstein series として、例えば、

$$\begin{aligned} f^8+14f^4g^4+f^8 &= E_4, \\ f^{12}-33f^8g^4-33f^4g^8+g^{12} &= E_6 \end{aligned}$$

を満たす上半平面上の正則関数 f,g は（一意的に？）決めることは出来るのでしょうか。（Jacobi のテーター関数 $f=\theta_3(2\tau),g=\theta_2(2\tau)$ が一つの解ですが？）（正則性だけで弱すぎるならばある種の modular forms になっていることを仮定して。この場合は f,g は $\Gamma(4)$ の weight 1/2 の modular form になっていますが。）

2．例えば、

$$\begin{aligned} f^4+8fg^3 &= E_4, \\ f^6-20f^3g^3-8g^6 &= E_6 \end{aligned}$$

を満たす上半平面上の正則関数 f,g は（一意的に？）決めることは出来るのでしょうか。（答えは

$$\begin{aligned} f &= 1+6(q+q^3+q^4+2q^7+q^9+q^{12}+2q^{13}+....), \\ g &= 3q^{1/3}(1+q+2q^2+2q^4+......) \end{aligned}$$

が一つの解ですが？ (f,g は $\Gamma(3)$ の weight 1 の modular form になっていますが。)

3. 本当に知りたいのは、

$$\begin{aligned}(f^{20}+g^{20})-228(f^{15}g^5-f^5g^{15})+494f^{10}g^{10} &= E_4,\\ (f^{30}+g^{30})+522(f^{25}g^5-f^5g^{25})-10005(f^{20}g^{10}-f^{10}g^{20}) &= E_6\end{aligned}$$

(Klein の訳本の 59 ページの多項式）を満たす上半平面上の正則関数 f, g なのですが。

もし、問 3 の答えがわかると、それが、主合同部分群 $\Gamma(5)$ の weight 1/5 の modular forms になっているはずと考えています。(weight 1/5 の modular forms が何かは良くしらないのですが、そのようなものがあるとして。）逆に、主合同部分群 $\Gamma(5)$ の weight 1/5 の modular forms という条件を付けて、問 3 の解を決めても良いのですが。（問 3 の式は右辺の E_4, E_6 の前に定数が加わる可能性もあります。）

坂内英一

%%

1, 2, 3 はそれぞれ正 8 面体方程式，正 4 面体方程式，正 20 面体方程式と関係している．1, 2 については Ebeling ([3]) で取り上げている．3 はどういうわけかそこでは扱われていない．その代わりに Hirzebruch の Hilbert modular 群と正 20 面体群の関係を調べた結果を扱っている．

7. この質問を受け取って，まさしくその解答はすでにクラインによって得られていたことか，あるいはそれを詳しく吟味すればでてくるもののように感じられた．以下ではこの質問に対する解答を説明していく．

8. まず何を考えるのか？それは (u_1, u_2) についての次の連立方程式である：

$$(\mathrm{HIEQ})\begin{cases} E_4(\tau) = u_1^{20}+u_2^{20}-228(u_1^{15}u_2^5-u_1^5u_2^{15})+494u_1^{10}u_2^{10}(=-H)\\ E_6(\tau) = u_1^{30}+u_2^{30}+522(u_1^{25}u_2^5-u_1^5u_2^{25})-10005(u_1^{20}u_2^{10}+u_1^{10}u_2^{20})(=T)\end{cases}$$

ここで $E_{2k}(\tau)\,(k=2,3)$ は正規化されたアイゼンシュタイン級数である．この方程式と正 20 面体方程式との関係を見てみよう．以下では

$$q = e^{\pi i\tau}$$

を断りなく使う．

$$\frac{J(\tau)}{J(\tau)-1} = \frac{E_4(\tau)^3}{E_6(\tau)^2}$$

に注意する．この式を書き直せば

$$J(\tau) = \frac{E_4(\tau)^3}{E_4(\tau)^3-E_6(\tau)^2}$$

を得る．したがって，(u_1, u_2) が (HIEQ) の解であれば，$E_4(\tau)=-H, E_6(\tau)=T$ と関係式 (2) より，$J(\tau)=T^3/(1728f^5)$ が成り立つ．すなわち，$z=u_1/u_2$ は正 20 面体方程式の解になる．この意味で，(HIEQ) を「斉次正 20 面体方程式」と呼ぶことにする．

正 20 面体方程式の解 $z=\Lambda(\tau)$ の定義 (5) を見ると，$\alpha_1 = q^{2/5}\sum_{k=-\infty}^{\infty}(-1)^k q^{5k^2-3k}, \alpha_2 = \sum_{k=-\infty}^{\infty}(-1)^k q^{5k^2-k}$ とおけば，$(u_1, u_2) = (\alpha_1, \alpha_2)$ が斉次正 20 面体方程式の解になるだろうと期待される．この安易な発想は間違っているが，しかしながら，当たらずといえども遠からず．次が成り立つことを小池氏が証明した．

Theorem 1 α_1, α_2 を下のように定義すれば，$(u_1, u_2) = (\alpha_1, \alpha_2)$ は斉次正 *20* 面体方程式の解になる．

$$\begin{aligned}\alpha_1(\tau) &= q_0^{-3/5} q^{2/5} \sum_{k=-\infty}^{\infty} (-1)^k q^{5k^2-3k},\\ \alpha_2(\tau) &= q_0^{-3/5} \sum_{k=-\infty}^{\infty} (-1)^k q^{5k^2-k}\end{aligned}$$

ここで

$$q_0 = \prod_{n=1}^{\infty}(1-q^{2n})$$

これで，(HIEQ) の解が少なくとも一つ構成できたことになる．

それでは，次に (HIEQ) の解をすべて構成する．斉次正 20 面体方程式をみると，$(w_1, w_2) = (u_1^5, u_2^5)$ の方程式とみなせる．そこで斉次正 20 面体方程式を (w_1, w_2) の方程式に書き直して，w_1 を消去して w_2 だけの方程式を求める．すると $t = w_2^2 (= u_2^{10})$ についての方程式

$$g(t) = 0$$

を得る．ここで

$$\begin{aligned}g(t) = {} & 2^{12}\cdot 3^6\cdot 5^{25}t^{12} - 2^{13}\cdot 3^6\cdot 5^{21}\cdot 11\cdot 17E_4t^{10} - 2^{12}\cdot 3^6\cdot 5^{20}\cdot 7\cdot 11\cdot 13E_6t^9\\ & -2^{12}\cdot 3^6\cdot 5^{16}\cdot 7\cdot 11\cdot 43^2E_4^2t^8 - 2^{13}\cdot 3^6\cdot 5^{15}\cdot 11\cdot 3557E_4E_6t^7\\ & -2^7\cdot 3^3\cdot 5^{11}(11\cdot 179\cdot 229\cdot 1847E_4^3 + 5^3\cdot 7^2\cdot 11\cdot 61\cdot 271E_6^2)t^6\\ & -2^{12}\cdot 3^6\cdot 5^{10}\cdot 11\cdot 41\cdot 181E_4^2E_6t^5\\ & -2^7\cdot 3^4\cdot 5^6\cdot 11(23\cdot 31\cdot 111509E_4^3 - 5^3\cdot 13\cdot 79\cdot 587E_6^2)E_4t^4\\ & +2^9\cdot 3^3\cdot 5^5\cdot 11(7\cdot 223\cdot 541E_4^3 - 5^3\cdot 17\cdot 409E_6^2)E_6t^3\\ & +2^7\cdot 3^3\cdot 11(-3196001E_4^3 + 5^4\cdot 4721E_6^2)E_4^2t^2\\ & -2^8\cdot 3^3(307E_4^3 + 5^3E_6^2)E_4E_6t + (E_4^3 - E_6^2)^2.\end{aligned}$$

さらに，w_1 は w_2 の多項式で表される．$w_1 = u_1^5$ を考慮すれば，斉次正 20 面体方程式の解は $120 \times 5 = 600$ 個存在することがわかる．

9. ここで，二項正 20 面体群の復習をする．[8] によれば，以下のような (u_1, u_2) の線形変換が二項正 20 面体変換のすべてである：

$$A_\mu : \begin{cases} u_1' &= \pm\varepsilon^{3\mu}\cdot u_1,\\ u_2' &= \pm\varepsilon^{2\mu}\cdot u_2,\end{cases}$$

$$B_\mu : \begin{cases} u_1' &= \mp\varepsilon^{2\mu}\cdot u_2,\\ u_2' &= \pm\varepsilon^{3\mu}\cdot u_1,\end{cases}$$

$$C_{\mu,\nu} : \begin{cases} \sqrt{5}u_1' &= \pm\varepsilon^{3\nu}(-(\varepsilon-\varepsilon^4)\varepsilon^{3\mu}\cdot u_1 + (\varepsilon^2-\varepsilon^3)\varepsilon^{2\mu}\cdot u_2),\\ \sqrt{5}u_2' &= \pm\varepsilon^{2\nu}(+(\varepsilon^2-\varepsilon^3)\varepsilon^{3\mu}\cdot u_1 + (\varepsilon-\varepsilon^4)\varepsilon^{2\mu}\cdot u_2),\end{cases}$$

$$D_{\mu,\nu} : \begin{cases} \sqrt{5}u_1' &= \mp\varepsilon^{2\nu}(+(\varepsilon^2-\varepsilon^3)\varepsilon^{3\mu}\cdot u_1 + (\varepsilon-\varepsilon^4)\varepsilon^{2\mu}\cdot u_2),\\ \sqrt{5}u_2' &= \pm\varepsilon^{3\nu}(-(\varepsilon-\varepsilon^4)\varepsilon^{3\mu}\cdot u_1 + (\varepsilon^2-\varepsilon^3)\varepsilon^{2\mu}\cdot u_2),\end{cases}$$

ここで $\mu,\nu=0,1,2,3,4$ であり，$\varepsilon=e^{2\pi i/5}$ とした．T,H などはこれらの変換で不変になることに注意すれば，斉次正20面体方程式の解 $(u_1,u_2)=(\beta_1,\beta_2)$ に対して，$A_\mu,B_\mu,C_{\mu,\nu},D_{\mu,\nu}$ などを (β_1,β_2) に作用させたものも斉次正20面体方程式の解になる．一方では，$g(\beta_2^{10})=0$ も成り立つ．これらのことから，$g(t)$ は次のように因数分解される：

$$\begin{aligned} g(t) &= 2^{12}\cdot 3^6\cdot 5^{-25}(t-\alpha_1^{10})(t-\alpha_2^{10}) \\ &\quad\times\prod_{\mu=0}^{4}[5^5t-\{-(\varepsilon-\varepsilon^4)\varepsilon^{3\mu}\cdot\alpha_1+(\varepsilon^2-\varepsilon^3)\varepsilon^{2\mu}\cdot\alpha_2\}^{10}] \\ &\quad\times\prod_{\mu=0}^{4}[5^5t-\{+(\varepsilon^2-\varepsilon^3)\varepsilon^{3\mu}\cdot\alpha_1+(\varepsilon-\varepsilon^4)\varepsilon^{2\mu}\cdot\alpha_2\}^{10}] \end{aligned}$$

10. Theorem 1 で定義した $\alpha_1(\tau),\alpha_2(\tau)$ を調べる．まず，アイゼンシュタイン級数の基本的な性質だが，

$$E_{2k}\left(\frac{a\tau+b}{c\tau+d}\right)=(c\tau+d)^{2k}E_{2k}(\tau)\quad\left(\forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL(2,\mathbf{Z}),k=2,3,4,\dots\right),$$

が成り立つ．このことから，$(\beta_1(\tau),\beta_2(\tau))$ が (HIEQ) の解であれば，

$$\left((c\tau+d)^{-\frac{1}{5}}\beta_1\left(\frac{a\tau+b}{c\tau+d}\right),(c\tau+d)^{-\frac{1}{5}}\beta_2\left(\frac{a\tau+b}{c\tau+d}\right)\right)\quad\left(\forall\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL(2,\mathbf{Z})\right)$$

もそうである．

$SL(2,\mathbf{Z})$ の生成元を定義しておく．

$$S=\begin{pmatrix}1&1\\0&1\end{pmatrix},\quad T=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$$

とおけば，S,T は $SL(2,\mathbf{Z})$ を生成する．また，$SL(2,\mathbf{R})$ の元の τ への作用は

$$\begin{pmatrix}a&b\\c&d\end{pmatrix}\cdot\tau=\frac{a\tau+b}{c\tau+d}$$

で定義する．特に

$$S\tau=\tau+1,\quad T\tau=-\frac{1}{\tau}$$

である．

定義式をみれば，$\alpha_1(\tau),\alpha_2(\tau)$ が変換 $S\tau=\tau+1$ によってどう変化するかはすぐにわかる．結果は以下の通りである：

$$(8)\quad\begin{cases}\alpha_1(\tau+1) &= \varepsilon\alpha_1(\tau)\\ \alpha_2(\tau+1) &= \alpha_2(\tau).\end{cases}$$

一方，$\alpha_1(\tau),\alpha_2(\tau)$ が変換 $T\tau=-\frac{1}{\tau}$ によってどう変化するかはすぐにはわからない．変換 $T\tau=-\frac{1}{\tau}$ に対してどうなるかについて説明する．そのために，まず Dedekind のエータ関数と Jacobi のテータ関数を導入する：

$$\begin{aligned}\eta(\tau) &= q^{\frac{1}{12}}\prod_{n=1}^{\infty}(1-q^{2n}),\\ \vartheta_3(v,\tau) &= \sum_{n=-\infty}^{+\infty}q^{n^2}e^{2\pi niv}\\ &= \prod_{n=0}^{\infty}(1-q^{2n+2})(1+q^{2n+1}e^{2\pi iv})(1+q^{2n+1}e^{-2\pi iv})\end{aligned}$$

次はよく知られている公式である：

$$(9)\quad \begin{aligned} \eta\left(-\frac{1}{\tau}\right) &= e^{-\frac{\pi i}{4}}\tau^{\frac{1}{2}}\eta(\tau) \\ \vartheta_3\left(\frac{v}{\tau},-\frac{1}{\tau}\right) &= e^{\frac{\pi i v^2}{\tau}}e^{-\frac{\pi i}{4}}\tau^{\frac{1}{2}}\vartheta_3(v,\tau) \end{aligned}$$

$\vartheta_3(v,\tau)$ の q 展開式より，$\alpha_1(\tau),\alpha_2(\tau)$ は次のように表示できる．

$$(10)\quad \begin{cases} \alpha_1(\tau) &= q^{\frac{9}{20}}\eta(\tau)^{-\frac{3}{5}}\vartheta_3\left(\dfrac{3\tau+1}{2},5\tau\right) \\ \alpha_2(\tau) &= q^{\frac{1}{20}}\eta(\tau)^{-\frac{3}{5}}\vartheta_3\left(\dfrac{\tau+1}{2},5\tau\right) \end{cases}$$

エータ関数とテータ関数の変換公式 (9) を使うと，次の公式が証明できる．

Lemma 1 (11)
$$\begin{cases} \sqrt{5}\tau^{-\frac{1}{5}}\alpha_1\left(-\dfrac{1}{\tau}\right) &= -\varepsilon\{-(\varepsilon-\varepsilon^4)\alpha_1(\tau)+(\varepsilon^2-\varepsilon^3)\alpha_2(\tau)\} \\ \sqrt{5}\tau^{-\frac{1}{5}}\alpha_2\left(-\dfrac{1}{\tau}\right) &= -\varepsilon\{(\varepsilon^2-\varepsilon^3)\alpha_1(\tau)+(\varepsilon-\varepsilon^4)\alpha_2(\tau)\} \end{cases}$$

Remark 1 (1) [8], p.42 の斉次正 20 面体変換 T と補題の右辺は同じになる．

(2) この補題を計算して後のある日，大学生協の書籍部で「数学って何だろう」[6] という本を何とはなしに手にして中身をみたところ，なにやら同じような式がでているのに気づいた．$\vartheta_3\left(\frac{3\tau+1}{2},5\tau\right),\vartheta_3\left(\frac{\tau+1}{2},5\tau\right)$ は Rodgers-Ramanujan の恒等式に現れる式で，さらにこれらはバクスターによって求められた統計物理のある問題の exact solution としても現れ，特に補題の $\tau\to-1/\tau$ についての変換公式が臨界温度での挙動の調べるのに使われていることがわかった．これらの話題については，[6] の他に [1], [13] なども参照されるとよい．

この補題から次の定理が得られる．

Theorem 2 次の式で定義される $(\alpha_1'(\tau),\alpha_2'(\tau))$ もまた斉次正 *20* 面体方程式の解になる．

$$(12)\quad (\alpha_1'(\tau),\alpha_2'(\tau))=\left(\tau^{-\frac{1}{5}}\varepsilon^3\alpha_1\left(-\frac{1}{\tau}\right),\tau^{-\frac{1}{5}}\varepsilon^3\alpha_2\left(-\frac{1}{\tau}\right)\right)$$

11. $\alpha_1(\tau),\alpha_2(\tau)$ の $\Gamma(5)$ についてのモジュラ不変性について説明する．まず

$$\Gamma(5)=\{A\in SL(2,\mathbf{Z});A\equiv I_2\,(5)\}$$

とおく．

宗政によって次の補題が得られた．

Lemma 2 *(1)* $\Gamma(5)$ は *11* 個の元から生成される自由群である.

(2) $\Gamma(5)$ の生成元はすべて $A^{-1}S^5A$ $(A \in SL(2,\mathbf{Z}))$ の形のものに取れる.

(3) 次の元が $\Gamma(5)$ を生成する:

$$m_1 = \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}, \quad m_2 = \begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix}, \quad m_3 = \begin{pmatrix} 6 & 5 \\ -5 & -4 \end{pmatrix}$$
$$m_4 = \begin{pmatrix} -4 & 5 \\ -5 & 6 \end{pmatrix}, \quad m_5 = \begin{pmatrix} 11 & 20 \\ -5 & -9 \end{pmatrix}, \quad m_6 = \begin{pmatrix} -9 & 20 \\ -5 & 11 \end{pmatrix}$$
$$m_7 = \begin{pmatrix} 11 & 5 \\ -20 & -9 \end{pmatrix}, \quad m_8 = \begin{pmatrix} 31 & 45 \\ -20 & -29 \end{pmatrix}, \quad m_9 = \begin{pmatrix} -9 & 5 \\ -20 & 11 \end{pmatrix}$$
$$m_{10} = \begin{pmatrix} -29 & 45 \\ -20 & 31 \end{pmatrix}, \quad m_{11} = \begin{pmatrix} -49 & 125 \\ -20 & 51 \end{pmatrix}.$$

Remark 2 次のように A_j $(j = 2, \ldots, 11)$ を定めれば, $m_j = A^{-1}S^5A_j$ $(j = 2, \ldots, 11)$ が成り立つ.

$$A_2 = T, \quad A_3 = TS, \quad A_4 = TST, \quad A_5 = TS^2, \quad A_6 = TS^{-2},$$
$$A_7 = TS^{-2}T, \quad A_8 = TS^{-2}TS, \quad A_9 = TS^2T, \quad A_{10} = TS^2TS^{-2}, \quad A_{11} = TS^2TS^{-2}.$$

この補題の各生成元の $(\alpha_1(\tau), \alpha_2(\tau))$ への作用を見ることによって, 次が証明できる. 本質的には宗政による.

Theorem 3 $\alpha_1(\tau), \alpha_2(\tau)$ は $\Gamma(5)$ について重み $\frac{1}{5}$ のモジュラ形式である.

この定理の意味やより詳しい内容を以下で説明する.

12. まず, $SL(2,\mathbf{R})$ の普遍被覆群を構成する. 少し遠回りになるが, $SL(2,\mathbf{R})$ と同型な $SU(1,1)$ の普遍被覆群を Pukanszky [14] が構成しているので, それを使う. (実際には, 松下 [10] にならっているので, 孫引きかもしれない. 別の構成が吉田 [16] にある.)

$\tilde{G} = \{(\gamma, \omega);\ |\gamma| < 1,\ \omega \in R\}$ とおく. $a_0 = (\gamma, \omega), a_0' = (\gamma', \omega') \in \tilde{G}$ に対して, それらの積 $a_0'' = (\gamma'', \omega'') = a_0 a_0'$ を

$$(13) \quad \begin{cases} \gamma'' &= \dfrac{\gamma e^{-2i\omega'} + \gamma'}{1 + \gamma\bar{\gamma}' e^{-2i\omega'}} \\ \omega'' &= \omega + \omega' + \dfrac{1}{2i}\{\mathrm{Log}(1 + \gamma\bar{\gamma}' e^{-2i\omega'}) - \mathrm{Log}(1 + \bar{\gamma}\gamma' e^{2i\omega'})\} \end{cases}$$

で定義する. ここで Log$z$ は $z = re^{i\theta}$, $|\theta| < \pi$ に対して $\mathrm{Log}z = \log r + i\theta$ として定義する. $|\gamma\bar{\gamma}' e^{-2i\omega'}| < 1$ なので, ω'' は問題なく定まる. 逆元を求める. 直接計算によって,

$$(\gamma, \omega)^{-1} = (-\gamma e^{2i\omega}, -\omega)$$

がわかる. $\tilde{G}$ は単連結なリー群になる.

$$SU(1,1) = \left\{ \begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix};\ |\alpha|^2 - |\beta|^2 = 1 \right\}$$

として，$\tilde{G}$ から $SU(1,1)$ への写像 ρ を

$$\rho((\gamma,\omega)) = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}$$

で定義する．ここで，

$$\alpha = \frac{e^{i\omega}}{\sqrt{1-|\gamma|^2}}, \quad \beta = \frac{\gamma e^{i\omega}}{\sqrt{1-|\gamma|^2}}.$$

とした．ρ は被覆写像で $\mathrm{Ker}(\rho) = \{(0, n\pi); n \in \mathbf{Z}\}$ がわかる．

$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$ とおいて，$g \in SL(2,\mathbf{R})$ に対して，$\sigma(g) = CgC^{-1}$ とおく．σ は $SL(2,\mathbf{R})$ と $SU(1,1)$ の間の同型をあたえることは明らか．具体的には，

$$C \begin{pmatrix} a & b \\ c & d \end{pmatrix} C^{-1} = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}$$

のとき，

$$\alpha = \frac{1}{2}(a+d+i(b-c)), \quad \beta = \frac{1}{2}(a-d-i(b+c))$$

となる．以上のことから，$\tilde{G}$ から $SL(2,\mathbf{Z})$ への 被覆写像 φ は

$$\varphi((\gamma,\omega)) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

とおけば，

$$\begin{aligned} a &= \frac{\mathrm{Re}\{(1+\gamma)e^{i\omega}\}}{\sqrt{1-|\gamma|^2}}, & b &= \frac{\mathrm{Im}\{(1-\gamma)e^{i\omega}\}}{\sqrt{1-|\gamma|^2}}, \\ c &= -\frac{\mathrm{Im}\{(1+\gamma)e^{i\omega}\}}{\sqrt{1-|\gamma|^2}}, & d &= \frac{\mathrm{Re}\{(1-\gamma)e^{i\omega}\}}{\sqrt{1-|\gamma|^2}} \end{aligned}$$

が成り立つように定義できる．いま

$$\mathcal{G} = \{(\gamma,\omega); |\gamma| < 1, \omega \in \mathbf{R}/10\pi\mathbf{Z}\}$$

とおけば，$\mathcal{G}$ は $SL(2,\mathbf{R})$ の 5 重の被覆群になる．φ_5 を $\mathcal{G}$ から $SL(2,\mathbf{R})$ への被覆写像とする．

次のような対応がある．

$SL(2,\mathbf{R})$	$\longleftrightarrow$	$SU(1,1)$	$\longleftarrow$	$\mathcal{G}$
$u_\theta = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$	$\longleftrightarrow$	$\begin{pmatrix} e^{\frac{i\theta}{2}} & 0 \\ 0 & e^{-\frac{i\theta}{2}} \end{pmatrix}$	$\longleftarrow$	$(0, \frac{\theta}{2}) = \tilde{u}_\theta$
$a_t = \begin{pmatrix} e^{\frac{t}{2}} & 0 \\ 0 & e^{-\frac{t}{2}} \end{pmatrix}$	$\longleftrightarrow$	$\begin{pmatrix} \cosh\frac{t}{2} & \sinh\frac{t}{2} \\ \sinh\frac{t}{2} & \cosh\frac{t}{2} \end{pmatrix}$	$\longleftarrow$	$(\tanh\frac{t}{2}, 0) = \tilde{a}_t$
$n_x = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$	$\longleftrightarrow$	$\begin{pmatrix} 1+\frac{ix}{2} & -\frac{ix}{2} \\ \frac{ix}{2} & 1-\frac{ix}{2} \end{pmatrix}$	$\longleftarrow$	$\left(-\frac{\frac{ix}{2}}{1+\frac{ix}{2}}, \mathrm{Tan}^{-1}\frac{x}{2}\right) = \tilde{n}_x$

$\tilde{u}_\theta$ の θ は $\mathbf{R}/20\pi\mathbf{Z}$ の元である.

$K=\{u_\theta;\theta\in\mathbf{R}\}$, $A=\{a_t;t\in\mathbf{R}\}$, $N=\{n_x;x\in\mathbf{R}\}$ とおけば, 岩沢分解 $SL(2,\mathbf{R})=KAN$ が成り立つ. この分解は一意的であることに注意する. 同様に $\tilde{K}=\{\tilde{u}_\theta;\theta\in\mathbf{R}\}$, $\tilde{A}=\{\tilde{a}_t;t\in\mathbf{R}\}$, $\tilde{N}=\{\tilde{n}_x;x\in\mathbf{R}\}$ とおけば, 岩沢分解 $\mathcal{G}=\tilde{K}\tilde{A}\tilde{N}$ が成り立つ. N と $\tilde{N}$ は同型なので, 岩沢分解の一意性より, $S=n_1$ に対応する $\tilde{N}$ の元は $\tilde{S}=\tilde{n}_1$ とする. 一方, $T=u_\pi$ に対応する $\tilde{K}$ の元として, $\tilde{T}=\tilde{u}_\pi=\left(0,\frac{\pi}{2}\right)$ をとることにする.

13. $A\in SL(2,\mathbf{Z})$ に対して, $\varphi_5(A')=A$ となる $A'\in\varphi_5^{-1}(SL(2,\mathbf{Z}))$ をとる. A' の選び方は一意ではないが, $A'^{-1}\tilde{S}^5A'$ は A から一意に定まる. そこで, $A'^{-1}\tilde{S}^5A'$ を $Ad_A(\tilde{S}^5)$ で表すことにする.

Lemma 3 M_0 を $Ad_A(\tilde{S}^5)\,(A\in SL(2,\mathbf{Z}))$ で生成される $\varphi_5^{-1}(SL(2,\mathbf{Z}))$ の部分群とすると, M_0 は $\Gamma(5)$ に同型である.

(略証) $\Gamma(5)$ が自由群であるので, M_0 が $\mathcal{G}$ の中心元を含まないことがわかる. そのことから, M_0 自身も自由群になり, よって $M\simeq\Gamma(5)$ がでる. []

M_0 の生成元を具体的にあたえておく.

$$\begin{aligned}
\tilde{m}_1 &= \left(-\frac{25+10i}{29},\mathrm{Tan}^{-1}\frac{5}{2}\right) & \tilde{m}_2 &= \left(\frac{25+10i}{29},\mathrm{Tan}^{-1}\frac{5}{2}\right)\\
\tilde{m}_3 &= \left(\frac{5-25i}{26},\mathrm{Tan}^{-1}5\right) & \tilde{m}_4 &= \left(\frac{-5+25i}{26},\mathrm{Tan}^{-1}5\right)\\
\tilde{m}_5 &= \left(\frac{-335-530i}{629},\mathrm{Tan}^{-1}\frac{25}{2}\right) & \tilde{m}_6 &= \left(\frac{-415+470i}{629},\mathrm{Tan}^{-1}\frac{25}{2}\right)\\
\tilde{m}_7 &= \left(\frac{415-470i}{629},\mathrm{Tan}^{-1}\frac{25}{2}\right) & \tilde{m}_8 &= \left(\frac{-1505-3950i}{4229},\mathrm{Tan}^{-1}\frac{65}{2}\right)\\
\tilde{m}_9 &= \left(\frac{335+530i}{629},\mathrm{Tan}^{-1}\frac{25}{2}\right) & \tilde{m}_{10} &= \left(\frac{-1745+3850i}{4229},\mathrm{Tan}^{-1}\frac{65}{2}\right)\\
\tilde{m}_{11} &= \left(\frac{-15425+14290i}{21029},\mathrm{Tan}^{-1}\frac{145}{2}\right)
\end{aligned}$$

とおくと, $M_0=\langle\tilde{m}_i;\ i=1,2,\ldots,11\rangle$ が成り立つ. さて

$$\tilde{S}=\left(\frac{-1-2i}{5},\ \mathrm{Tan}^{-1}\frac{1}{2}\right),\quad \tilde{T}=\left(0,\frac{\pi}{2}\right),\quad \gamma_C=\tilde{T}^2$$

とおく.

$$\varphi_5(\tilde{S})=S,\ \varphi_5(\tilde{T})=T$$

が成り立つ. また γ_C は $\mathcal{G}$ の中心 C を生成する.

$$C=\{\gamma_C^n=(0,n\pi);n=0,1,\ldots,9\}\simeq\mathbf{Z}/10\mathbf{Z}$$

がわかる. M_0 の生成元 $\tilde{m}_i$ への $\tilde{S},\tilde{T}$ の作用を見る. まず, 定義より,

$$\tilde{S}\tilde{m}_1\tilde{S}^{-1}=\tilde{m}_1,\quad \tilde{T}\tilde{m}_i\tilde{T}^{-1}=\tilde{T}^{-1}\tilde{m}_i\tilde{T}\,(i=1,2,\ldots,11)$$

そして次もわかる：

$$
\begin{array}{lll}
\tilde{S}\tilde{m}_2\tilde{S}^{-1} = \tilde{m}_4 & \tilde{T}\tilde{m}_1\tilde{T}^{-1} = \tilde{m}_2 \\
\tilde{S}\tilde{m}_3\tilde{S}^{-1} = \tilde{m}_2 & \tilde{T}\tilde{m}_3\tilde{T}^{-1} = \tilde{m}_4 \\
\tilde{S}\tilde{m}_4\tilde{S}^{-1} = \tilde{m}_6 & \tilde{T}\tilde{m}_5\tilde{T}^{-1} = \tilde{m}_9 \\
\tilde{S}\tilde{m}_5\tilde{S}^{-1} = \tilde{m}_3 & \tilde{T}\tilde{m}_6\tilde{T}^{-1} = \tilde{m}_7 \\
\tilde{S}\tilde{m}_6\tilde{S}^{-1} = \tilde{m}_1\tilde{m}_5\tilde{m}_1^{-1} & \tilde{T}\tilde{m}_8\tilde{T}^{-1} = \tilde{m}_4\tilde{m}_{10}\tilde{m}_4^{-1} \\
\tilde{S}\tilde{m}_7\tilde{S}^{-1} = \tilde{m}_9 & \tilde{T}\tilde{m}_{11}\tilde{T}^{-1} = (\tilde{m}_2\tilde{m}_9\tilde{m}_4\tilde{m}_{10}\tilde{m}_6\tilde{m}_{11}\tilde{m}_1\tilde{m}_5\tilde{m}_8\tilde{m}_3\tilde{m}_7)^{-1} \\
\tilde{S}\tilde{m}_8\tilde{S}^{-1} = \tilde{m}_7 \\
\tilde{S}\tilde{m}_9\tilde{S}^{-1} = \tilde{m}_{10} \\
\tilde{S}\tilde{m}_{10}\tilde{S}^{-1} = \tilde{m}_{11} \\
\tilde{S}\tilde{m}_{11}\tilde{S}^{-1} = \tilde{m}_1\tilde{m}_8\tilde{m}_1^{-1}
\end{array}
$$

クラインの本 [8] との対応をみるために

$$\tilde{U} = \tilde{T}\tilde{S}^2\tilde{T}\tilde{S}^3\tilde{T}\tilde{S}^2$$

を導入しておく．すると

$$\tilde{U} = \left(-\frac{11+22i}{25}, \mathrm{Tan}^{-1}\frac{1}{2} + \frac{5\pi}{2}\right)$$

がわかる．$\tilde{S}, \tilde{T}, \tilde{U}$ の間の関係式をいくつか計算しておく．

$$
\begin{aligned}
(\tilde{S}\tilde{T})^3 &= \gamma_C^2 \\
\tilde{T}\tilde{S}^2\tilde{T}\tilde{S}^3\tilde{T}\tilde{S}^2 &= \gamma_C^{-1}\tilde{T}\tilde{S}^3\tilde{T}\tilde{S}^2\tilde{T}\tilde{S}^3\tilde{m}_5 \\
\tilde{m}_5^{-1}\tilde{U} &= \tilde{U}\tilde{m}_8\tilde{m}_3\tilde{m}_7^{-1}\tilde{m}_3^{-1}\tilde{m}_8^{-1} \\
\tilde{T}\tilde{S}\tilde{T} &= \gamma_C\tilde{S}^4\tilde{T}\tilde{S}^4(\tilde{m}_4\tilde{m}_1)^{-1} \\
\tilde{T}\tilde{S}^2\tilde{T} &= \gamma_C^{-1}\tilde{U}\tilde{S}^3\tilde{T}\tilde{S}^2(\tilde{m}_1\tilde{m}_5)^{-1} \\
\tilde{T}\tilde{S}^3\tilde{T} &= \tilde{U}\tilde{S}^2\tilde{T}\tilde{S}^3(\tilde{m}_4\tilde{m}_6\tilde{m}_1)^{-1} \\
\tilde{T}\tilde{S}^4\tilde{T} &= \tilde{S}\tilde{T}\tilde{S}\tilde{m}_2 \\
\tilde{T}\tilde{S}^{-1}\tilde{T} &= \tilde{S}\tilde{T}\tilde{S} \\
\tilde{S}\tilde{U} &= \gamma_C^2\tilde{U}\tilde{S}^4(\tilde{m}_8\tilde{m}_3\tilde{m}_1)^{-1} \\
\tilde{S}^2\tilde{T}\tilde{S}^3\tilde{T}\tilde{S}^2 &= \gamma_C^{-1}\tilde{S}^3\tilde{T}\tilde{S}^2\tilde{T}\tilde{S}^3\tilde{m}_5 \\
(\tilde{T}\tilde{S}^3\tilde{T}\tilde{S}^2)^3 &= \gamma_C^8(\tilde{m}_8\tilde{m}_3\tilde{m}_7)^{-1} \\
\tilde{U}^2 &= \gamma_C^7(\tilde{m}_8\tilde{m}_3)^{-1}
\end{aligned}
$$

14. $\mathbf{C}[\alpha_1, \alpha_2]$ に作用している位数 600 の複素鏡映群 G_{600} の構成に言及する．(この群の具体的な定義は後述する．) $-I_2 \notin \Gamma(5)$ なので，$\Gamma(5)$ は $PSL(2,\mathbf{Z})$ の部分群と見なせる．さらに，よく知られていることだが，

(14) $PSL(2,\mathbf{Z})/\Gamma(5) \simeq A_5$

が成り立つ．ここで，A_5 は 5 次交代群であり，正 20 面体群と同一視してよい．

次のようにして，G_{600} は自然に構成できる．以前と同じく，

$$\varepsilon = e^{2\pi i/5}$$

として，

$$S_1 = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}, \quad T_1 = \frac{\bar{\varepsilon}}{\sqrt{5}} \begin{pmatrix} -(\varepsilon - \varepsilon^4) & \varepsilon^2 - \varepsilon^3 \\ \varepsilon^2 - \varepsilon^3 & \varepsilon - \varepsilon^4 \end{pmatrix},$$

$$U_1 = T_1 S_1^2 T_1 S_1^3 T_1 S_1^2 = \varepsilon^3 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

とおく．すると

$$(S_1 T_1)^3 = \varepsilon, \quad T_1^2 = -\varepsilon^3 = e^{\pi i/5}$$

が成り立つ．このとき $T_1 S_1^k T_1$ $(k = 1, 2, 3, 4)$ は以下のように表される：

$$T_1 S_1 T_1 = -\varepsilon^3 S_1^4 T_1 S_1^4, \quad T_1 S_1^2 T_1 = -\varepsilon^2 U_1 S_1^3 T_1 S_1^2,$$

$$T_1 S_1^3 T_1 = U_1 S_1^2 T_1 S_1^3, \quad T_1 S_1^4 T_1 = S_1 T_1 S_1.$$

さらに

$$S_1 U_1 = \varepsilon U_1 S_1^4, \quad T_1 U_1 = -U_1 T_1.$$

いま G_{600} を S_1, T_1 で生成される群とする．定義より G_{600} は以下のような元からなる：

$$\pm\varepsilon^j \begin{pmatrix} \varepsilon^k & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm\varepsilon^j \begin{pmatrix} 0 & -1 \\ \varepsilon^k & 0 \end{pmatrix} \quad (j, k = 0, 1, 2, 3, 4),$$

$$\pm\frac{\varepsilon^j}{\sqrt{5}} \begin{pmatrix} -\varepsilon^{k+l}(\varepsilon - \varepsilon^4) & \varepsilon^k(\varepsilon^2 - \varepsilon^3) \\ \varepsilon^l(\varepsilon^2 - \varepsilon^3) & \varepsilon - \varepsilon^4 \end{pmatrix}, \quad \pm\frac{\varepsilon^j}{\sqrt{5}} \begin{pmatrix} -\varepsilon^l(\varepsilon^2 - \varepsilon^3) & -(\varepsilon - \varepsilon^4) \\ -\varepsilon^{k+l}(\varepsilon - \varepsilon^4) & \varepsilon^k(\varepsilon^2 - \varepsilon^3) \end{pmatrix}$$

$$(j, k, l = 0, 1, 2, 3, 4).$$

特に

$$S_1^k = \begin{pmatrix} \varepsilon^k & 0 \\ 0 & 1 \end{pmatrix} \quad (k = 0, 1, 2, 3, 4),$$

$$U_1 S_1^k = \varepsilon^3 \begin{pmatrix} 0 & -1 \\ \varepsilon^k & 0 \end{pmatrix} \quad (k = 0, 1, 2, 3, 4),$$

$$S_1^k T_1 S_1^l = \frac{\varepsilon^4}{\sqrt{5}} \begin{pmatrix} -\varepsilon^{k+l}(\varepsilon - \varepsilon^4) & \varepsilon^k(\varepsilon^2 - \varepsilon^3) \\ \varepsilon^l(\varepsilon^2 - \varepsilon^3) & \varepsilon - \varepsilon^4 \end{pmatrix}, \quad (k, l = 0, 1, 2, 3, 4)$$

$$U_1 S_1^k T_1 S_1^l = \frac{\varepsilon^2}{\sqrt{5}} \begin{pmatrix} -\varepsilon^l(\varepsilon^2 - \varepsilon^3) & -(\varepsilon - \varepsilon^4) \\ -\varepsilon^{k+l}(\varepsilon - \varepsilon^4) & \varepsilon^k(\varepsilon^2 - \varepsilon^3) \end{pmatrix}, \quad (k, l = 0, 1, 2, 3, 4)$$

G_{600} の位数が 600 になることは上の具体的な計算からわかる．

Remark 3 ここで，上記の S_1, T_1, U_1 とクラインの本 *[8]* の *42* ページの S, T, U との関係について言及しておく．線形変換の積を右からするのか左からするのかの違いがあるので，そのままでは一致しないが，だいたい $(S_1, T_1, U_1) \longleftrightarrow (S, T, U)$ という対応になる．

さて，$\varphi_5^{-1}(SL(2,\mathbf{Z}))$ から G_{600} への群準同型 ϖ を

$$\tilde{S} \to S_1, \quad \tilde{T} \to T_1, \quad \varpi(M) = 1$$

で定義する．これが適正に定義されることは上記の $\tilde{S},\tilde{T}$ の間の関係式と S,T の間のそれらからわかる．

いままでの議論から，次の完全列が得られる：

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & 1 & \longrightarrow & M & \longrightarrow & \Gamma(5) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & C & \longrightarrow & \varphi_5^{-1}(SL(2,\mathbf{Z})) & \longrightarrow & PSL(2,\mathbf{Z}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & C & \longrightarrow & \varphi_5^{-1}(SL(2,\mathbf{Z}))/M & \longrightarrow & PSL(2,\mathbf{Z})/\Gamma(5) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

すでに述べたことだが，

$$PSL(2,\mathbf{Z})/\Gamma(5) \simeq \mathcal{A}_5, \quad \varphi_5^{-1}(SL(2,\mathbf{Z}))/M \simeq G_{600}$$

が成り立つ．

15. のちに使うので偏角を定義しておく．$z = re^{i\theta}$ と複素数 z を極座標で表す．ただし，$0 < r$, $-\pi < \theta \leq \pi$ とする．このとき，$\mathrm{Arg}(z) = \theta$ とする．また，

$$\begin{aligned}
\tilde{n}_0(x) &= \left(-\frac{ix}{2+ix}, \mathrm{Tan}^{-1}\frac{x}{2}\right) \\
\tilde{a}_0(y) &= \left(\frac{y-1}{y+1}, 0\right)(y>0) \\
\tilde{u}_0(\omega) &= (0, \omega)
\end{aligned}$$

とおく．岩沢分解より，任意の $(\gamma,\omega) \in \mathcal{G}$ に対して，

$$(\gamma,\omega) = \tilde{n}_0(x)\tilde{a}_0(y)\tilde{u}_0(\omega)$$

が成り立つ $x \in \mathbf{R}$, $y \in \mathbf{R}_{>0}(= \{r \in \mathbf{R}; r > 0\})$, $\omega \in \mathbf{R}/10\pi\mathbf{Z}$ が一意に存在することがわかる．$\mathcal{U} = \{\tilde{u}(0,\omega); \omega \in \mathbf{R}/10\pi\mathbf{Z}\}$ とおけば，岩沢分解の一意性より，$\mathcal{G}/\mathcal{U}$ の元は $\tilde{n}_0(x)\tilde{a}_0(y)\mathcal{U}\,(y>0)$ の形に一意に表される．この元 $\tilde{n}_0(x)\tilde{a}_0(y)\mathcal{U}$ に $z = x+iy$ を対応させることによって，$\mathcal{G}/\mathcal{U}$ と上半平面 H_+ との同一視が得られる．

定義より，

$$\tilde{S}\tilde{n}_0(x)\tilde{a}_0(y) = \tilde{n}_0(x+1)\tilde{a}_0(y),$$

はすぐにわかるが，

$$\tilde{T}\tilde{n}_0(x)\tilde{a}_0(y) = \tilde{n}_0\left(-\frac{x}{x^2+y^2}\right)\tilde{a}_0\left(\frac{y}{x^2+y^2}\right)\tilde{u}_0\left(0,\ \mathrm{Tan}^{-1}\frac{x}{y}+\frac{\pi}{2}\right)$$

も直接計算によって確かめられる．上であたえた上半平面との同一視によれば，

$$\tilde{S}: z \to z+1, \quad \tilde{T}: z \to -\frac{1}{z}$$

がわかり，これは以前で説明した

$$S: z \to z+1, \quad T: z \to -\frac{1}{z}$$

と整合する．

さらに次がわかる．

Lemma 4 任意の $(\gamma,\omega) \in \mathcal{G}, z = x+iy \in H_+$ に対して，

$$(\gamma,\omega)\tilde{n}_0(x)\tilde{a}_0(y) = \tilde{n}_0(x')\tilde{a}_0(y')\tilde{u}_0(\omega'),$$

となる $z' = x'+iy' \in H_+, \omega \in \mathbf{R}/10\pi\mathbf{Z}$ は

$$\begin{aligned} z' &= -i\cdot\frac{\{e^{2i\omega}(\gamma+1)+(\bar{\gamma}+1)\}z + i\{e^{2i\omega}(\gamma-1)-(\bar{\gamma}-1)\}}{\{e^{2i\omega}(\gamma+1)-(\bar{\gamma}+1)\}z + i\{e^{2i\omega}(\gamma-1)+(\bar{\gamma}-1)\}} \\ \omega' &= \omega - \mathrm{Arg}\{-i(z+i)\} - \mathrm{Arg}\left(\frac{(\bar{\gamma}+1)z - i(\bar{\gamma}-1)}{z+i}\right) \\ &\quad + \mathrm{Arg}\left(-\frac{(\bar{\gamma}+1)z - i(\bar{\gamma}-1)}{\{e^{2i\omega}(\gamma+1)-(\bar{\gamma}+1)\}z + i\{e^{2i\omega}(\gamma-1)+(\bar{\gamma}-1)\}}\right), \end{aligned}$$

で表される．

さらに，$\varphi_5((\gamma,\omega)) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ のとき，$z' = \dfrac{az+b}{cz+d}$ となる．

特に $(\gamma,\omega) = \tilde{m}_j (j = 1,2,\ldots,11)$ の場合に計算すると次がわかる．

Lemma 5 *(?)* $j = 1,2,\ldots,11$ に対して，$m_j = \varphi_5(\tilde{m}_j) = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$ のとき，$z_j = x_j+iy_j = \dfrac{a_jz+b_j}{c_jz+d_j}$ で z_j, x_j, y_j などを定義すると，

$$\tilde{m}_j\tilde{n}_0(x)\tilde{a}_0(y) = \tilde{n}_0(x_j)\tilde{a}_0(y_j)\tilde{u}_0(-\mathrm{Arg}(c_jz+d_j))$$

この補題の証明だが，

$$\tilde{m}_j\tilde{n}_0(x)\tilde{a}_0(y) = \tilde{n}_0(x')\tilde{a}_0(y')\tilde{u}_0(\omega')$$

としたとき，$x' = x_j, y' = y_j$ になることを示すのはそれほど難しくはない．$\omega' = -\mathrm{Arg}(c_jz+d_j)$ が成り立つことを示すのが大変である．

16. これから，次の条件 (A1), (A2) を満たす $\mathcal{G}$ 上のベクトル値関数 $F(g) = \begin{pmatrix} f_1(g) \\ f_2(g) \end{pmatrix}$ を考える．

(A1): すべての $g \in \mathcal{G}, \omega \in \mathbf{R}$ に対して，$F(g\tilde{u}_0(\omega)) = e^{i\omega/5}F(g)$ が成り立つ．
(A2): すべての $g \in \varphi_5^{-1}(SL(2,\mathbf{Z}))$ に対して，

$$F(g\tilde{n}_0(x)\tilde{a}_0(y)\tilde{u}_0(\omega)) = J(g;x,y)^{-1/20}\varpi(g)F(\tilde{n}_0(x)\tilde{a}_0(y)\tilde{u}_0(\omega))$$

が成り立つ．ここで ϖ は以前に定義した M_0 から G_{600} への全射準同型とした．

条件 (A1) は $f_1(g), f_2(g)$ いずれもが，上半平面 H_+ 上の同じ均質線束の切断になることを意味する．
この条件 (A1,2) を満たす (ベクトル値) 関数 $F(g)$ に対して

$$F_0(z) = F(\tilde{n}_0(x)\tilde{a}_0(y))$$

とおく．
$g = \tilde{S}, \tilde{T}$ のときに $F(g\tilde{n}_0(x)\tilde{a}_0(y))$ を計算する．

Lemma 6

$$\begin{aligned} F_0(z+1) &= \varpi(\tilde{S})F_0(z) \\ F_0\Big(-\frac{1}{z}\Big) &= -\varepsilon^2 r^{1/5}(e^{i\theta})^{1/5}\varpi(\tilde{T})F_0(z). \end{aligned}$$

ここで，$z = x + iy = re^{i\theta}$ $(r > 0,\ 0 < \theta < \pi)$ とした．

$\alpha_1(\tau), \alpha_2(\tau)$ を 8. の定理で導入した斉次正 20 面体方程式の解のとき，$H_0(z) = \begin{pmatrix} \alpha_1(z) \\ \alpha_2(z) \end{pmatrix}$ とおく．このとき，$H_0(z)$ は上の補題の等式と同じ関係式をみたす．すなわち，

$$\begin{aligned} H_0(z+1) &= \varpi(\tilde{S})H_0(z) \\ H_0\Big(-\frac{1}{z}\Big) &= -\varepsilon^2(re^{i\theta})^{1/5}\varpi(\tilde{T})H_0(z). \end{aligned}$$

が成り立つ．以上の議論から次の結果がわかる．

Theorem 4 *$\alpha_1(\tau), \alpha_2(\tau)$ を前述の斉次正 20 面体方程式の解のとき，$H_0(z) = \begin{pmatrix} \alpha_1(z) \\ \alpha_2(z) \end{pmatrix}$ とおく．このとき，条件 (A1), (A2) を満たす $\mathcal{G}$ 上のベクトル値関数 $F(g) = \begin{pmatrix} f_1(g) \\ f_2(g) \end{pmatrix}$ で $F(\tilde{n}_0(x)\tilde{a}_0(y)) = H_0(x+iy)$ となるものが存在する．*

Remark 4 この定理は坂内，小池，宗政氏との数回の議論をしていた過程で考えたことを筆者なりに定式化してまとめたものである．その後，大阪大学の伊吹山知義氏から教えていただいたことだが，保型形式を表現論的にみるところは専門家にとっては確立していることで，またこのレポートの内容のいくつかはもうすこし一般の分数ウェイトの保型形式についての命題として氏が整理されたそうである．詳しくは氏のレポート「分数ウェイトの 1 変数保型形式について」*([7])* を参照せよ．

参考文献

[1] G. Andrews : *The Theory of Partitions.* Addison-Wesley, 1976.

[2] 坂内英一：モジュラー形式についての考察．研究集会講演報告 (1999)

[3] G. W. Ebeling : *Lattices and Codes.* Vieweg, 1994.

[4] J. Harnad and J. McKay : Modular solutions to equations of generalized Halphen type. preprint.

[5] 平松豊一：数論を学ぶ人のための相互法則．牧野書店 (1998)

[6] 猪狩惺 編：数学って何だろう．第７講：恒等式の背後には... (長谷川浩司　著)（日本評論社, 1997)

[7] 伊吹山知義：分数ウェイトの１変数保型形式について．本報告集収録．

[8] F. Klein 著：正２０面体と５次方程式．シュプリンガー・フェアラーク東京

[9] 久保田富雄：整数論の一側面．一つの新観点からみた平方剰余．科学 38(1964), 551-555.

[10] O. Matsushita: The Plancherel formula for th universal covering group of $SL(2,\mathbf{R})$. Sci. Papers of College of Gen. Ed., Univ. Tokyo, 29 '1979), 105-123.

[11] Y. Ohyama : Differential equations of theta functions. Osaka J. Math. 32 (1995), 431-450.

[12] Y. Ohyama : Systems of nonlinear differential equations related to second order linear equations. Osaka J. Math. 33 (1996), 927-949.

[13] 尾角正人，神保道夫，三輪哲二：2次元の可解な格子模型とモジュラー函数．数学 40(1988), 1-18.

[14] L. Pukanszky: The Plancherel formula for th universal covering group of $SL(R,2)$. Math. Ann. 156(1964), 96-143.

[15] 関口次郎：Icosahedral equation and differential equation. 研究集会「超幾何系ワークショップ in 神戸 '98」予稿.

[16] H. Yoshida: Remarks on metaplectic representations of $SL(2)$. J. Math. Soc. Japan, 44(1992), 351-373.

多重ゼータ値と荒川-金子のゼータ関数の特殊値について

大野泰生

大阪大学 理学研究科・学振研究員

ある種類の多重ゼータ値（本稿では便宜上“多重S値”と呼ぶ）たちの各重さにおける総和が、同じ重さのリーマンゼータ関数の特殊値の有理数倍であることが判ったのでこれを本稿で説明する。昨年の講演の定理で、この種類の多重ゼータ値が荒川—金子のゼータ関数の特殊値を与えていることが判っているので、今回の結果と合わせると、荒川—金子のゼータ関数の正整数点での値のある種の和とリーマンゼータ関数の特殊値との関係式も自動的に導かれる。

まずここで、昨年の講演で述べた定理([18])には含まれなかったが、今回の定理には含まれている関係式の一例を挙げておく。

weight 4 の多重ゼータ値は、

$$\zeta(1,1,2),\quad \zeta(1,3),\quad \zeta(2,2),\quad \zeta(4)$$

の合計4個定義できるが、実はこれら全ての間には有理数係数の線型関係式が存在している。昨年の講演での結果（もしくは sum formula）を用いると、

$$\zeta(1,1,2)=\zeta(4),$$

$$\zeta(1,3)+\zeta(2,2)=\zeta(4)$$

というふたつの関係式が得られる（3章参照）。しかし、昨年の結果からは、次のような関係式は得られない。

$$\zeta(2,2) = \frac{3}{4}\zeta(4).$$

この式の場合は、リーマンゼータ関数の特殊値を用いて次のように導かれる。

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}$$

であるから、

$$\zeta(2)^2 = \frac{5}{2}\zeta(4)$$

である。昨年の報告集にも書いた

$$\begin{aligned}
\zeta(2)^2 &= \left(\sum_{m_1=1}^{\infty} \frac{1}{{m_1}^2}\right)\left(\sum_{m_2=1}^{\infty} \frac{1}{{m_2}^2}\right) \\
&= \sum_{m_1=1}^{\infty}\sum_{m_2=1}^{\infty} \frac{1}{{m_1}^2{m_2}^2} \\
&= \left(\sum_{0<m_1<m_2} \frac{1}{{m_1}^2{m_2}^2}\right) + \left(\sum_{0<m_1=m_2} \frac{1}{{m_1}^2{m_2}^2}\right) + \left(\sum_{0<m_2<m_1} \frac{1}{{m_1}^2{m_2}^2}\right) \\
&= 2\left(\sum_{0<m_1<m_2} \frac{1}{{m_1}^2{m_2}^2}\right) + \left(\sum_{0<m} \frac{1}{m^4}\right) \\
&= 2\zeta(2,2) + \zeta(4)
\end{aligned}$$

なる関係式を利用すれば、

$$\zeta(2,2) = \frac{3}{4}\zeta(4)$$

がわかる。

このように、すでに知られている関係式の中にも、昨年の結果に含まれていない関係式はたくさん存在しているのであるが、それらを多く含むような、関係式の新たな系統立った理解が我々の目標としているところである。今回の結果は、上記の関係式 $\zeta(2,2) = \frac{3}{4}\zeta(4)$ を含むような、昨年の結果とはまた別の、関係式の無限系列である。

昨年の本講演の報告集の記事([18])も合わせて見ていただけるととても嬉しい。

1 多重ゼータ値

まずはじめに、多重ゼータ値を二種類定義する。近年通常、多重ゼータ値と呼ばれているのは、$\zeta(\mathsf{k})$ の方であるが、他方の $S(\mathsf{k})$ も古くから存在し、例えば Euler が扱ったのは、むしろ $S(\mathsf{k})$ の方であった。後に述べるように、この二つの値は互いに関係の深い値である。

整数 $n \geq 1$, $k_1, k_2, \ldots, k_{n-1} \geq 1$ および $k_n \geq 2$ に対して、

$$\mathsf{k} = (k_1, k_2, \ldots, k_n)$$

を index set と呼ぶことにする。今後、index set に付随して決まる次の三つの値が重要になる。

index set $\mathsf{k} = (k_1, k_2, \ldots, k_n)$ に対して、

$k = k_1 + k_2 + \cdots + k_n$ を k の **weight** と言い、

n を k の **depth** と言い、

$s = \sharp\{k_i > 1\}$ を k の **height** と言う。

index set k に対する多重ゼータ値 $\zeta(\mathsf{k})$ を、

$$\zeta(\mathsf{k}) = \zeta(k_1, k_2, \ldots, k_n) = \sum_{0<m_1<m_2<\cdots<m_n} \frac{1}{{m_1}^{k_1} {m_2}^{k_2} \cdots {m_n}^{k_n}}$$

で定義する。他方、$S(\mathsf{k})$ を、

$$S(\mathsf{k}) = \zeta(k_1, k_2, \ldots, k_n) = \sum_{0<m_1\leq m_2\leq\cdots\leq m_n} \frac{1}{{m_1}^{k_1} {m_2}^{k_2} \cdots {m_n}^{k_n}}$$

で定義する。本稿では便宜上、この $S(\mathsf{k})$ のことを、"多重S値" と呼ぶことにする。上述の index set の条件下では、このふたつの級数はそれぞれ収束する。

多重S値と多重ゼータ値の間には関係があって、多重S値を多重ゼータ値で書くことができる。これは、和が絶対収束していることから、和のところの大小関係の

条件を、等号成立時と不等号成立時とに分けることにより導かれる。例えば、以下のような関係式である。

$$S(k_1,k_2)=\zeta(k_1,k_2)+\zeta(k_1+k_2),$$

$$S(\underbrace{1,\dots,1}_{n-1},k-n+1)=\sum_{l=1}^{n}\sum_{a_1+\cdots+a_l=n}\zeta(a_1,\dots,a_{l-1},k-n+a_l).$$

2 主結果

今回の研究で得られた多重S値の線型関係式を述べる。主定理に登場する多重S値の型は、height が 1 のものに限られている。後の節で見るように、荒川一金子のゼータ関数の特殊値に一致していたのは、この型の多重S値であった。height が 1 以上のものについても類似の公式の予想を得ているが、証明は未完成である。

定理 1 任意の整数 $k\geq 2$ に対して次が成り立つ。

$$\sum_{n=1}^{k-1}S(\underbrace{1,\dots,1}_{n-1},k-n+1)=2(k-1)(1-2^{1-k})\zeta(k).$$

定理1の証明には、Kontsevich によって与えられた、多重ゼータ値の "Drinfel'd 積分表示" (cf.[21]) と呼ばれる以下の表記が用いられる。

$$\zeta(k_1,\dots,k_n)=I(1,\underbrace{0,\dots,0}_{k_1-1},1,\underbrace{0,\dots,0}_{k_2-1},\dots,1,\underbrace{0,\dots,0}_{k_n-1}),$$

ただしここで $\varepsilon_1=1,\varepsilon_k=0,\varepsilon_2,\dots,\varepsilon_{k-1}\in\{0,1\}$ とし、$A_0(t)=t$, $A_1(t)=1-t$ とするとき、

$$I(\varepsilon_1,\dots,\varepsilon_k)=\int\cdots\int_{0<t_1<\cdots<t_k<1}\frac{dt_1}{A_{\varepsilon_1}(t_1)}\cdots\frac{dt_k}{A_{\varepsilon_k}(t_k)}$$

とする。sum formula や duality formula そして、昨年の講演で述べた、これらの拡張の定理（定理2）の証明にも上述の Drinfel'd 積分表示が有効である。

定理1の左辺の多重S値は第1節で述べた、多重S値の多重ゼータ値による書き換えの例に合致しているので、これを用いて定理1を多重ゼータ値の和とリーマンゼータ値との関係式として述べることができる。こうして得られた公式は各 weight ごとにひとつずつ関係式を与える、関係式の無限系列になっている。そして、この系列が与える関係式の中に、昨年の講演で述べた関係式の無限系列（定理2）からは構成できないもの（序文で述べた関係式など）が含まれていることがわかっている。

後の節で見るように、荒川—金子のゼータ関数の特殊値への応用だけを考えるなら、定理1で扱った型（つまり height が1）の多重S値だけで十分なのだが、我々には多重ゼータ値の線型関係式の大きな系列を構成する、という他の目的があるので、定理1を一般の height に拡張することが望まれる。これについて、以下の予想を得た。

予想 1 任意の $1 \leq s \leq \frac{k}{2}$ をみたす s, k に対して以下を予想する。

$$\sum_{\substack{height(\mathrm{k})=s,\\ weight(\mathrm{k})=k}} S(\mathrm{k}) = 2\binom{k-1}{2s-1}(1-2^{1-k})\zeta(k).$$

3 復習

この節では、以前筆者が得た多重ゼータ値間の線型関係式について復習したい。この線型関係式は、それ以前から知られていた3つの関係式の無限系列（sum formula, duality formula, Hoffman's formula (詳しくは昨年の報告集参照)）を同時に含んだものであった。

まず dual index を定義する。任意の index set k に対して、

$$\mathrm{k} = (\underbrace{1,\ldots,1}_{a_1-1}, b_1+1, \underbrace{1,\ldots,1}_{a_2-1}, b_2+1, \ldots, \underbrace{1,\ldots,1}_{a_s-1}, b_s+1)$$

をみたす整数 $s \geq 1$ と $a_1, b_1, a_2, b_2, \ldots, a_s, b_s \geq 1$ が、一意的に決まる。(この s が height であった。) それらに対して index set k' を

$$\mathsf{k}' = (\underbrace{1, \ldots, 1}_{b_s - 1}, a_s + 1, \underbrace{1, \ldots, 1}_{b_{s-1} - 1}, a_{s-1} + 1, \ldots, \underbrace{1, \ldots, 1}_{b_1 - 1}, a_1 + 1)$$

と定める。このとき、k' を k の dual index set と呼ぶ。

この節で復習したい関係式は以下のものである。

定理 2 任意の *index set* $\mathsf{k} = (k_1, k_2, \ldots, k_n)$ と整数 $l \geq 0$ に対して $Z(\mathsf{k}; l)$ を

$$Z(\mathsf{k}; l) = \sum_{\substack{c_1 + c_2 + \cdots + c_n = l \\ \forall c_j \geq 0}} \zeta(k_1 + c_1, k_2 + c_2, \ldots, k_n + c_n),$$

とし、k' を k の *dual index set* とする。この時、次が成り立つ。

$$Z(\mathsf{k}'; l) = Z(\mathsf{k}; l).$$

序文で述べたふたつの関係式は以下のようにして得られる:

$\mathsf{k} = (4), \mathsf{k}' = (1,1,2), l = 0$ とすれば、

$$\zeta(1,1,2) = \zeta(4),$$

$\mathsf{k} = (3), \mathsf{k}' = (1,2), l = 1$ とすれば、

$$\zeta(1,3) + \zeta(2,2) = \zeta(4)$$

である。

5 荒川-金子のゼータ関数の特殊値

ここでは、第3節で復習した以前の結果 (定理2) に加えて、第2節で述べた主結果 (定理1) を荒川—金子のゼータ関数の正整数点での特殊値に応用することを述べる。

多重ベルヌーイ数 $B_n^{(k)}$ は、通常のベルヌーイ数の一般化として金子[10]により定義された。$k=1$ の時 $B_n^{(1)}$ は通常のベルヌーイ数である。

荒川一金子[1]は、多重ベルヌーイ数を特殊値に持つような関数 $\xi_k(s)$ を構成した。それは、$k \geq 1$ に対して以下の定義で与えられる。

$$\xi_k(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{t^{s-1}}{e^t - 1} Li_k(1 - e^{-t}) dt.$$

ここで、任意の整数 k に対し、$Li_k(z) = \sum_{m=0}^{\infty} \frac{z^m}{m^k}$ (k-th polylogarithm と呼ばれている関数) である。

荒川一金子 はこの関数が $Re(s) > 0$ で収束し、s の整関数に解析接続され、非正整数点での特殊値は多重ベルヌーイ数で与えられることを示し、$k = 1$ の時に $\xi_1(s) = s\zeta(s+1)$ であることを示した。そしてさらに、このゼータ関数の正整数点での値については、多重ゼータ値で書けるという考察がなされた。つまり、多重ベルヌーイ数と、リーマンゼータ関数の一種の多重化の関数の特殊値である多重ゼータ値とが、この荒川一金子のゼータ関数を介して関連しているのである。荒川一金子のゼータ関数の正整数点の値についての定理は以下のとおりである。

定理 3 (荒川一金子 [1][2]) 整数 $k \geq 1$ と $m \geq 0$ に対して

$$\xi_k(m+1) = \sum_{\substack{a_1+a_2+\cdots+a_k=m \\ \forall a_j \geq 0}} (a_k+1)\zeta(a_1+1, a_2+1, \ldots, a_{k-1}+1, a_k+2).$$

この定理3に定理2を使うと、$\xi_k(s)$ の正整数点での値は以下のように書き換えることができる。

定理 4 整数 $k \geq 1$ と $n \geq 1$ に対して

$$\xi_k(n) = S(\underbrace{1, \ldots, 1}_{n-1}, k+1).$$

つまり、荒川一金子のゼータ関数の特殊値は、非正整数点では多重ベルヌーイ数で与えられ、正整数点では多重S値そのものになるのである。そして、この定理4の右辺の多重S値が、定理1の左辺に見える多重S値と同じ型（つまり height が 1）であることから、定理1を定理4で書き換えることにより、荒川一金子のゼータ関数の特殊値とリーマンゼータ値の関係式が得られる。それは以下のようになる。

定理 5 任意の整数 $k \geq 2$ に対して、次が成り立つ。

$$\sum_{n=1}^{k-1} \xi_{k-n}(n) = 2(k-1)(1-2^{1-k})\zeta(k).$$

参考文献

[1] T. Arakawa and M. Kaneko, Multiple zeta values, poly-Bernoulli numbers, and related zeta functions, *Nagoya Math. J.*, **153** (1999), 1-21.

[2] 荒川恒男 金子昌信, 多重ゼータ値、多重ベルヌーイ数 および関連するゼータ関数, 津田塾大学数学・計算機科学研究所報, **13**, 第2回津田塾大学整数論シンポジウム報告集 (1996), 133-144.

[3] J. M. Borwein, D. M. Bradley and D. J. Broadhurst, Evaluations of k-fold Euler/Zagier sums: a compendium of results for arbitrary k, *preprint* (1996).

[4] J. M. Borwein, D. M. Bradley, D. J. Broadhurst and P. Lisonec, Special values of multidimentional polylogarithms, *preprint*, CECM Research Report 98-106, May, 1998.

[5] D. Borwein, J. M. Borwein and R. Girgensohn, Explicit evaluation of Euler sums, *Proc. Edin. Math. Soc.*, **38** (1995), 277-294.

[6] M. Hoffman, Multiple harmonic series, *Pacific J. Math.*, **152** (1992), 275-290.

[7] M. Hoffman, On algebras of multiple harmonic series, *J. of Algebra*, **194** (1997), 477-495.

[8] J. G. Huard, K. S. Williams and Zhang Nan-Yue, On Tornheim's double series, *Acta Arithmetica*, **75-2** (1996), 105-117.

[9] M. Kaneko, Poly-Bernoulli numbers, *J. de Théorie des Nombres de Bordeaux*, **9** (1997), 221-228.

[10] 金子昌信, 多重ゼータ値と多重ベルヌーイ数, 都立大学数学教室セミナー報告, 1998.

[11] 金子昌信, 多重ゼータ値入門, 代数的整数論とその周辺（シンポジウム講演報告集）, 数理解析研究所講究録**1097** (1999), 50-68.

[12] T. Q. T. Le and J. Murakami, Kontsevich's integral for the Homfly polynomial and relations between values of multiple zeta functions, *Topology and its Applications*, **62** (1995), 193-206.

[13] L. Lewin, *Polylogarithms and Associated Functions*, Tata Institute, Bombey, 1980.

[14] Y. Ohno, A generalization of the duality and sum formulas on the multiple zeta values, *J. Number Theory*, **74** (1999) 39-43.

[15] Y. Ohno, On multiple harmonic series, *preprint*.

[16] 大野泰生, 多重ゼータ値の関係式について, 第５回整数論サマースクール報告集 (1997), 197-204.

[17] 大野泰生, 多重ゼータ値間の或る関係式の集合について, 第１５回代数的組合せ論シンポジウム報告集 (1998), 222-231.

[18] C. L. Siegel, *Advanced Analytic Number Theory*, Chelsea Publ. Co., New York, 1950.

[19] L. Tornheim, Harmonic double series, *Amer. J. Math.*, **72** (1950), 303-314.

[20] D. Zagier, Values of zeta functions and their applications, in ECM volume, *Progress in Math.*, **120** (1994), 497-512.

[21] D. Zagier, Multiple zeta values, *in preparation*.

Yasuo Ohno
Department of Mathematics
Graduate school of Science
Osaka University
Machikaneyama 1-1
Toyonaka, Osaka, 560-0043 Japan
e-mail: ohno@math.sci.osaka-u.ac.jp

Quasithin association scheme と置換群との関係について

平坂　貢
九大数理

平成11年10月25日

1　概要

本講演の内容はM. Muzychuk（Netanya大学）との共同研究によるもので, 可換とは限らないQuasithin association scheme（以下QASと略す）に関する結果, および置換群との関係を述べたものである。

有限集合Ωに可移に働く置換群Gは$\Omega\times\Omega$にも自然に作用する。その軌道全体のもつ代数的な性質を一般化した形で定義されているのがAssociation scheme（以下ASと略す）である。AS全体を眺めたとき, 可移な置換群から構成されるものとそうでないものとの差異は少なからずあり, この差異を明確にしたいというのが筆者の研究の基本姿勢である。ただし本講演はQASという非常に特別な条件の上での話なので, 上に挙げた基本姿勢を全うしようとする立場から見ると枝葉末節に映る議論なのは否めない。しかしながら, 与えられた構造定数による特徴付けを行うという点から筆者の基本姿勢にも殉ずるものであると思われるし, QASの構造の解明につながるものである, というのが筆者の見解である。

用語の定義については次節を参照していただくとして, 主要な結果を述べる。(X,R)をQASとする。ただしXは有限集合であり, Rは$X\times X$の分割である。任意の$x\in X$に対して, $\phi_x : X\to X$を$(y\mapsto y')$によって定義する。ただし$\{y,y'\}$はxのr-近傍(rは(x,y)を含むRの元で唯一つに定まる。)である。このとき, $N:=\langle\phi_x|x\in X\rangle\le \mathsf{Aut}(X,R):=\bigcap_{r\in R}\mathsf{Aut}(X,r)$であり, もし$2\text{-}orb(N;z^N)$, $z\in X$がthinでなければ, $(X/N,R/\!\!/N)$はthin ASになる。このことを大雑把にいうと「(X,R)の部分ASが置換群によっ

て構成されており, その商 AS も正則な置換群によって構成されている。」ということであり, (X,R) が置換群から構成されていることを言うためにはその部分 AS を如何にして Lifting up するかが課題であることを示唆している。この Lifting up は $|X|$ が二つの素数の積であるときには可能で, (X,R) が可移な置換群の 2-orbits になることが証明できる。

今後の課題としては「QAS は可移な置換群の 2-orbits である。」ことの証明に近づくこと, あるいは反例を見つけることで, さしあたっては, $|X|$ が奇数という仮定を付けて上を証明することが身近な目標である。

2 用語の定義

X を有限集合として, $r \subset X \times X$ を任意の二項関係とする。このとき, r の転置を次のように,

$$r^* := \{(x,y) | (y,x) \in r\}$$

また, $x \in X$ の r-近傍を次のように定義する。

$$x^r := \{y \in X | (x,y) \in r\}$$

定義 2.1 ([20]) X を有限集合, R を $X \times X$ の空集合を含まない分割とする。(X,R) は次の条件を満たすときアソシエーションスキームと呼ばれる：

(i) $1_X := \{(x,x) | x \in X\} \in R$;
(ii) 任意の $r \in R$ に対して, $r^* \in R$;
(iii) 任意の $d, e, f \in R$ と $x, y \in X$ に対して, $|x^d \cap y^{e^*}|$ は $(x,y) \in f$ の選び方に依らない定数である。

上の定義に出てくる $|x^d \cap y^{e^*}|$ を λ_{def} と記し, $\{\lambda_{def} | d,e,f \in R\}$ を R の構造定数と呼ぶ。任意の $r \in R$ に対して, $n_r := \lambda_{rr^* 1_X}$ と省略して書き, この数を r の次数と呼ぶ。

これ以降 (X,R) を任意の AS と仮定して話をすすめる。

F を R の部分集合とするとき, 次の記法を用いる。

$$n_F := \sum_{f \in F} n_f, \quad F^\times := F - \{1_X\}, \quad F^+ := \bigcup_{f \in F} f, F^* := \{f^* | f \in F\}.$$

任意の $x, y \in X$ に対して, r_{xy} を (x,y) を含む R の元として定義する。(R は $X \times X$ の分割なので well-defined であることに注意)

[20]で定義された記法に従い, 任意の $E, F \subseteq R$ に対して, E と F の積を次の式で定義する。

$$EF := \{f \in R | \sum_{d \in E} \sum_{e \in F} \lambda_{def} \neq 0\}, \tag{1}$$

簡便のため, E, F が一点集合のときは $\{e\}\{f\}$ を ef と省略することにする。

$F \subseteq R$ が $FF^* \subseteq F$ を満たすとき, 閉じている という。$C(R)$ を R の閉じている部分集合全体とする。任意の $E \subseteq R$ に対して, $\langle E \rangle := \bigcap_{E \subseteq F \in C(R)} F$ と定義する。

(X, R)が次の性質を満たすとき, それぞれ *thin* (*quasithin*) と呼ばれる。

$$\max_{r \in R} n_r \leq 1 \text{ (res. } \leq 2).$$

任意の $F \in C(R)$ と $x \in X$ に対して, (X, R) の (F, x) に関する部分 AS, $(X, R)_{x^F}$ を次の式で定義する：

$$(X, R)_{x^F} := (x^F, \{r_{x^F}\}_{r \in R}), \ r_{x^F} := r \cap (x^F \times x^F).$$

更に (X, R) の F による商 AS, $(X, R)^F := (X/F, R/\!\!/F)$ を次の式で定義する：

$$X/F := \{x^F | x \in X\}, R/\!\!/F := \{r^F | r \in R\} \text{ただし} r^F := \{(y^F, z^F) | z \in y^{FrF}\}.$$

実際, 部分 AS や商 AS が AS の定義をみたすことは [20] の中で証明されている。

$(X, R)^F$ の構造定数は次の式で求めることができる:

$$\lambda_{d^F e^F f^F} = \frac{1}{n_F} \sum_{b \in FdF} \sum_{c \in FeF} \lambda_{bcf}, \ \text{特に} \ n_{g^F} = \frac{n_{FgF}}{n_F}, \ n_F |X/F| = |X|. \tag{2}$$

任意の $F \in C(R)$ に対して, F の *thin radical*, *thin residue* をそれぞれ次の式で定義する。

$$\mathbf{O}_\theta(F) := \{f \in F | n_f = 1\} \text{ and } \mathbf{O}^\theta(F) := \langle \bigcup_{f \in F} f^* f \rangle.$$

Ωを有限集合として, GをΩに可移に作用する置換群とする。Gは$\Omega \times \Omega$に自然に作用して（$(x, y)^g := (x^g, y^g), x, y \in \Omega, g \in G$), その軌道全体を 2-orbits と呼び, 2-$orb(G; \Omega)$ と記す。

補題 2.2 ([20, p. 39]) $(X, R)^{\mathbf{O}^\theta(R)}$ は *thin* である。

補題 2.3 ([4, p. 56], [2, Prop. 5.1]) 任意の d, e, $f \in R$ に対して, 次が成り立つ:

(i) $n_d n_e = \sum_{f \in R} \lambda_{def} n_f$;
(ii) $\lambda_{def} n_f = \lambda_{fe^* d} n_d = \lambda_{d^* fe} n_e$;
(iii) $\lambda_{d1_X e} = \delta_{d,e}$;
(iv) $\mathsf{lcm}(n_d, n_e) \mid \lambda_{def} n_f$;
(v) $\gcd(n_d, n_e) \geq |de|$.

補題 2.4 任意の e, $f \in R$ と任意の $(x, y) \in e$ に対して,

$$ef = \{r_{xz} | z \in y^e\}$$

が成り立つ。

証明 ef の定義により, $ef \supseteq \{r_{xz} | z \in y^e\}$ は明らかである。$g \in ef$ を任意にとってくる。このとき $\lambda_{gf^* e} = \lambda_{efg} n_g / n_e > 0$ なので, $z \in y^e \cap x^g$ が存在して, $g = r_{xz}$ となり, 等号が成立する。 ∎

命題 2.5 H を $\mathsf{Aut}(R) := \bigcap_{r \in R} \mathsf{Aut}(X, r)$ の部分群として, $N := \langle H_x \rangle_{x \in X}$ と定義する。このとき, 次が成立つ。

(i) 任意の $x \in X$ に対して, $x^N \subseteq x^{\mathbf{O}^\theta(R)}$ である;
(ii) 任意の $x \in X$ と $r \in R$ に対して, H_x が x^r に可移に働くならば $X/N = X/\mathbf{O}^\theta(R)$ が成り立つ。

証明 (i) 以下のことを示せば十分である。「任意の x, $y \in X$ に対して $x^{H_y} \subset x^{\mathbf{O}^\theta(R)}$.」もし $x = y$ ならば, $x^{H_x} = x$ なので, 問題なし。今, $x \neq y$ かつ $w \in x^{H_y}$ とする。そのとき $r_{yx} = r_{yw}$ で, $\mathbf{O}^\theta(R)$ の定義により, $r_{xw} \in r^* r \subseteq \mathbf{O}^\theta(R)$ が成り立つ。ただし $r := r_{yx}$ である。

(ii) (i) から $X/N \preceq X/\mathbf{O}^\theta(R)$ である。ただし $\preceq$ は X の分割全体の refinement によって定義された半順序である。今, 任意の $(x', x'') \in \mathbf{O}^\theta(R)^+$ を考える。そのとき, 以下のような X の元の列

$$(x_1 := x', y_1, x_2, y_2, \ldots, x_k := x'')$$

が存在して

「任意の $1 \leq i \leq k-1$ に対して, $r_{x_i y_i} = r_{x_{i+1} y_i}$ を満たす。」

このとき

$$x_2 \in x_1^{H_{y_1}}, x_3 \in x_2^{H_{y_2}}, \ldots, x_k \in x_{k-1}^{H_{y_{k-1}}},$$

が成り立ち, それゆえ $x_k \in x_1^N$ である。よって, (ii)が証明できた。 ∎

3 QASの性質について

本節においては特に断らないかぎり, (X, R) を QAS としておく。

補題 3.1 任意の $x \in X$ に対して, $\phi_x : X \to X$ を次のように定義する:

$$\phi_x(y) := y' \text{ ただし } x^{r_{xy}} = \{y, y'\} \text{ である。}$$

そのとき $\phi_y \in \mathsf{Aut}(X, R)$ である。

証明 ϕ_x が well-defined であることは (X, R) が quasithin であることから導かれる。次を示せば十分である。

$$\text{「任意の } r \in R \text{ と } (u, v) \in r \text{ に対して } (\phi_y(u), \phi_y(v)) = (u', v') \in r$$

$$\text{ただし } y^{r_{yu}} = \{u, u'\},\ y^{r_{yv}} = \{v, v'\} \text{である。」}$$

簡便のため, $s := r_{yu}$, $t := r_{yv}$ としておく。$r_{uv}, r_{u'v'} \in s^*t = \{r_{uv}, r_{uv'}\}$ なので, $r_{uv} \neq r_{u'v'}$ と仮定すると, 補題 2.3(v) により $n_s = n_t = 2$ かつ $r_{u'v'} = r_{uv'}$ が成り立つ。このことは $u, u' \in y^s \cap v'^{r}_{u'v'}$ かつ $u \neq u'$ を意味するので, 補題 2.3(ii) により, $2 \leq \lambda_{sr_{u'v't}} = \lambda_{s^*tr_{u'v'}}$ となり, これから $|s^*t| = 1$ が導かれ, $r_{uv} \neq r_{u'v'}$ という仮定に矛盾する。 ∎

命題 3.2 (X, R) を *QAS* として, $H := \mathsf{Aut}(X, R)$ と定義する。このとき次が成り立つ:

(i) 任意の $x \in X$ に対して, $|H_x| \geq 2$ である;
(ii) $N := \langle H_x \rangle_{x \in X} \trianglelefteq H$ であり, $X/N = X/\mathbf{O}^\theta(R)$.

証明 (i) は補題 3.1 からの直接得られる。

(ii) N が正規部分群であることは明らか。$X/N = X/\mathbf{O}^\theta(R)$ は補題 2.5(ii) より成り立つ。 ∎

$H := \mathsf{Aut}(X, R)$, $N := \langle H_x \rangle_{x \in X}$ と定義する。「どのような状況のとき $N = \langle \phi_x | x \in X \rangle$ となるのだろうか?」について考える。もし $(X, R) = 2\text{-}orb(C_2; C_2) \wr 2\text{-}orb(C_n; C_n)$ (ただし C_2, $C_n (n > 1)$ はそれぞれ C_2, C_n の

右正則置換であり, $\wr$ は AS の wreath 積である) ならば, (X, R) は QAS であり, $N \simeq C_2^n$ かつ $\langle \phi_x | x \in X \rangle \simeq C_2$ となり, N とは一致しない。次の命題は上の問に答えるものである。なお, 証明は煩雑になるので省略する。

命題 3.3 (X, R) を QAS として, $H := \mathrm{Aut}(X, R)$, $N := \langle H_x \rangle_{x \in X}$ と定義する。もし, $n_{\mathbf{O}^\theta(R)} > 2$ ならば $N = \langle \phi_x | x \in X \rangle$ である。

次の結果は命題 3.2, 3.3 の直接の結果である。

系 3.4 もし $\mathbf{O}^\theta(R) = R$ ならば R はある可移な置換群の 2-*orbits* である。

X の位数が二つの素数の積のときは分類されていて, 分類結果のいずれも可移な置換群の 2-orbits になっている。なお, この結果は quasithin という仮定を外して, 「$\exists r \in R$ s.t. $n_r = 2$ and $\langle r \rangle = R$」という条件のもとでも得られる。

本稿で紹介しなかった文献も参考のために記しておく。なお, 本稿の内容は M. Muzychuk との共著論文で, 現在, European Journal of Combinatorics に投稿中である「Association schemes with a relation of valency two」の一部を抜粋してまとめたものである。

参考文献

[1] Z. Arad, E. Fisman, M. Muzychuk, On a Product of Two Elements in Non-commutative C-algebras, *Algebra Colloquim 5:1 (1998) 85–97.*

[2] Z. Arad, E. Fisman, M. Muzychuk, Generalized table algebras, to appear in *Israel Journal of Mathematics.*

[3] L. Babai. Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar., 29 (1977), pp. 329–336.*

[4] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, *Benjamin / Cummings, Menlo Park, CA, 1984.*

[5] E. Bannai, S.Y. Song, Character tables of fission schemes, *European J. of Combin. , 14(1993), n.5 pp. 385–396.*

[6] C.D. Godsil, On the full automorphism group of a graph, *Combinatorica 1 (1981), pp. 243–256.*

[7] R. Guralnick, Subgroups of prime order index in a simple group, *J. Algebra 81 (1983), pp. 304–311.*

[8] D.G. Higman, Coherent configurations Part I: ordinary representation theory, *Geometriae Dedicata, v. 4 (1975), pp. 1–32.*

[9] M.H. Klin, R. Pöschel. The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings. *Colloq. Math. Soc. J. Bolyai, 25. Algebraic methods in graph theory, Szeged, (1978). North-Holland, Amsterdam, (1981); pp. 405-434.*

[10] C.H. Li, On isomorphism of connected Cayley graphs. *Disc. Math., v. 178 (1998), pp. 109–122.*

[11] C.H. Li, On isomorphism of connected Cayley graphs II. *J. Combin. Theory (B) v. 74, 1998, pp. 28–34.*

[12] C.H. Li, On isomorphism of connected Cayley graphs III. *Bull. Austral. Math. Soc. v. 58 (1998), pp. 137–145.*

[13] C.H. Li, Isomorphism of finite Cayley digraphs of bounded valency, to appear.

[14] D. Marušič, Half-Transitive Group Actions on Finite Graphs of Valency 4, *J. Combin. Theory (B) v. 73, 1998, pp. 41–76.*

[15] S.A. Evdokimov, I.N. Ponomarenko, Two inequalities for the parameters of a cellular algebra, *Zapiski Nauchmykh Seminarov, POMI, v. 240, 1997*

[16] M.W.Liebeck and L.Pyber. Upper bounds for the number of conjugacy classes of a finite group. *J. of Algebra, 198(1997), no 2, pp. 538-562.*

[17] H. Wielandt, Finite Permutation Groups. *Academic Press, 1964, Berlin.*

[18] H. Wielandt, Permutation groups through invariant relations and invariant functions. *Lect. Notes., Dept. Math.m Ohio St. Univ, Colimbus, 1969.*

[19] B. Weisfeiler, On Construction and Identification of Graphs, *Springer, LNM 558.*

[20] P.H. Zieschang, An Algebraic Approach to Association Schemes, *Springer, LNM 1628.*

Four-weight spin model について

坂内悦子
九大・数理

スピンモデル (two-weight) は V.F.R. Jones [13] によって絡み目とか結び目の位相不変量を構成するために定義された. その後川越-宗政-綿谷 [16] によって必ずしも対称でない場合に拡張され, さらに坂内-坂内 [1] によって一般化され four-weight スピンモデル が定義された. ここでは始めに four-weight スピンモデルについて最近筆者が得た結果 (後述の定理 A) および four-weight スピンモデルに現われる行列に関する一つの観察を述べ, 次にいわゆる「exactly two values on W_2」を満たす four-weight スピンモデルに関する筆者と澤野光弘君 (九大・数理) の共同研究の結果 (後述の定理 B) を報告する.

まずこの報告の中で使う言葉と記号を定義しておく.

記号 X は n 個の点からなる有限集合とする. 行列およびベクトルはその行および列をこの有限集合 X で添字付けることにする. 記号 $M_{\mathbf{C}}(X)$ は X で添字付けらえた複素数体 $\mathbf{C}$ 上の行列全体の集合を表し, 記号 $\mathbf{C}^{|X|}$ は X で添字付けらえた複素数体上の縦ベクトル全体の集合とする. 記号 I は $M_{\mathbf{C}}(X)$ の単位行列を表し, 記号 J は全ての成分が 1 である様な $M_{\mathbf{C}}(X)$ の行列を表す. $x,\ y \in X$ とする時に, 行列 $M \in M_{\mathbf{C}}(X)$ に対して $M(x,y)$ は M の (x,y) 成分をあらわし, ベクトル $Y \in \mathbf{C}^{|X|}$ に対して $Y(x)$ はその x 成分を表す. $M_{\mathbf{C}}(X)$ の 2 つの行列 M と N に対して $M \circ N$ はその Hadamard 積を表す. すなわち任意の $x,\ y \in X$ に対して $(M \circ N)(x,y) = M(x,y)N(x,y)$ と定義する. $M_{\mathbf{C}}(X)$ の行列でその成分が全て 0 または 1 である様なものを $(0,1)$-行列と呼ぶ.

Four-weight スピンモデルは次のように定義される.

定義 1 W_1, W_2, W_3, W_4 を $M_{\mathbf{C}}(X)$ の行列とする. 次の条件 *(1)-(3)* が成り立つ時に $(X,\ W_1,\ W_2, W_3, W_4;\ D)$ を *four- weight* スピンモデルと言う.

(1) $W_1 \circ {}^tW_3 = J, \quad W_2 \circ {}^tW_4 = J,$

(2) $W_1W_3 = nI, \quad W_2W_4 = nI,$

(3) X に含まれる任意の元 $a,\ b$, および c に対して次の等式達が成り立つ:

$$(i) \quad \sum_{x \in X} W_2(a,x)W_2(b,x)W_4(x,c) = DW_1(b,a)W_3(a,c)W_3(c,b),$$
$$(ii) \quad \sum_{x \in X} W_2(x,a)W_2(x,b)W_4(c,x) = DW_1(a,b)W_3(c,a)W_3(b,c).$$

ただしここで D は $D^2 = |X| = n$ を満たす実数とする.

注意： Four-weight スピンモデルが $W_1 = W_2 = W_+$, $W_3 = W_4 = W_-$ を満たしていることと $(X, W_+, W_-; D)$ が川越-宗政-綿谷の意味での（two-weight）スピンモデルであることは同値である．

スピンモデル (two-weight) はその後組合せ論の研究者達によって代数的組合せ論の研究対象の中の中心的なものの一つであるアソシエーションスキームと密接に係わっていることが次第に解明され最終的には Jaeger-松本-野村 [11] により，全ての two-weight スピンモデルは自己双対的なアソシエーションスキームの Bose-Mesner 代数の中にモジュラー不変方程式の解を使って構成できることが明らかにされた．スピンモデルはその位相不変量を構成するという本来の目的を抜きにして代数的組合せ論の立場から見ても非常に興味のある対象である．two-weight スピンモデルを与えるアソシエーションスキームを全て見つけようとすると，時には有限幾何等の昔から知られている難しい問題と出合うことになったりするのである．

この報告では Jaeger-松本-野村 [11] の結果， Guo-Huang の結果などを少し紹介しながら冒頭に述べた様に定理 A, 定理 B を紹介する．

Four-weight スピンモデルの定義から 4 つの行列 W_1, W_2, W_3, W_4 は全て正則でありそれらの全ての行列要素は零でない複素数であることがわかる．この時各 a, $b \in X$ に対してベクトル $Y^{4,1}_{a,b}$ および $Y^{1,4}_{a,b}$ を

$$Y^{4,1}_{a,b}(x) = W_4(a,x)W_1(x,b), \quad Y^{1,4}_{a,b}(x) = W_1(a,x)W_4(x,b), \quad \text{for } \forall x \in X$$

で定義する．この時次の命題が成り立つ（論文 [1] の Proposition 5, Theorem 1 参照）．

命題 2 *(1)* $W_1 \circ I = \mu I$, $W_2 J = J W_2 = D\mu^{-1} J$

(2) 定義 *1* の条件 *(1)* と *(2)* を仮定すると定義 *1* の条件 *(3)* は次の条件と同値になる：
任意の $a, b \in X$ に対して

$$W_1 Y^{4,1}_{a,b} = D W_4(a,b) Y^{4,1}_{a,b},$$
$$^t W_1 Y^{1,4}_{a,b} = D W_4(a,b) Y^{1,4}_{a,b}.$$

注意： 命題 2 の条件 (2) より行列 DW_4 の各行および各列には重複度もこめて行列 W_1 の固有値が並んでいることが示される．

Jaeger-松本-野村 の理論では上記の注意に述べたこととスピンモデルに現れる行列達が次に定義する Type II 行列になっていることに着目している．

定義 3 $M_{\mathbb{C}}(X)$ に含まれる成分が全て零でない様な行列 W は次の条件を満たす時 *Type II* 行列であると言う：

$$\sum_{x \in X} \frac{W(x,a)}{W(x,b)} = n\, \delta_{a,b}$$

が任意の a, $b \in X$ に対して成り立つ．

W を $M_{\mathbb{C}}(X)$ に含まれる Type II 行列とする．W, と各 a, $b \in X$ に対してベクトル $Y_{a,b} = Y^W_{a,b} \in \mathbb{C}^{|X|}$ を

$$Y^W_{a,b}(x) = \frac{W(x,a)}{W(x,b)}, \quad x \in X$$

で定義する.

さらに W に対して集合 $N = N(W)$ を次のように定義する.

$$N = N(W) = \left\{ M \in M_{\mathbb{C}}(X) \;\middle|\; \begin{array}{l} \text{任意の } a,b \in X \text{ に対して} \\ Y_{a,b} \text{ は } M \text{ の固有ベクトルである} \end{array} \right\}$$

注意: 特に two-weight スピンモデルの場合には定義 1 において $W_+ = W_1 = W_2$, $W_- = W_3 = W_4$ となる場合に相当するので $Y_{a,b}^{4,1} = Y_{b,a}^{W_+}$, $Y_{a,b}^{1,4} = Y_{b,a}^{{}^tW_+}$ となるので 命題 2, (2) の条件より全ての a, $b \in X$ に対して $Y_{b,a}^{W_+}$ は W_+ の固有ベクトルになっている. すなわち $W_+ \in N(W_+)$ という条件を満たしていることが解る.

定義から明らかに N はベクトル部分空間であり普通の行列の積に関して閉じている (普通の行列の積に関して代数となっている) ことが解る.

次に N 上で定義される線形写像 $\Psi = \Psi_W : N \longrightarrow M_{\mathbb{C}}(X)$ を任意の $M \in N$ に対してその像となる行列 $\Psi(M) = \Psi_W(M)$ の各 (a,b)-成分 $\Psi(M)(a,b)$ が

$$MY_{a,b} = \Psi(M)(a,b)Y_{a,b} \quad a,b \in X$$

となるように定義する.

W が Type II 行列であることと ${}^tW$ が Type II 行列であることは同値であるから ${}^tW$ に対しても上記の集合および写像が定義できる. それらを次の様な記号で表す

$$\begin{aligned} N' &= N'(W) = N({}^tW), \\ Y'_{a,b} &= Y'^{W}_{a,b} = Y^{{}^tW}_{a,b}, \\ \Psi' &= \Psi'_W = \Psi_{{}^tW}. \end{aligned}$$

この様な準備のもとに次の定理が [11] において証明されている.

定理 4 *(Jaeger-松本-野村)*

(1) N および N' はそれぞれあるアソシエーションスキームの *Bose-Mesner* 代数である.

(2) $\Psi(N) \subset N'$, $\Psi'(N') \subset N$ が成り立ちさらに

$$\Psi'(\Psi(M)) = |X|^t M, \quad \Psi(\Psi'(M')) = |X|^t M'$$

を満たす (したがって $\Psi(N) = N'$, $\Psi'(N') = N$) . また Ψ と Ψ' は *Bose-Mesner* 代数の間の双対写像 (*duality*) になっている.

(3) $N = N'$ かつ $\Psi = \Psi'$ が成り立つならば $N = N'$ は自己双対的 (*self-dual*) なアソシエーションスキームの *Bose-Mesner* 代数である.

注意: 一般に Bose-Mesner 代数の間の全単射である線形写像が

$$\Psi(M_1M_2) = \Psi(M_1) \circ \Psi(M_2), \quad \Psi(M_1 \circ M_2) = \frac{1}{|X|}\Psi(M_1)\Psi(M_2)$$

を満たす時に Ψ を双対写像 (duality) という．上の定理 4 により Type II 行列があると N と N' という Bose-Mesner 代数の dual pair が定義できることがわかる．この様にして得られる Bose-Mesner 代数のことを野村-代数と呼ぶ．また定理 4 の (3) より W が対称ならば $N = N'$ は自己双対的な Bose-Mesner 代数であることも解る．

さらに [11] において次の定理が証明されている．

定理 5 *(Jaeger-松本-野村)* $W_+ \in M_C(X)$ を *Type II* 行列とし $\mathfrak{x}$ を $N(W_+)$ を *Bose-Mesner* 代数として持つアソシエーションスキームとする．この時次の *(1)* および *(2)* が成り立つ．

(1) $W_+ \in N(W_+)$ であることと $(X, W_+, W_-; D)$ がスピンモデル (*two-weight*) であることは同値である．ここで $W_- = \frac{1}{|X|} {W_+}^{-1}$, かつ D の符合は W_+ により定まる．

(2) *(1)* が成り立つならば次の *(i)-(iii)* が成り立つ．

(*i*) $\mathfrak{x}$ は自己双対的なアソシエーションスキームである．
(*ii*) $\mathfrak{x}$ は *modular* 不変性を持つ．
(*iii*) W_+ は *modular* 不変方程式の解により書きあらわされる．

注意： アソシエーションスキームの modular 不変性については [2], [3] 等を参照されたい．

定理 5 により two-weight スピンモデルを構成する問題は完全に代数的組合せ論のアソシエーションスキームの問題に置き換えることができる．Four-weight スピンモデルの場合にはそこにあらわれる行列を定理 5 の様に完全に捕らえることに成功しているとはまだ言えないが，Guo-Huang [7] ([6] も参照) は four-weight スピンモデルの 4 つの行列について Jaeger-松本-野村の方法を用いて次の様なことを証明している．

定理 6 (*Guo-Huang*)

(1) ${}^tW_2W_2 = W_2{}^tW_2$ が成り立つ．

(2) $N(W_1) = N'(W_1) = N(W_3) = N'(W_3)$ が成り立つ．

(3) $N(W_1)$ は自己双対的なアソシエーションスキームの *Bose-Mesner* 代数である．

上の (1), (2), (3) を証明するために使われた事実の中で中心的な役割を果たすのが Jaeger [10] と 出口 [5] により独立に導入された Gauge 変換の理論である．Jaeger の用いた表現を使うと，次の様な定理にまとめることができる．

定理 7 (*Odd gauge* 同値) $(X, W_1, W_2, W_3, W_4; D)$ を *four-weight* スピンモデルとする．

(1) 次の *(i)* と *(ii)* は同値である．
(i) $(X, W_1', W_2, W_3', W_4; D)$ は *four-weight* スピンモデルである．
(ii) 正則な対角行列 $\Delta \in M_C(X)$ が存在して $W_1' = \Delta^{-1}W_1\Delta$ および $W_3' = \Delta^{-1}W_3\Delta$ が成り立つ．

(2) *(1)* が成立する時 *2* つの *four-weight* スピンモデル $(X, W_1, W_2, W_3, W_4; D)$ と $(X, W_1', W_2, W_3', W_4; D)$ の与える絡み目の不変量は一致する．(この時 *2* つの *four-weight* スピンモデルは *odd gauge* 同値であると言う．)

(3) 正則な対角行列 $\Delta \in M_C(X)$ で ${}^tW_1 = \Delta^{-1}W_1\Delta$ および ${}^tW_3 = \Delta^{-1}W_3\Delta$ を満たすものが存在する.

(4) W_1' および W_3' が対称である *four-weight* スピンモデル $(X, W_1', W_2, W_3', W_4; D)$ が存在する.

定理 8 (*Even gauge* 同値) $(X, W_1, W_2, W_3, W_4; D)$ を *four-weight* スピンモデルとする.

(1) 次の *(i)* と *(ii)* は同値である.
(i) $(X, W_1, W_2', W_3, W_4'; D)$ は *four-weight* スピンモデルである.
(ii) 置換行列 P, $Q \in M_C(X)$ が存在して $W_2' = PW_2 = W_2Q$ および $W_4' = W_4\,{}^tP = {}^tQW_4$ が成り立つ.

(2) *(1)* が成立する時 *2* つの *four-weight* スピンモデル $(X, W_1, W_2, W_3, W_4; D)$ と $(X, W_1, W_2', W_3, W_4'; D)$ の与える絡み目の不変量は一致する. (この時 *2* つの *four-weight* スピンモデルは *even gauge* 同値であると言う.)

(3) 置換行列 $P \in M_C(X)$ で ${}^tW_2 = PW_2 = W_2P$ および ${}^tW_4 = {}^tPW_4 = W_4\,{}^tP$ を満たすものが存在する.

(4) 上記 *(3)* にでてくる置換行列 P に対して $P = Q^2$, $QW_2 = W_2Q$ を満たす置換行列が存在するならば W_2' および W_4' が対称である様な *four-weight* スピンモデル $(X, W_1, W_2', W_3, W_4'; D)$ が存在する.

前述の Guo-Huang の定理 6 の (2) および (3) は上記の odd gauge 同値に関する定理 7, (3) に出てくる対角行列を用いることにより証明することができる.

これまで even gauge 同値の定理 8, (3) に出てくる置換行列 P が four-weight スピンモデルのどのような性質を与えるかは定理 8, (4) 以外には知られていなかったが最近筆者はこの置換行列 P を使って次の定理を証明することができることに気がついた ([4] 参照).

定理 A $(X, W_1, W_2, W_3, W_4; D)$ を *four-weight* スピンモデルとし $N = N(W_1)$, P を定理 *8* で与えた置換行列とする. この時次の *(1)-(3)* が成り立つ.

(1) $N(W_i) = N'(W_i) = N$ *for* $i = 1, 2, 3, 4$.

(2) $N = W_2^{-1}NW_2 = {}^tPNP$.

(3) $\Psi_{W_2}(M) = \Psi_{W_1}(W_2^{-1}MW_2)$ *for* $\forall M \in N$,

$\Psi'_{W_2}(M) = {}^tP\Psi_{W_2}(M)P$ *for* $\forall M \in N$.

注意: 定理 A により four-weight スピンモデルに対して自己双対的なアソシエーションスキームが一意的に定まることが解る. またその Bose-Mesner 代数 (野村-代数) は W_2 および P によって全行列環 $M_C(X)$ の中で normalize されていることも解る.

定理 8 で与えた置換行列 P は X の元を適当に並べ替えることによって

$$P=\begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_k \end{pmatrix},\quad P_i=\begin{pmatrix} & & & 1 \\ & & \iddots & \\ & 1 & & \\ 1 & & & \end{pmatrix}\quad \text{for } i=1,\dots,k$$

の形で表すことができる．ここで は自然数で各 i, $1\le i\le k$, に対して P_i は n_i 次の置換行列であり $n_1\ge n_2\ge\cdots\ge n_k\ge 1$ とする．次に W_2 を P と同じサイズのブロックに分解して考える．すなわち

$$W_2=\begin{pmatrix} & W_{i,j} & \end{pmatrix},\quad W_{i,j} \text{ は } n_i\times n_j \text{ 行列},\ 1\le i,\ j\le k$$

と表すと ${}^tW_{i,j}=P_jW_{j,i}=W_{j,i}P_i$ が任意の i, j, $1\le i,\ j\le k$, に対して成り立つ．したがって特に

$$W_{i,i}=\sum_{l=0}^{n_i-1}a_{i,l}P_i^l,\quad i=1,2,\dots,k$$

と表わすことができる．さらに n_i が偶数ならば $a_{i,l}=a_{i,n_i-l}$ が成り立っている．また $i\neq j$ のときも $W_{i,j}$ の列ベクトル達は第一列ベクトルを巡回的に並べかえて行くことによって得られる形の行列で $W_{i,j}$ の成分に現れる互いに異なる複素数の個数は高々 (n_i,n_j) (すなわち n_i と n_j の最大公約数) 個である．

以上のように four-weight スピンモデルの場合にもある程度の情報が得られるのであるが一般には各行列 W_i は必ずしも野村-代数 $N(W_1)$ の中に入っているとは限らないし，したがって定理 8 で与えられる置換行列 P も X 上の置換として考えた時に必ずしも同じ長さの cycle の積になっているとは限らないので Jaeger-野村 [12] で定義されている two-weight スピンモデルの index に相当するものは定義できないのである．

Four-weight スピンモデルの場合に，行列 W_i, $i=1,2,3,4$, 達をどこに求めたら良いのか？ Two-weight スピンモデルにおけるアソシエーションスキームの Bose-Mesner 代数にかわる組合せ論的対象は何か？ 適当な組合せ論的対象があったとして，アソシエーションスキームの自己双対性とか modular 不変性に対応する概念があるのか？ などという疑問，問題が生じてくるのである．

これ等の問いかけに対してはっきりした答えはまだ出ていないのであるが特別な場合について Guo-Huang [8] ([6] も参照) が次のような考察を行っている．

Guo-Huang は $(X,W_1,W_2,W_3,W_4;D)$ を four-weight スピンモデルとした時に行列 W_1 が相異なる 2 つの固有値を持つ場合について考察している．この時，命題 2, (2) の条件により行列 DW_4 の各行各列には重複度もこめて W_1 の固有値が並んでいるのであるから定義 1, (1) の条件により W_2 は相異なる零でない複素数 α, β を用いて

$$W_2=\alpha A+\beta(J-A),$$

と表わすことができる．ここで A は $M_{\mathbb{C}}(X)$ に含まれる $(0,1)$-行列でありある自然数 k, $1\le k<|X|=n$, が存在して $AJ=JA=kJ$ という性質を持っている．Guo と Huang はこの様な W_2 に関する条件を exactly two values on W_2 と呼んでいる．次の定理は [8] に証明されている．

定理 9 (*Guo-Huang*) $(X, W_1, W_2, W_3, W_4; D)$ を *four-weight* スピンモデルとし W_2 が $((0,1)$ 行列 $A \in M_C(X)$ と零でない相異なる複素数 α, β を使って $W_2 = \alpha A + \beta(J - A)$ と表わされていると仮定する．この時次の条件が成り立つ：

(1) A はある *symmetric* 2-(n, k, λ) *design* $\mathcal{D}(X, \mathcal{B})$ の 結合行列 (*incidence matrix*) になっている．

(2) $B \in \mathcal{B}$ を任意に固定して $\mathcal{B}|_B = \{B \cap B' \mid B' \in \mathcal{B}\}$ とおくと 2-$(k, \lambda, \lambda - 1)$ *design* $(B, \mathcal{B}|_B)$ を定義することができるが $(B, \mathcal{B}|_B)$ はさらに *intersection number* が次に定義される s_+ または s_- であるような *quasi-symmetric design* である．

$$s_\pm = n^{-1}(k\lambda + \lambda - k \pm (k - \lambda)\sqrt{k - \lambda}),$$

(3) $k - \lambda = q^2$ を満たす自然数 q が存在する．

定理 9 の条件を満たす symmetric design の例としては symmetric difference property を持つ symmetric design が知られている．symmetric difference property は Kantor [15] によって定義された概念で任意の 3 つのブロックの symmetric difference がブロックまたはブロックの補集合のいずれかであるという性質を意味する．この様な design については [15],[14], [17] 等の研究が知られている．Kantor は symmetric difference property を持つ symmetric design のパラメーターは $k \leq \frac{n}{2}$ とすると

$$n = 4q^2, \quad k = 2q^2 - q, \quad \lambda = q^2 - q,$$

で与えられることを証明している．ここで $q = 2^{m-1}$, m は自然数である．
また Jungnickel-Tonchev は symmetric difference property を持つ symmetric design $\mathcal{D}(X, \mathcal{B})$ のパラメーターを $(4q^2, 2q^2 - q, q^2 - q)$ とする時，ひとつのブロック B に制限して得られる 2 design はパラメーターが $(2q^2 - q,\ q^2 - q,\ q^2 - q - 1)$ で intersection number が $\frac{1}{2}q^2 - q$ と $\frac{1}{2}q^2 - \frac{1}{2}q$ の quasi -symmetric design であることを証明している [14]．特に $q = 2$ の場合には $(16, 6, 2)$ design である．$(16, 6, 2)$ をパラメーターに持つ symmetric design は同型を除いて 3 種類あることが知られている．サイズが 4 の Potts モデル 2 個のテンソル積は $(16, 6, 2)$ の symmetric design を与えている．([8] 参照)．
後でまた述べるが exactly two values on W_2 である様な four-weight スピンモデルにおいては $n = 4q^2$ であることと $\alpha = -\beta$ が成り立つことは同値であることが解る．山田美枝子氏は Hadamard 行列を用いてこの様な four-weight スピンモデル例の無限シリーズを構成している ([18], [19] 参照)．$\alpha = -\beta$ を満たすこれらのスピンモデルがサイズが 4 の Potts モデルのいくつかのテンソル積と Gauge 同値になるかどうか興味のある問題である． Guo は [6] の中で symmetric difference property を持つ symmetric design が four-weight スピンモデルを与えるための必要十分条件が後述の定理 B の条件 (2) に相当すると主張しているがそれだけでは不十分であることが解った．筆者と澤野光弘 (九大・数理) は共同で Guo および Guo-Huang の論文を検証しなおして 定理 9 の逆の命題に当たる次の定理を得た．すなわち symmetric design の結合行列が four-weight スピンモデルを与えるための必要十分条件を与えた．

定理 B $A \in M_C(X)$ を 定理 *9* の条件を満たす *symmetric design* $(X, \mathcal{B})$ の結合行列とする．この時次の *(1)-(3)* が成り立つ．
(1) 次の *3* つの条件は $W_2 = \alpha A + \beta(J - A)$ をみたす *four-weight* スピンモデルが存在するための必要十分条件である．

(i) $(X,\mathcal{B})$ の点集合 X からブロックの集合 $\mathcal{B}$) への全単射 φ が存在して

$$\sharp\{B\in\mathcal{B}\mid a,b,c\in B\}=|B_a\cap B_b\cap B_c|$$

が成り立つ．ここで $\varphi(x)=B_x$, $x\in X$ とする．

(ii) $X_3=\{T\subset X\mid |T|=3\}$ とする．この時点 $p\in X$ と X_3 から $\{-1,1\}$ への写像 ε が存在して

$$\varepsilon(\{a,b,c\})=\varepsilon(\{a,b,p\})\varepsilon(\{a,c,p\})\varepsilon(\{b,c,p\})$$

が p を含まない任意の $\{a,b,c\}\in X_3$ に対して成り立つ．

(iii) 任意の $\{a,b,c\}\in X_3$ に対して

$$\sharp\{B\in\mathcal{B}\mid a,b,c\in B\}=|B_a\cap B_b\cap B_c|=s_{\varepsilon(\{a,b,c\})}$$

が成り立つ．

(2) 上の条件 *(i), (ii)* および *(iii)* が成立する時 α, β および W_1 を D および k により次の様に定義する．
α は

$$t^2-\frac{D(2k-D^2+1)}{k}t+1=0$$

の根である．

$$\beta=\frac{D-k\alpha}{D^2-k}.$$

次に $\gamma=-\frac{(\alpha-\beta)\alpha}{D\alpha\beta}$ で定義する．(γ は $\gamma^2=-\frac{1}{\alpha\beta}$ を満たすことがわかる．) このγ を使って W_1 は次のように定義する．

$$\begin{aligned}&W_1(x,x)=1,\quad for\quad \forall x\in X\\&W_1(x,p)=W_1(p,x)=\gamma,\quad for\quad \forall x\neq p\\&W_1(x,y)=W_1(y,x)=\varepsilon(\{x,y,p\})\gamma,\quad for\quad x\neq y,\ x\neq p,\ y\neq p\end{aligned}$$

この時 W_1 と W_2 は *four-weight* スピンモデルを与える．
(3) $\alpha=-\beta$ が成り立つことと $n=4q^2$ が成り立つことは同値である．またこの時 $k=2q^2-q$, $\lambda=q^2-q$ かつ q は偶数でなければならない．

注意： X の元を適当に並べかえることによって W_1 は次の様に表すことができる．

$$W_1=A_1+A_2+\gamma(A_3+A_5+A_6)-\gamma A_4$$

ここで A_1, $A_2,\ldots,$ $A_6\in M_C(X)$ は次の様な形の $(0,1)$ 行列：

$$A_1=\begin{pmatrix}1&0&\cdots&0\\0&&&\\\vdots&&0&\\0&&&\end{pmatrix},\quad A_2=\begin{pmatrix}0&0&\cdots&0\\0&1&&\\\vdots&&\ddots&\\0&&&1\end{pmatrix}$$

$$A_3 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \overline{A}_3 & \\ 0 & & & \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \overline{A}_4 & \\ 0 & & & \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{pmatrix}, \quad A_6 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & & & \\ \vdots & & 0 & \\ 1 & & & \end{pmatrix}$$

さらに, $\{I, \overline{A}_3, \overline{A}_4\}$ はクラス 2 のアソシエーションスキームを与える. $\overline{A}_3$ に対応する valency は $\frac{(n-2)q+n-2k}{2q}$ となっている. さらに $\{A_1, A_2, \ldots, A_6\}$ は coherent configuration を与える. 以下に W_2 が exactly two valued である様な four-weight スピンモデルを与える可能性のあるパラメーターをいくつか与えておく.

$\alpha = -\beta$ の場合

$$n = 16r^2,\ k = 8r^2 - 2r,\ \lambda = 4r^2 - 2r,\ s_+ = 2r^2 - r,\ s_- = 2r^2 - 2r$$

$\alpha \neq -\beta$ の場合の $n,\ k,\ \lambda,\ s_+,\ s_-$

(n, k, λ)	s_+	s_-	q
(1350, 285, 60),	15,	10,	15;
(15125, 4180, 1155),	330,	308,	55;
(332928, 48756, 7140),	1071,	1020,	204; $n = 8q^2$
(3650400, 771420, 163020),	34580,	34320,	780; $n = 6q^2$
(164497840, 9487270, 547170),	31720,	31395,	2990;
(116021808, 15394302, 2042586),	271440,	270599,	3654;
(152490250, 17185905, 1936880),	218680,	217899,	3905; $n = 10q^2$
(228826125, 63245985, 17480760),	4832916,	4830210,	6765; $n = 5q^2$
(1119980407, 193390561, 33393360),	5767944,	5764330	12649; $n = 7q^2$
(3541816125, 225641340, 14375115),	916674,	914940,	14535;
(31903181856, 534843036, 8966412),	150696,	149940,	22932

以上 $q \leq 25000$ の場合で大森俊治君
(九大・数理) の計算結果である.

$n = 5q^2$ の場合をさらにさがした
(3461452808000, 956722026040, 264431464440), 73087225640, 73086892824, 832040; $n = 5q^2$

注意： 上記のパラメーターは全て Bruck-Ryser-Chowla の条件を満たしている. (おそらく $n = 5q^2$ のものも無数に存在するであろう.)

References

[1] Ei. Bannai and Et. Bannai, *Generalized generalized spin models (four-weight spin models)*, Pacific J. of Math. 170 (1995) 1–16.

[2] Ei. Bannai, Et. Bannai and F. Jaeger, *On Spin Models, Modular Invariance, and Duality*, J. Alg. Combin. 6 (1997), 203–228.

[3] Et. Bannai, *Modular invariance property and spin models attached to cyclic group association schemes*, J. of Stasti. Plann. and Inference bf 51 (1996) 107–124.

[4] Et. Bannai, *Bose-Mesner Algebras Associated with Four-weight Spin Models*, preprint.

[5] T. Deguchi, *Generalized generalized spin models associated with exactly solvable models*, Progress in Algebraic Combinatorics, Advanced Studies in Pure Mathematics 24, Math. Soc. of Japan, (1996) 81–100.

[6] H. Guo, *On four-weight spin models*, PhD Thesis, Kyushu University, (1997).

[7] H. Guo and T. Huang, *Four-weight spin models and related Bose-Mesner algebras*, preprint.

[8] H. Guo and T. Huang, *Some Classes of Four-weight Spin Models*, preprint.

[9] F. Jaeger, Strongly regular graphs and spin models for the Kauffman polynomial, Geom. Dedicata, 44 (1992), 23–52.

[10] F. Jaeger, *On four-weight spin models and their gauge transformations*, preprint.

[11] F. Jaeger, M. Matsumoto and K. Nomura, *Bose-Mesner Algebras Related to Type II Matrices and Spin Models*, J. Alg. Combin. 8 (1998), 39–72.

[12] F. Jaeger and K. Nomura, *Symmetric versus non-symmetric spin models for link invariants*, preprint

[13] V.F.R. Jones, *On knot invariants related to some statistical mechanical models*, Pac. J. Math 137(1989), 311–334.

[14] D. Jungnickel and V.D. Tonchev, *On Symmetric and Quasi-Symmetric Designs with the Symmetric Difference Property and their Codes*, J. of Combinatorial Theory, (A) bf 59 (1992), 40–50.

[15] W.M. Kantor, *Symmetric Groups, Symmetric Designs, and Line Ovals*, J. of Algebra 33 (1975), 43–58.

[16] K. Kawagoe, A. Munemasa and Y. Watatani, *Generalized spin models*, J. of Knot Theory and its Ramifications 3, no. 4 (1994), 465–475.

[17] V.D. Tonchev, *Quasi-symmetric designs, codes, quadrics, and hyperplane sections*, Geometric Dedicata 48 (1993), 295–308.

[18] M. Yamada *The construction of four-weight spin models by using Hadamrd matrices and M-structure*, The Australasian J. of Combi. 10 (1994).237–244.

[19] M. Yamada *Hadamard matrices and spin models*, J. of Stasti. Plann. and Inference bf 51 (1996) 309–321.

Four-weight spin models of size 6, 7

Hirofumi TSUCHIYAMA
Graduate School of Mathematics
Kyushu University
10-1, Hakozaki 6-chome, Higashi-ku,
Fukuoka-shi Fukuoka 812-8581, JAPAN

Hiroshi SUZUKI
Department of Mathematics
International Christian University
10-2, Osawa 3-chome, Mitaka-shi Tokyo 181-8585, JAPAN

1 序

Spin model は、V.F.R.Jones によって、絡み目の不変量を構成するために 2 個の対称行列を用いて定義された。その後、川越、宗政、綿谷によって、対称条件がはずされた 2-weight spin model が定義され、最後に坂内英一、坂内悦子によって、4 個の行列を用いた 4-weight spin model に拡張された。Two-weight spin model から自然に four-weight spin model が構成される。しかし、本質的に four-weight の例（つまり two-weight からは得られない）は知られていない。行列のサイズが 4 以下の 4-weight spin model は H.Guo によって、また、サイズが 5 の場合には坂内悦子と澤野によって、分類されている。本稿では、サイズが 6 、7 の場合の分類を紹介します。

まず始めに、4-weight spin model の定義を見ておこう。

Definition 1.1 (Four-weight spin models)[1] Let X be a finite set with $|X| = n$, and let $W_i \in \mathrm{Mat}_X(\boldsymbol{C})$ $(i = 1, 2, 3, 4)$. Then $(X, W_1, W_2, W_3, W_4; D)$ is called a four-weight spin model if the following conditions are satisfied for all $\alpha, \beta, \gamma \in X$:

(1) $W_1[\alpha, \beta]W_3[\beta, \alpha] = W_2[\alpha, \beta]W_4[\beta, \alpha] = 1$.
(2) $\sum_{x \in X} W_1[\alpha, x]W_3[x, \beta] = \sum_{x \in X} W_2[\alpha, x]W_4[x, \beta] = n\delta_{\alpha\beta}$.
(3) $\sum_{x \in X} W_1[\alpha, x]W_1[x, \beta]W_4[\gamma, x] = DW_1[\alpha, \beta]W_4[\gamma, \beta]W_4[\gamma, \alpha]$,
$\sum_{x \in X} W_1[x, \alpha]W_1[\beta, x]W_4[x, \gamma] = DW_1[\beta, \alpha]W_4[\beta, \gamma]W_4[\alpha, \gamma]$,

where D is a complex number satisfying $D^2 = |X|$.

F.Jaegerは、four-weight spin modelに次の同値関係を定義した。

Definition 1.2 [5] Let $(X, W_1, W_2, W_3, W_4; D)$ and $(X, W_1', W_2', W_3', W_4'; D)$ be 4-weight spin model. Then $(X, W_1', W_2', W_3', W_4'; D)$ is said to gauge equivalent to $(X, W_1, W_2, W_3, W_4; D)$, when $(X, W_1', W_2', W_3', W_4'; D)$ is expressed as $(X, \lambda\Delta W_1\Delta^{-1}, \lambda^{-1}SW_2, \lambda^{-1}\Delta W_3\Delta^{-1}, \lambda W_4\,{}^tS; D)$, with an invertible diagonal matrix Δ, a permutation matrix S and a nonzero scalar λ.

Gauge 同値な spin modelから構成される不変量は同値であることが知られている。この関係で分類することが、我々の目的である。

ここで、spin modelを研究する上で重要な概念であるtype II 行列を定義しよう。

Definition 1.3 Let W be a matrix in $\mathrm{Mat}_X(C)$ whose entries are all nonzero. We associate a matrix W^- in $\mathrm{Mat}_X(C)$ defined by the following.

$$W^-[x, y] = \frac{1}{W[y, x]}.$$

W is said to be a type II matrix if $WW^- = nI$, where $n = |X|$.

Type II 行列の概念は、spin model の研究から生まれたものである。実際、Defnition 1.1 (1), (2) から、four-weight spin modelにあらわれる行列がすべてtypt II 行列 であることはすぐにわかる。(詳細は、[4]、[6]、[10]を参照。) Typt II行列 にも次の同値関係が定義されています。

Definition 1.4 Let W and W' be type II matrices. Then W' is said to type II equivalent to W, when W' is expressed as $S\Delta W\Delta' S'$, with an invertible diagonal matrix Δ, a permutation matrix S.

次にあげるのは、four-weight spin model と typt II 行列の基本的な例です。

Example 1.1 (1) Let η be a primitive n-th or $2n$-th root of unity when n is odd or even respectively, and let $\xi = \sum_{i=1}^{n} \eta^{i^2}$. Then $(X, W_1, W_2, W_1^-, W_2^-; D)$ becomes a four-weight spin model, where

$$W_1[i, j] = \eta^{(i-j)^2},\ W_2 = \frac{D}{\xi} W_1.$$

It is called a cyclic model, and W_1 is called a cyclic type II matrix.

(2) Let α be a root of $t^2 + nt + n = 0$. Then $(W_1, W_2, W_1^-, W_2^-; D)$ becomes a four-weight spin model, where

$$W_1[i, j] = \begin{cases} \alpha + 1 & \text{if } i = j \\ 1 & \text{otherwise} \end{cases},\ W_2 = \frac{D}{\alpha} W_1.$$

It is called a Potts model, and W_1 is called a Potts type II matrix.

$W_4[x,y]$がちょうど2値をとるとき、H.Guoは次を示している。

Proposition 1.5 [4, Theorem 5.5] Let $(X, W_1, W_2, W_3, W_4; D)$ be a four-weight spin model with $W_4 = \eta B + \xi(J-B)$ for some (0,1)-matrix B and let $BJ = JB = kJ$, then there exists a positive integer λ such that B is the incidence matrix of a symmetric design (n, k, λ) with the properties:

(1) $k-\lambda$ is a square,

(2) its derived design with respect to any block is a quasi-symmetric design with intersection numbers

$$\begin{aligned} x &= n^{-1}(k\lambda+\lambda-k-(k-\lambda)\sqrt{k-\lambda}), \\ y &= n^{-1}(k\lambda+\lambda-k+(k-\lambda)\sqrt{k-\lambda}). \end{aligned}$$

次にあげる坂内悦子と澤野の結果は本稿の主結果の証明に本質的である。

Proposition 1.6 [3] Let $(X, W_1, W_2, W_3, W_4; D)$ be a four-weight spin model.

1. If one of the four type II matrices W_1, W_2, W_3, W_4 is type II equivalent to a Potts type II matrix, then $(X, W_1, W_2, W_3, W_4; D)$ is gauge equivalent to a Potts model.
2. If one of the four type II matrices W_1, W_2, W_3, W_4 is type II equivalent to a cyclic type II matrix, then $(X, W_1, W_2, W_3, W_4; D)$ is gauge equivalent to a cyclic model.

2 Cyclic model と Potts modelについて

Type II 行列 $W \in \mathrm{Mat}_X(C)$ と $x, y \in X$ に対して、列ベクトル $\boldsymbol{u}^W_{x,y}$ を次で定義する。

$$\boldsymbol{u}^W_{x,y}[z] = \frac{W[z,x]}{W[z,y]}.$$

そして、type II 行列 $W \in \mathrm{Mat}_X(C)$ に対して、$\mathcal{N}(W)$ を

$$\mathcal{N}(W) = \{M \in \mathrm{Mat}_X(C) \mid \boldsymbol{u}^W_{x,y} \text{ is an eigenvector for } M \text{ for all } x, y \in X\}.$$

と定義すると、可換association schemeのBose-Mesner代数になることが知られてい、野村代数と呼ばれている。(詳しくは[6, 10]参照。) まず、次にあげる二つの補題が証明できる。

Lemma 2.1 Let W be a type II matrix in $\mathrm{Mat}_X(C)$ with $|X| = n$, and $E_0 = (1/|X|)J, E_1, \cdots, E_d$ be orthogonal idempotents of $\mathcal{N}(W)$ expressing I as a sum, i.e.,

$$E_iE_j = \delta_{i,j}E_i, \text{ for } 0 \le i, j \le d, \text{ and } I = E_0 + E_1 + \cdots + E_d.$$

Let $m_i = \mathrm{rank}E_i$. Then W is type II equivalent to a matrix $U = [U_0, U_1, \ldots, U_d]$ satisfying the following conditions.

(1) Each U_i is of size $n \times m_i$, whose entries in the first row are all 1, all entries are nonzero, and $U_0 = j$, the all 1 vector.

(2) Let $U_i = [u_1^{(i)}, u_2^{(i)}, \ldots, u_{m_i}^{(i)}]$. Then $\mathrm{Span}(u_1^{(i)}, u_2^{(i)}, \ldots, u_{m_i}^{(i)})$ is equal to the column space of E_i. In particular, they are linearly independent.

(3) $\mathcal{N}(W) = \mathcal{N}(U)$.

Lemma 2.2 Let $W = [w_1, w_2 \cdots, w_n]$ be a type II matrix in $\mathrm{Mat}_X(C)$ with $n = |X|$. Let $\mathcal{M} \subset \mathcal{N}(W)$ be a Bose-Mesner algebra of a commutative association scheme. Let $A_0, A_1, \cdots, A_d$ be the adjacency matrices, let $E_0, E_1, \cdots, E_d$ be the primitive idempotents. Suppose $w_1 = j$ and $w_{i_1}, \cdots, w_{i_m}$, with $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ span the column space of E_i. Then

$$\sum_{h=1}^{m} \frac{W[k, i_h]}{W[j, i_h]} = nE_i[k, j]$$

for every $1 \leq j, k \leq n$.

先の二つの補題を使うと、野村代数が symmetrization of a regular group sckeme of Z_n の Bose-Mesner 代数を含むような type II 行列が決定できる。この時には、cyclic type II 行列 と type II 同値になることがわかる。

Proposition 2.3 Let W be a type II matrix of size $n \geq 5$ or $n = 3$. Let A be a matrix with $A[i, j] = \delta_{i+1,j}$, where indices are considered as elements of Z_n, and let $\tilde{A} = A + A^{n-1}$. If $\tilde{A}$ is in $\mathcal{N}(W)$, there exist diagonal matrices Δ and Δ' and a permutation matrix S such that $\Delta W \Delta' S$ is a cyclic type II matrix.

Proposition 1.6 と Proposition 2.3 とから、次の定理が導かれる。

Theorem 2.1 *Let $(X, W_1, W_2, W_3, W_4; D)$ be a four-weight spin model. Suppose that the Nomura algebra $\mathcal{N}(W_1)$ contains a Bose-Mesner algebra of the symmetrization of a regular group scheme of a cyclic group. Then $(X, W_1, W_2, W_3, W_4; D)$ is gauge equivalent to a cyclic model.*

また、type II 行列 W が $W\,{}^tW \in \mathrm{Span}(I, J)$ を満たしているときは、ある条件（サイズが 6、7 の spin model を構成する type II 行列なら満たしている）のもとで決定でき、この場合には、Potts type II matrix に type II 同値になることが分かる。

Proposition 2.4 Let $W \in \mathrm{Mat}_X(C)$ with $n = |X| \geq 2$. Suppose the following.

(1) $WW^- = nI$, i.e., W is a type II matrix.

(2) $WJ = \alpha J$ for some $\alpha \in C$.

(3) $W\,{}^tW = \beta I + \gamma J$.

Then $W[x,y]$ takes exactly two values. Moreover, if $W = \eta B + \xi(J - B)$ for some $(0,1)$ matrix B, then $B^tB \in \mathrm{Span}(I,J)$ and B becomes the incidence matrix of a symmetric design of size n. In particular if $BJ = kJ$, then $k(k-1)/(n-1)$ is a rational integer. If $k = 1$ or $n-1$, then there is a permutation matrix S and a scalar $\mu \in \boldsymbol{C}$ such that $WS = \mu(\alpha I + J)$, where α is a root of $t^2 + nt + n = 0$.

Proposition 1.6 と Proposition 2.4 とから、次の定理が導かれる。

Theorem 2.2 *Let $(X, W_1, W_2, W_3, W_4; D)$ be a four-weight spin model. If $W_4{}^tW_4$ is a linear combination of I and J, then one of the following holds.*

(i) $(X, W_1, W_2, W_3, W_4; D)$ is gauge equivalent to a Potts model; or

(ii) There is a $(0,1)$ matrix B such that $W_4 = \eta B + \xi(J - B)$, and the conclusion of Proposition 1.5 holds. In particular there are rational integers k, λ such that $2 \leq k \leq n-2$, $B\,{}^tB = (k-\lambda)I + \lambda J$, $k(k-1)/(n-1)$ and $\sqrt{k-\lambda}$ are integers.

3 サイズ6、7のFour-weight spin modelについて

Four-weight spin model を構成する type II 行列の野村代数は自己双対的可換 association scheme になることが知られている。([4]、[6]参照。) サイズ6、7の association scheme の分類は知られており、自己双対的可換 association scheme は、以下の通りである。([9]参照。)

- size 6
  - $AS(6c1 : \boldsymbol{Z}_6)$
  - $AS(6s5 : 6c1(0, 1+5, 2+4, 3))$
  - $AS(6s8 : 6c1(0, 1+2+3+4+5))$
- size 7
  - $AS(7c1 : \boldsymbol{Z}_7)$
  - $AS(7s2 : 7c1(0, 1+6, 2+5, 3+4))$
  - $AS(7c3 : 7c1(0, 1+2+4, 3+5+6))$
  - $AS(7s4 : 7c1(0, 1+2+3+4+5+6))$

$(X, W_1, W_2, W_3, W_4; D)$ を four-weihgt spin model とする。$\mathcal{N}(W_1)$ が $AS(6c1 : \boldsymbol{Z}_6)$、$AS(6s5 : 6c1(0, 1+5, 2+4, 3))$、$AS(7c1 : \boldsymbol{Z}_7)$、$AS(7c2 : 7c1(0, 1+6, 2+5, 3+4))$ の Bose-Mesner 代数のときは Theorem 2.1、$AS(6s8 : 6c1(0, 1+2+3+4+5))$、$AS(7c3 : 7c1(0, 1+2+4, 3+5+6))$、$AS(7c4 : 7c1(0, 1+2+3+4+5+6))$ の時は、Theorem 2.2 の条件を満たしているので、我々は次の定理を得る。

Theorem 3.1 *Every four-weight spin model of size six and seven is gauge equivalent to either a cyclic model or a Potts model.*

参考文献

[1] E. Bannai and E. Bannai, Generalized generalized spin models (four-weight spin models), Pacific J. Math. 170 (1995), 1–16.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin-Cummings, California, 1984.

[3] E. Bannai and M. Sawano, The classification of certain four-weight spin models, preprint.

[4] H. Guo, On four-weight spin models, Ph. D. Thesis, Kyushu University, (1997).

[5] F. Jaeger, On four-weight spin models and their gauge transformation, preprint.

[6] F. Jaeger, M. Matsumoto and K. Nomura, Bose-Mesner algebras related to type II matrices and spin models, J. Alg. Combin. 8 (1998), 39–72.

[7] V. F. R. Jones, On knot invariants related to some statistical mechanical models, Pacific Journal of Mathematics 137 (1989), 311–334.

[8] K. Kawagoe, A. Munemasa and Y. Watatani, Generalized spin models, J. Knot Theory and Its Ramification 3 (1994), 465–476.

[9] E. Nomiyama, Classification of association schemes with at most ten vertices, Kyushu J. Math. 49 (1995), 163–195.

[10] K. Nomura, An algebra associated with a spin model, J. Alg. Combin. 6 (1997), 53–58.

[11] K. Nomura, Type II matrices of size five, Graphs and Combinatorics. 15 (1999), 79-92.

単純群のシロー 2 部分群

原田耕一郎
オハイオ州立大学
ラング（M.L.Lang）による報告付記

1. 問題提起

(N). 殆ど不可能：単純群のシロー 2 部分群になりうる 2 群をすべて分類すること（単純群の分類を使わずに）.
(P). 可能：単純群のシロー 2 部分群になっている 2 群をすべて記述すること.
(E). 容易：シロー 2 部分群の位数が高々 2^{46} になっている単純群をすべて決めること（ラングによる報告参照）. 2^{46} は単純群モンスターのシロー 2 部分群の位数である.
(P-46). 単純群のシロー 2 部分群になっている 2 群で位数が高々 2^{46} であるものをすべて記述すること（ラングによって進行中）.
(C). 単純群のシロー 2 部分群になっている 2 群を（2 群の内部的性質のみから）特徴づけること.
(S). 散在型単純群シロー 2 部分群とそのほかの単純群のシロー 2 部分群の質的違いを見出すこと.

2. 実現可能な 2-群

G を単純群とする（本稿では非可換な単純群しか考えない）. $2||G|$ がファイト・トンプソンの定理から従う. さらに
$|L_2(5)| = 2^2 \cdot 3 \cdot 5 = 60$,
$|L_2(7)| = 2^3 \cdot 3 \cdot 7 = 168$,
$|Sz(8)| = 2^6 \cdot 5 \cdot 7 \cdot 13 = 29120$.
であるから 2 がすべての単純群の位数を割り切る唯一の素数であることがわかる.

高々 2^9 の位数の 2 群の同型類の個数（2^6 までは Hall-Senior, 2^7 は James-Newman-O'Brien, 2^8 は O'Brien, 2^9 は Eick-O'Brien による:）:

2^n	2	4	8	16	32	64	128	256	512
number	1	2	5	14	51	267	2328	56092	10494213
realizable	0	1	2	3	4	8	7	?	?
odd auto	0	1	2	5	15	56	261	?	?

注 (G.Higman-C.Sims). 位数 p^n の p 群の個数はぜんきん的に次の式に等しい.

$$p^{a(n,p)n^3}, \quad a(n,p) = \frac{2}{27} + O(\sqrt[3]{n}).$$

定義. 2 群 S はそれに同型な群をシロー部分群として持つ非可換単純群 G が存在するとき**実現可能** (G に対して実現可能) という.

注. 上の表の一番下の数は自明でない奇数位数の自己同型を持つ 2 群の数をあらわす.

定義. 2群 S が有限群 G のシロー 2 群に同型のとき S を G 型という.

G を有限群とし, P をそのシロー p 部分群とする. P をその共役類の直和集合として次のようにあらわす.

$$P = C_0 \cup C_1 \cdots \cup C_k.$$

これら P の共役類のいくつかは G の中で共役となり,「融合する」といわれる. これは次のようにあらわされる.

$$P = C_0' \cup C_1' \cdots \cup C_{k'}'.$$

定義によって各々の C_i' はいくつかの C_j の和集合であり, すべての C_i' の元は G の中ですべて共役である. $C_0 = C_0' = 1$ となるように記号を選ぶとする.

今後 $p = 2$ の時には P のかわりに S と書く.

定義 A. S を 2 群とし, $\mathcal{D}(S) = \mathcal{D}$ を S の $C_S(D) \subset D$ (自己中心的) となる部分群 D で, しかも $N_S(D)$ をシロー 2 群として持ち $O_{2'}(\tilde{D}) = 1, D = O_2(\tilde{D})$ となっている有限群 $\tilde{D}$ が存在して, さらに次の条件 (I) または (II) の一方を満足するもの全体の集合とせよ (そのような D を許容可能 (admissible) と呼ぶ. また集合 $\{(D, \tilde{D}), D \in \mathcal{D}\}$ を許容族, その部分集合を許容部分族という.)

(I). $N_S(D)/D$ は巡回群または一般 4 元数群である.

または,

(II). 剰余群 $\tilde{D}/D$ は奇数指数の正規部分群 L/D で $L_2(2^n), Sz(2^{2n-1})$ または $U_3(2^n), n \geq 2$ のどれかに同型になるものを含む.

注. $\mathrm{Aut}(S)$ が 2 群でないとき $S \in \mathcal{D}$ とする. $\tilde{S}$ としては S の自明でない奇数位数の自己同型による拡大を使う. admissible な部分群 D に対して一般には複数の $\tilde{D}$ の可能性がある.

定理 A. 2 群 S が実現可能のときには次の条件が成立する.

(i). S は初等可換群でなければ直既約である.

(ii). C_i, $i = 1, \ldots, k$ を S の共役類とする. そのとき適当な許容部分族 $\mathcal{A}$ が存在して C_i', $i = 1, \ldots, k'$ を S のすべての $(D, \tilde{D}) \in \mathcal{A}$ に属する $\tilde{D}$ から生ずる融合であるとき以下の条件 (a),(b),(c) が成立する.

(a). すべての $i = 0, 1, 2, \ldots, k'$ に対して $|C_i'| > 1$,

(b). $S = \langle xy^{-1}, x, y \in C_i', i = 1, 2, \ldots, k' \rangle$,
(c). x_i を C_i' の元で $|C_S(x_i)|$ がすべての $y \in C_i'$ の元の中で極大になっているとするとき, $C_S(y)$ は $C_S(x_i)$ の部分群に同型でその同型写像は S の元の融合と compatible である.

注. 定理 A の (i) を示すためには単純群の分類が必要である. ゴレンシュタインと私は二つの 2 面体群の直積は実現可能ではないことを証明した (Annals of Math.,1972). しかし直既約分解できるシロー 2 部分群を持つ群に関する一般的な定理は存在しない. 定理 A の (ii) は分類以前の結果だけで証明可能である

注. A_8 型のシロー 2 部分群をもついかなる単純群 G に対しても許容族 $\{(D, \tilde{D}) | D \in \mathcal{D}(S)\}$ のある元 $(D, \tilde{D})$ が存在して $N_G(D)$ が $N_S(D)$ に等しくなっている. ゆえに A_8 においては $\tilde{D}$ として許される構造を持っていない.

定義. 有限群 G のシロー p 部分群 P の融合は $k' = k$ (すなわち $C_i' = C_i$ がすべての i について成立) となっているとき自明であるという.

定理 (Grün). 有限群 G のシロー p 部分群 P が自明な融合を持つならば G は p ベキ零である. 特に ($P \neq 1$ ならば) G は単純ではない.

ゆえに, G が非可換単純ならば P の融合は自明ではない.

定理 (Alperin-Goldschmidt). 有限群 G の部分群の集合 $\{N_G(D), D \in \mathcal{D}(S)\}$ はシロー 2 部分群の融合を統制する. すなわち, $x, y \in S$, $g \in G$ で $g^{-1}xg = y$ であれば, 元 $g' = x_1 x_2 \cdots x_n$ が存在して $g'^{-1}xg' = y$, $x_i \in N_G(D_i), D_i \in \mathcal{D}$ が成立している. .

定理 A の (ii)(c) で述べた元 x_i は *extremal* な元とよばれているものに対応している. その意味は S が群 G のシロー 2 群であるとき $C_S(x_i)$ は $C_G(x_i)$ のシロー 2 部分群になる.

次の重要な結果が定理 A の中に組み入れられている.

定理 (Glauberman's Z^* 定理). G を有限で非可換な単純群とする. このときシロー 2 群 S のすべての位数 2 の元 t にたいして $s \in S \backslash t$ が存在して t は G の中で s に共役となっている.

定理 (Thompson の移送定理). G を有限群, S をそのシロー 2 部分群, T を S の極大部分群とせよ. このとき G が指数 2 の部分群を含まないならば, $S \backslash T$ のすべての位数 2 の元 t は G の中で T のある元 s と共役になる.

定理 (Grün). P を群 G のシロー p 部分群とするとき そのフォーカル部分群 $P \cap G'$ は xy^{-1} と書ける元で生成される. ここで $x, y \in P$ で x は G の中で y に共役である.

3. 位数の小さい実現可能な 2 群 (定理 A の逆は真か ?)

定理 A の条件は融合単純群 (fusion-simple)(すなわち $Z(G/O_{2'}(G)) = 1, G = O^2(G)$) と（通常の）単純群を区別することが出来ない．だから，$G = A_5 \wr A_5$ のような群のシロー 2 部分群が定理 A の逆の反例を与えるかも知れない．実現可能な 2 群 S にたいする，定理 A の許容部分族 $\mathcal{A}$ はもちろん空集合ではない．なぜならば，もしそうなら，対応する群は正規 2 補群をもつことになってしまう．一方，実現可能な群で許容部分族 $\mathcal{A}$ が全許容族の真部分集合になっている例も存在する．それゆえ重要な課題は考えている群 G が単純群（融合単純というだけでなく）になるためには許容部分族 $\mathcal{A}$ はどの程度「豊富」でないといけないかを見つけることである．きちんと定義できる「豊富」な許容部分族 $\mathcal{A}$ が存在すると信じられる．

30 年ほど前私はホール・シニアーの 2 群の表を使い位数高々 2^6 の群で実現可能なものをすべてきめることができた．(その当時としては直既約分解可能なものも候補者として含める必要があったが．) いろいろな分類定理がつかえる今日では単純群の分類を使わなくても，ある程度の労力で高々位数 2^7 の実現可能な 2 群をすべてきめることはできるであろう．

高々位数 2^7 の実現可能な 2 群

4 ： 初等可換群．

8 ： 初等可換群，2 面体群．

16：初等可換群，2 面体群，半 2 面体群．

32：初等可換群，2 面体群，半 2 面体群，環積 $Z_4 \wr Z_2$．

64：初等可換群，2 面体群，半 2 面体群，または $Sz(8), U_3(4), L_4(2), L_3(4), G_2(3)$ のシロー 2 群．

128：初等可換群，2 面体群，半 2 面体群，環積 $Z_8 \wr Z_2$，または $L_4(3), U_4(3), Janko_2$ のシロー 2 群．

定理 A の逆の証明を高々位数 2^7 の 2 群に対して証明しようとすれば，上にあげた 2 群以外には定理 A の条件 (i)(ii) を満たすものがないことをいう必要がある．しかしなかなか面倒なので，非常に小さい群を除いて，ここではそれを試みない．

定理． 2 群 S の許容部分族 $\mathcal{D}(S)$ が位数 4 の部分群を含んでいるときは S は 2 面体群か半 2 面体群である．

$\mathcal{D}(S)$ が位数 4 の元 D を含んでいるとすると D は初等可換群の E_4 であるから次の補題をつかえばよい．

補題. 2 群 S が自己中心的な初等可換群 E_4 を含んでいれば S は 2 面体群または半 2 面体群である.

定理. S を実現可能な 2 群とし, 集合 $\mathcal{D}(S)$ が位数 8 の元 D を含んでいるとすれば S は初等可換群または半 2 面体群である.

$D \cong Q_8$ または $Z_2 \times Z_2 \times Z_2$ となる. 個々の場合に調べればよい. 次の補題も使える.

補題. 2 群 S が正規な E_4 をもっていないとせよ. このとき S は巡回群, 一般 4 元数群, 2 面体群 (位数 8 以上), または半 2 面体群である.

これらの結果により $\mathcal{D}(S)$ が位数 4 または 8 の元を含んでいるときは簡単である. $|D| = 16$ になると面倒である. 次の補題は証明が容易だからあげておく.

補題. S を位数 16 の非可換群で奇数位数の自明でない自己同型をもつとせよ. このとき S は $Q_8, Z_2 \times Q_8$ または $Z_4 * Q_8$ に同型である.

この結果を使えば

定理. 定理 A の逆は位数 32 以下の 2 群に対しては成立する.

が (手計算で) 証明できる.

位数 64 の群に関しては第 2 の可能性 (II) を考える必要がある. このときは $D \cong E_{16}$ である. さて $D \cong E_{16}$ とせよ. このとき $L_2(4)$ は D の上に忠実に作用する. 実はその作用は 2 通りある. $\tilde{D}/D \cong L_2(4)$ とすれば, どちらの作用の場合でも $\tilde{D}$ は D の分離拡大となる. $\tilde{D}$ のシロー 2 群は $L_2(4)$ が $D\backslash 1$ に可移に作用すれば $L_3(4)$ 型であり, そうでないときは $L_4(2)$ 型である. それゆえ S の構造はただちにきまってしまう.

$G = L_3(4)$ においては, $N_G(D)/D$ は E_{16} の $L_2(4)$ による拡大である. 一方, S が $L_4(2) \cong A_8$ 型ならば, S は $PSp_4(3)$ 型でもある. $G = A_8$ においては, $N_G(D)/D$ は $S_3 \times S_3$ に同型であり, $G = PSp_4(3)$ においては, $N_G(D)/D$ は E_{16} の $L_2(4)$ による拡大となっている. ゆえに $G = A_8$ においては $D \cong E_{16}$ は実際には許容部分族に属していない. 同じような興味ある例が $D \cong E_{16}$ のとき $Janko_2$ と $Janko_3$ で生じている.

このようにして定義 A の可能性 (II) をかんがえなければいけない場合は簡単に S の構造がわかるが (I) だけが生ずる場合は面倒である. そもそも定理 A の逆は計算器を使うことを念頭にいれてあるのでこれ以上の「悪あがき」はしないことにする. しかし多少の労力を惜しまなければつぎの定理は手計算でできるだろう.

定理 ?. S を実現可能な 2 群で位数 16 の許容部分群をもっているときは S のセクション階数 (sectional rank) は 4 以下である.

定理．S を実現可能な非可換 2 群で位数が高々2^7 ならば S のセクション階数は 4 以下である．

後書き．本稿はモントリオールで開かれたモンスターワークショップ (1999 年 5 月 29 日-6 月 4 日) の報告集へ投稿する論文を短くして翻訳したものである．ここではラングの報告を付記としたが実際にはすべてを合わせて共著として提出する．

A preliminary report on simple groups whose Sylow 2-subgroups are of order at most 2^{46} by Mong Lung Lang

We list all the finite simple groups G such that $\mathrm{ord}_2(G)$ is less than or equal to 2^{46}. The report is organized as follow :

A1. Orders of Sylow 2-subgroups of the sporadic simple groups

A2. Orders of Sylow 2-subgroups of simple groups of Lie type

A3. Simple groups G of Lie type (odd characteristic) such that $\mathrm{ord}_2(G) = m$.

A4. Simple groups G of Lie type such that $\mathrm{ord}_2(G) = m$, $m \leq 46$.

A5. Simple groups G such that $\mathrm{ord}_2(G) = m$, $m \leq 46$.

A1. Orders of Sylow 2-subgroups of the sporadic simple groups

The orders of Sylow 2-subgroups of sporadic simple groups are

2^3	$Janko_1$
2^4	$Mathieu_1$
2^6	$Mathieu_2$
2^7	$Janko_2$, $Janko_3$, $Mathieu_3$, $Mathieu_4$, $McLaughlin$
2^8	$Lyons$
2^9	$Higman\text{-}Sims$, $O'Nan$
2^{10}	$Conway_3$, $Held$, $Mathieu_5$
2^{13}	$Suzuki$
2^{14}	$Harada$, $Rudvalis$
2^{15}	$Thompson$
2^{17}	$Fischer_1$
2^{18}	$Conway_2$, $Fischer_2$
2^{21}	$Conway_1$, $Fischer_3$, $Janko_4$
2^{41}	$Fischer_4$
2^{46}	$Monster$

A2. Orders of Sylow 2-subgroups of simple groups of Lie type

Let $n = 2^e(2m+1)$, where $e, m \in \mathbb{N} \cup \{0\}$. Define $\mathrm{ord}_2(n) = e$. The order of a Sylow 2-subgroup of a finite simple group of Lie type is given in the following table.

G	$\mathrm{ord}_2(G)$, q is odd.	$q = 2^m$
$A_n(q)$	$[\frac{n}{2}]\mathrm{ord}_2(q-1) + [\frac{n+1}{2}]\mathrm{ord}_2(q^2-1) + \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}] - \mathrm{ord}_2((n+1, q-1))$	$(n+1)nm/2$
${}^2A_n(q)$	$[\frac{n}{2}]\mathrm{ord}_2(q+1) + [\frac{n+1}{2}]\mathrm{ord}_2(q^2-1) + \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}] - \mathrm{ord}_2((n+1, q+1))$	$(n+1)nm/2$
$B_n(q)$	$n \cdot \mathrm{ord}_2(q^2-1) + \sum_{k=1}^{\infty}[\frac{2n}{2^{k+1}}] - 1$	n^2m
$C_n(q)$	$n \cdot \mathrm{ord}_2(q^2-1) + \sum_{k=1}^{\infty}[\frac{2n}{2^{k+1}}] - 1$	n^2m
$D_n(q)$	$(n-1)\,\mathrm{ord}_2(q^2-1) + \sum_{k=1}^{\infty}[\frac{2n-2}{2^{k+1}}] + \mathrm{ord}_2(q^n-1) - \mathrm{ord}_2((4, q^n-1))$	$n(n-1)m$
${}^2D_n(q)$	$(n-1) \cdot \mathrm{ord}_2(q^2-1) + \sum_{k=1}^{\infty}[\frac{2n-2}{2^{k+1}}] + \mathrm{ord}_2(q^n+1) - \mathrm{ord}_2((4, q^n+1))$	$n(n-1)m$
$E_6(q)$	$3 + 4 \cdot \mathrm{ord}_2(q^2-1) + 2 \cdot \mathrm{ord}_2(q-1)$	$36m$
$E_7(q)$	$7 \cdot \mathrm{ord}_2(q^2-1) + 2$	$63m$
$E_8(q)$	$8 \cdot \mathrm{ord}_2(q^2-1) + 6$	$120m$
$F_4(q)$	$4 \cdot \mathrm{ord}_2(q^2-1) + 3$	$24m$
$G_2(q)$	$2 \cdot \mathrm{ord}_2(q^2-1)$	$6m$
${}^3D_4(q)$	$2 \cdot \mathrm{ord}_2(q^2-1)$	$12m$
${}^2E_6(q)$	$4 \cdot \mathrm{ord}_2(q^2-1) + 2 \cdot \mathrm{ord}_2(q+1) + 3$	$36m$
${}^2G_2(3^{2n+1})$	3	*
${}^2B_2(2^{2n+1})$	*	$2(2n+1)$
${}^2F_4(2^{2n+1})$	*	$12(2n+1)$

A3. Simple groups G of Lie type (odd characteristic) such that $\mathrm{ord}_2(G) = m$

For each $m \in \mathbb{N}$, we determine in this section all the groups G of Lie type (odd characteristic) such that $\mathrm{ord}_2(G) = m$, where $1 \le m \le 46$.

A3.1. $L_n(q)$. $A_n(q) = L_{n+1}(q)$. The following lemmas gives the necessary and sufficient conditions on n and q such that the order of a Sylow 2-subgroup of $L_n(q)$ is 2^m.

Lemma 1. *Suppose that $n+1$ is odd and that q is a power of an odd prime. Then $\mathrm{ord}_2(L_{n+1}(q)) = m$ if and only if $e \ge 4$ is an integer and*

(i) $q \equiv 2^{e-2} - 1 \pmod{2^{e-1}}$, *or*
(ii) $q \equiv 2^{(e-1)/2} + 1 \pmod{2^{(e+1)/2}}$,

where

$$e = 2(m - \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}])/n\,.$$

Lemma 2. *Let $n+1$ be even. Suppose that $q \equiv 3 \pmod 4$. Then $\mathrm{ord}_2(L_{n+1}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} - 1 \pmod{2^e}$, where*

$$e = 2(m - [\frac{n}{2}] - \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}] + 1)/(n+1).$$

In the case $q \equiv 1 \pmod 4$, we have the following result.

Lemma 3. *Suppose that $2^{r_0} || n+1$ and $q \equiv 2^{r_1} + 1 \pmod{2^{r_1+1}}$, where $r_1 \geq 2$. Let $r = \min\{r_0, r_1\}$. Then $\mathrm{ord}_2(L_{n+1}(q)) = m$ if and only if*

$$r_1 = (m - [\frac{n+1}{2}] - \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}] + r)/n.$$

A complete list of $L_n(q)$ such that $\mathrm{ord}_2(L_n(q)) = m$ can be determined by applying Lemmas 2 and 3. Since $\mathrm{ord}_2(L_{n+1}(q) > 46$ if $n \geq 20$, A complete list of $L_n(q)$ such that $\mathrm{ord}_2(L_n(q)) \leq 46$ can be obtained by the following table. (The second row of the table is read as : if q is a power of an odd prime such that $q \equiv 2^{e-2} - 1 \pmod{2^{e-1}}$ or $q \equiv 2^{(e-1)/2} + 1 \pmod{2^{(e+1)/2}}$, where $e = m \geq 4$, then a Sylow 2-subgroup of $L_3(q)$ has order 2^m. The remaining rows are interpreted similarly.)

ord_2	$L_n(q)$	$q \equiv 3$		$q \equiv 1$		$e \geq 4$
2^m	$L_3(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = m$
2^m	$L_5(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-1)/2$
2^m	$L_7(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-1)/3$
2^m	$L_9(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-3)/4$
2^m	$L_{11}(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-3)/5$
2^m	$L_{13}(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-4)/6$
2^m	$L_{15}(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-4)/7$
2^m	$L_{17}(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-7)/8$
2^m	$L_{19}(q)$	$2^{e-2}-1$	$\pmod{2^{e-1}}$	$2^{(e-1)/2}+1$	$\pmod{2^{(e+1)/2}}$	$e = (m-7)/9$

ord_2	$L_n(q)$	$q \equiv 3$		$q \equiv 1$		$e \geq 3$	$f \geq 2$
2^m	$L_2(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = m+1$	$f = m$
2^m	$L_6(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-2)/3$	$f = (m-3)/5$
2^m	$L_{10}(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-6)/5$	$f = (m-7)/9$
2^m	$L_{14}(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-9)/7$	$f = (m-10)/13$
2^m	$L_{18}(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-14)/9$	$f = (m-15)/17$

ord_2	$L_n(q)$	$q \equiv 3$		$q \equiv 1$		$e \geq 3$	$f \geq 2$
2^m	$L_4(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-1)/2$	$f = (m-1)/3$
2^m	$L_8(q)$	$2^{e-1}-1$	$\pmod{2^e}$			$e = (m-5)/4$	
2^m	$L_{12}(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-8)/6$	$f = (m-7)/11$
2^m	$L_{16}(q)$	$2^{e-1}-1$	$\pmod{2^e}$			$e = (m-13)/8$	
2^m	$L_{20}(q)$	$2^{e-1}-1$	$\pmod{2^e}$	2^f+1	$\pmod{2^{f+1}}$	$e = (m-16)/10$	$f = (m-16)/19$

ord_2	$L_n(q)$	$q \equiv 5$		$q \equiv 1$		$f \geq 3$
2^{19}	$L_8(q)$	2^2+1	$\pmod{2^{2+1}}$			
2^{43}	$L_{16}(q)$	2^2+1	$\pmod{2^{2+1}}$			
2^m	$L_8(q)$			2^f+1	$\pmod{2^{f+1}}$	$f = (m-4)/7$

ord_2	$L_n(q)$	$q \equiv 9 \pmod{16}$	$q \equiv 1 \pmod{16}$	$f \geq 4$
2^{57}	$L_{16}(q)$	$2^3+1 \pmod{2^{3+1}}$		
2^m	$L_{16}(q)$		$2^f+1 \pmod{2^{f+1}}$	$f=(m-11)/15$

A3.2. $U_n(q)$. ${}^2A_n(q) = U_{n+1}(q)$. Note that $U_3(2) = 3^2Q_8$. Similar to the $L_n(q)$ case, we have the following :

(i) Suppose that $n+1$ is odd and that q is a power of an odd prime. Then $\mathrm{ord}_2(L_{n+1}(q)) = m$ if and only if $e \geq 4$ is an integer and

(a) $q \equiv 2^{e-2}+1 \pmod{2^{e-1}}$, or

(b) $q \equiv 2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$,

where

$$e = 2(m - \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}])/n\,.$$

(ii) Suppose that $n+1$ is even and $q \equiv 1 \pmod 4$. Then $\mathrm{ord}_2(L_{n+1}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1}+1 \pmod{2^e}$, where

$$e = 2(m - [\frac{n}{2}] - \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}] + 1)/(n+1)\,.$$

(iii) Suppose that $2^{r_0} \| n+1$ and $q \equiv 2^{r_1}+3 \pmod{2^{r_1+1}}$, where $r_1 \geq 2$. Let $r = \min\{r_0, r_1\}$. Then $\mathrm{ord}_2(L_{n+1}(q)) = m$ if and only if

$$r_1 = (m - [\frac{n+1}{2}] - \sum_{k=1}^{\infty}[\frac{n+1}{2^{k+1}}] + r)/n\,.$$

ord_2	$U_n(q)$	$q \equiv 1 \pmod 4$	$q \equiv 3 \pmod 4$	$e \geq 4$
2^m	$U_3(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=m$
2^m	$U_5(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-1)/2$
2^m	$U_7(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-1)/3$
2^m	$U_9(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-3)/4$
2^m	$U_{11}(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-3)/5$
2^m	$U_{13}(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-4)/6$
2^m	$U_{15}(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-4)/7$
2^m	$U_{17}(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-7)/8$
2^m	$U_{19}(q)$	$2^{e-2}+1 \pmod{2^{e-1}}$	$2^{(e-1)/2}-1 \pmod{2^{(e+1)/2}}$	$e=(m-7)/9$

ord_2	$U_n(q)$	$q \equiv 1 \pmod 4$	$q \equiv 3 \pmod 4$	$e \geq 3$	$f \geq 2$
2^m	$U_2(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=m+1$	$f=m$
2^m	$U_6(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-2)/3$	$f=(m-3)/5$
2^m	$U_{10}(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-6)/5$	$f=(m-7)/9$
2^m	$U_{14}(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-9)/7$	$f=(m-10)/13$
2^m	$U_{18}(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-14)/9$	$f=(m-15)/17$

ord_2	$U_n(q)$	$q \equiv 1 \pmod 4$	$q \equiv 3 \pmod 4$	$e \geq 3$	$f \geq 2$
2^m	$U_4(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-1)/2$	$f=(m-1)/3$
2^m	$U_8(q)$	$2^{e-1}+1 \pmod{2^e}$		$e=(m-5)/4$	
2^m	$U_{12}(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-8)/6$	$f=(m-7)/11$
2^m	$U_{16}(q)$	$2^{e-1}+1 \pmod{2^e}$		$e=(m-13)/8$	
2^m	$U_{20}(q)$	$2^{e-1}+1 \pmod{2^e}$	$2^f-1 \pmod{2^{f+1}}$	$e=(m-16)/10$	$f=(m-16)/19$

ord_2	$U_n(q)$	$q \equiv 3 \pmod 8$	$q \equiv 7 \pmod 8$	$f \geq 3$
2^{19}	$U_8(q)$	$2^2-1 \pmod{2^{2+1}}$		
2^{43}	$U_{16}(q)$	$2^2-1 \pmod{2^{2+1}}$		
2^m	$U_8(q)$		$2^f-1 \pmod{2^{f+1}}$	$f=(m-4)/7$

ord_2	$U_n(q)$	$q \equiv 7 \pmod{16}$	$q \equiv 15 \pmod{16}$	$f \geq 4$
2^{57}	$U_{16}(q)$	$2^3 - 1 \pmod{2^{3+1}}$		
2^m	$U_{16}(q)$		$2^f - 1 \pmod{2^{f+1}}$	$f = (m - 11)/15$

A3.3. $O_{2n+1}(q)$. $B_n(q) = O_{2n+1}(q)$. Note that $O_3(q) = L_2(q)$, $O_5(q) = S_4(q)$ and $O_5(2) = S_4(2)$ is the symmetric group on 6 letters. Let q be a power of an odd prime. Similar to $L_n(q)$, we have the following.

(i) $q \equiv 1 \pmod 4$, then $\mathrm{ord}_2(O_{2n+1}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} + 1 \pmod{2^e}$,

(ii) $q \equiv 3 \pmod 4$, then $\mathrm{ord}_2(O_{2n+1}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} - 1 \pmod{2^e}$,

where

$$e = (m - \sum_{k=1}^{\infty} [\frac{2n}{2^{k+1}}] + 1)/n .$$

ord_2	$O_{2n+1}(q)$	$q \equiv \pm 1 \pmod 4$	$e \geq 3$
2^m	$O_3(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m + 1$
2^m	$O_5(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m/2$
2^m	$O_7(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m/3$
2^m	$O_9(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 2/4$
2^m	$O_{11}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 2/5$
2^m	$O_{13}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 3/6$
2^m	$O_{15}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 3/7$
2^m	$O_{17}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 6/8$
2^m	$O_{19}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 6/9$
2^m	$O_{21}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 7/10$
2^m	$O_{23}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 7/11$
2^m	$O_{25}(q)$	$2^{e-1} + 1 \pmod{2^e}$	$e = m - 9/12$
2^m	$O_{27}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 9/13$
2^m	$O_{29}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 10/14$
2^m	$O_{31}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 10/15$
2^m	$O_{33}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 14/16$
2^m	$O_{35}(q)$	$2^{e-1} \pm 1 \pmod{2^e}$	$e = m - 14/17$

A3.4. $S_{2n}(q)$. $C_n(q) = S_{2n}(q)$. Note that $S_4(q) = O_5(q)$ and $S_4(2) = O_5(2)$ is the symmetric group on 6 letters. Let q be a power of an odd prime. Similar to $L_n(q)$, we have the following.

(i) $q \equiv 1 \pmod 4$, then $\mathrm{ord}_2(S_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} + 1 \pmod{2^e}$,

(ii) $q \equiv 3 \pmod 4$, then $\mathrm{ord}_2(S_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} - 1 \pmod{2^e}$,

where

$$e = (m - \sum_{k=1}^{\infty} [\frac{2n}{2^{k+1}}] + 1)/n .$$

ord_2	$S_{2n}(q)$	$q \equiv \pm 1$	(mod 4)	$e \geq 3$
2^m	$S_2(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m + 1$
2^m	$S_4(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m/2$
2^m	$S_6(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m/3$
2^m	$S_8(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 2/4$
2^m	$S_{10}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 2/5$
2^m	$S_{12}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 3/6$
2^m	$S_{14}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 3/7$
2^m	$S_{16}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 6/8$
2^m	$S_{18}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 6/9$
2^m	$S_{20}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 7/10$
2^m	$S_{22}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 7/11$
2^m	$S_{24}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 9/12$
2^m	$S_{26}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 9/13$
2^m	$S_{28}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 10/14$
2^m	$S_{30}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 10/15$
2^m	$S_{32}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 14/16$
2^m	$S_{34}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m - 14/17$

A3.5. $O^+_{2n}(q)$. $D_n(q) = O^+_{2n}(q)$. Note that $O^+_4(q) = L_2(q) \times L_2(q)$ and $O^+_6(q) = L_4(q)$. Let q be a power of an odd prime. Similar to $L_n(q)$, we have the following.

(i) n is even. Let $\mathrm{ord}_2(n) = r$. Then

(a) if $q \equiv 1 \pmod 4$, then $\mathrm{ord}_2(O^+_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} + 1 \pmod{2^e}$,

(b) if $q \equiv 3 \pmod 4$, then $\mathrm{ord}_2(O^+_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} - 1 \pmod{2^e}$,

where

$$e = (m - \sum_{k=1}^{\infty} [\frac{2n-2}{2^{k+1}}] - r + 3)/n .$$

(ii) n is odd. Then

(a) if $q \equiv 1 \pmod 4$, then $\mathrm{ord}_2(O^+_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^e + 1 \pmod{2^{e+1}}$,

(b) if $q \equiv 3 \pmod 4$, then $\mathrm{ord}_2(O^+_{2n}(q)) = m$ if and only if $f \geq 2$ is an integer and $q \equiv 2^f - 1 \pmod{2^{f+1}}$,

where

$$e = (m - \sum_{k=1}^{\infty} [\frac{2n-2}{2^{k+1}}] - n + 3)/n ,$$

$$f = (m - \sum_{k=1}^{\infty} [\frac{2n-2}{2^{k+1}}] - n + 1)/(n-1) .$$

ord_2	$O^+_{4n}(q)$	$q \equiv \pm 1$	(mod 4)	$e \geq 3$
2^m	$O^+_4(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m + 2)/2$
2^m	$O^+_8(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m/4$
2^m	$O^+_{12}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m - 1)/6$
2^m	$O^+_{16}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m - 4)/8$
2^m	$O^+_{20}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m - 5)/10$
2^m	$O^+_{24}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m - 7)/12$
2^m	$O^+_{28}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m - 8)/14$

ord_2	$O^+_{2n}(q)$	$q \equiv 1$	(mod 4)	$q \equiv 3$	(mod 4)	$e \geq 2$	$f \geq 2$
2^m	$O^+_6(q)$	$2^e + 1$	(mod 2^{e+1})	$2^f - 1$	(mod 2^{f+1})	$e = (m-1)/3$	$f = (m-3)/2$
2^m	$O^+_{10}(q)$	$2^e + 1$	(mod 2^{e+1})	$2^f - 1$	(mod 2^{f+1})	$e = (m-5)/5$	$f = (m-7)/4$
2^m	$O^+_{14}(q)$	$2^e + 1$	(mod 2^{e+1})	$2^f - 1$	(mod 2^{f+1})	$e = (m-8)/7$	$f = (m-10)/6$
2^m	$O^+_{18}(q)$	$2^e + 1$	(mod 2^{e+1})	$2^f - 1$	(mod 2^{f+1})	$e = (m-13)/9$	$f = (m-15)/8$
2^m	$O^+_{22}(q)$	$2^e + 1$	(mod 2^{e+1})	$2^f - 1$	(mod 2^{f+1})	$e = (m-16)/11$	$f = (m-18)/10$
2^m	$O^+_{26}(q)$	$2^e + 1$	(mod 2^{e+1})	$2^f - 1$	(mod 2^{f+1})	$e = (m-20)/13$	$f = (m-22)/12$

A3.6. $O^-_{2n}(q)$. ${}^2D_n(q) = O^-_{2n}(q)$. Note that $O^-_4(q) = L_2(q^2)$ and $O^-_6(q) = U_4(q)$. Let q be a power of an odd prime. Similar to $L_n(q)$, we have the following.

(i) n is even. Then

(a) if $q \equiv 1 \pmod 4$, then $\mathrm{ord}_2(O^-_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} + 1 \pmod{2^e}$,

(b) if $q \equiv 3 \pmod 4$, then $\mathrm{ord}_2(O^-_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} - 1 \pmod{2^e}$.

(ii) n is odd. Then

(a) if $q \equiv 1 \pmod 4$, then $\mathrm{ord}_2(O^-_{2n}(q)) = m$ if and only if $e \geq 3$ is an integer and $q \equiv 2^{e-1} + 1 \pmod{2^e}$,

(b) if $q \equiv 3 \pmod 4$, then $\mathrm{ord}_2(O^-_{2n}(q)) = m$ if and only if $f \geq 2$ is an integer and $q \equiv 2^f - 1 \pmod{2^{f+1}}$,

where

$$e = (m - \sum_{k=1}^{\infty}[\frac{2n-2}{2^{k+1}}])/(n-1)\,.$$

$$f = (m - \sum_{k=1}^{\infty}[\frac{2n-2}{2^{k+1}}] - n + 3)/n\,.$$

ord_2	$O^-_{4n}(q)$	$q \equiv \pm 1$	(mod 4)	$e \geq 3$
2^m	$O^-_4(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = m$
2^m	$O^-_8(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m-1)/3$
2^m	$O^-_{12}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m-3)/5$
2^m	$O^-_{16}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m-4)/7$
2^m	$O^-_{20}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m-7)/9$
2^m	$O^-_{24}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m-8)/11$
2^m	$O^-_{28}(q)$	$2^{e-1} \pm 1$	(mod 2^e)	$e = (m-10)/13$

ord_2	$O^-_{2n}(q)$	$q \equiv 1$	(mod 4)	$q \equiv 3$	(mod 4)	$e \geq 3$	$f \geq 2$
2^m	$O^-_6(q)$	$2^{e-1} + 1$	(mod 2^e)	$2^f - 1$	(mod 2^{f+1})	$e = (m-1)/2$	$f = (m-1)/3$
2^m	$O^-_{10}(q)$	$2^{e-1} + 1$	(mod 2^e)	$2^f - 1$	(mod 2^{f+1})	$e = (m-3)/4$	$f = (m-5)/5$
2^m	$O^-_{14}(q)$	$2^{e-1} + 1$	(mod 2^e)	$2^f - 1$	(mod 2^{f+1})	$e = (m-4)/6$	$f = (m-8)/7$
2^m	$O^-_{18}(q)$	$2^{e-1} + 1$	(mod 2^e)	$2^f - 1$	(mod 2^{f+1})	$e = (m-7)/8$	$f = (m-13)/9$
2^m	$O^-_{22}(q)$	$2^{e-1} + 1$	(mod 2^e)	$2^f - 1$	(mod 2^{f+1})	$e = (m-8)/10$	$f = (m-16)/11$
2^m	$O^-_{26}(q)$	$2^{e-1} + 1$	(mod 2^e)	$2^f - 1$	(mod 2^{f+1})	$e = (m-10)/12$	$f = (m-20)/13$

A3.7. Lie Groups of Exceptional Type. Let q be a power of an odd prime. Then the following holds.

(i) $E_6(q)$-case :

(a) $q \equiv 1 \pmod 4$, $\mathrm{ord}_2(E_6(q)) = m$ iff $q \equiv 2^{(m-7)/6} + 1 \pmod{2^{(m-1)/6}}$,
(b) $q \equiv 3 \pmod 4$, $\mathrm{ord}_2(E_6(q)) = m$ iff $q \equiv 2^{(m-9)/4} - 1 \pmod{2^{(m-5)/4}}$.

(ii) ${}^2E_6(q)$-case :

(a) $q \equiv 3 \pmod 4$, $\mathrm{ord}_2({}^2E_6(q)) = m$ iff $q \equiv 2^{(m-7)/6} - 1 \pmod{2^{(m-1)/6}}$,
(b) $q \equiv 1 \pmod 4$, $\mathrm{ord}_2({}^2E_6(q)) = m$ iff $q \equiv 2^{(m-9)/4} + 1 \pmod{2^{(m-5)/4}}$.

(iii) $E_7(q)$-case :

(a) $q \equiv 1 \pmod 4$, $\mathrm{ord}_2(E_7(q)) = m$ iff $q \equiv 2^{(m-9)/7} + 1 \pmod{2^{(m-2)/7}}$,
(b) $q \equiv 3 \pmod 4$, $\mathrm{ord}_2(E_7(q)) = m$ iff $q \equiv 2^{(m-9)/7} - 1 \pmod{2^{(m-2)/7}}$.

(iv) $E_8(q)$-case :

(a) $q \equiv 1 \pmod 4$, $\mathrm{ord}_2(E_8(q)) = m$ iff $q \equiv 2^{(m-14)/8} + 1 \pmod{2^{(m-6)/8}}$,
(b) $q \equiv 3 \pmod 4$, $\mathrm{ord}_2(E_8(q)) = m$ iff $q \equiv 2^{(m-14)/8} - 1 \pmod{2^{(m-6)/8}}$.

(v) $F_4(q)$-case :

(a) $q \equiv 1 \pmod 4$, $\mathrm{ord}_2(F_4(q)) = m$ iff $q \equiv 2^{(m-7)/4} + 1 \pmod{2^{(m-3)/4}}$,
(b) $q \equiv 3 \pmod 4$, $\mathrm{ord}_2(F_4(q)) = m$ iff $q \equiv 2^{(m-7)/4} - 1 \pmod{2^{(m-3)/4}}$.

(vi) $G_2(q)$-case :

(a) $q \equiv 1 \pmod 4$, $\mathrm{ord}_2(G_2(q)) = m$ iff $q \equiv 2^{(m-2)/2} + 1 \pmod{2^{m/2}}$,
(b) $q \equiv 3 \pmod 4$, $\mathrm{ord}_2(G_2(q)) = m$ iff $q \equiv 2^{(m-2)/2} - 1 \pmod{2^{m/2}}$.

Remark. Note that $\mathrm{ord}_2({}^3D_4(q)) = \mathrm{ord}_2(G_2(q))$.

A4. Simple groups G of Lie type such that $\mathrm{ord}_2(G) = m$, $m \leq 46$

We list in this section simple groups G of Lie type such that $\mathrm{ord}_2(G) = m$, $m \leq 46$.

A4.1. $L_n(q)$. We list in this section the groups $L_n(q)$ such that $\mathrm{ord}_2(L_n(q)) = m$, $m \leq 46$. In the case $q = 2^r$, the order of a Sylow 2-subgroup of $L_n(q)$ is $2^{n(n-1)r/2}$. In the case q is a power of an odd prime, the following table gives all the $L_n(q)$ such that $\mathrm{ord}_2(L_n(q)) = m$, $m \leq 46$.

2^m	G								
2^2	$(2,2\pm)$								
2^3	$(2,3\pm)$								
2^4	$(2,4\pm)$	$(3,2-)$							
2^5	$(2,5\pm)$	$(3,3-)$	$(3,2+)$						
2^6	$(2,6\pm)$	$(3,4-)$							
2^7	$(2,7\pm)$	$(3,5-)$	$(3,3+)$	$(4,2\pm)$					
2^8	$(2,8\pm)$	$(3,6-)$							
2^9	$(2,9\pm)$	$(3,7-)$	$(3,4+)$	$(4,3-)$	$(5,2-)$				
2^{10}	$(2,10\pm)$	$(3,8-)$	$(4,3+)$						
2^{11}	$(2,11\pm)$	$(3,9-)$	$(3,5+)$	$(4,4-)$	$(5,3-)$	$(5,2+)$	$(6,2-)$		
2^{12}	$(2,12\pm)$	$(3,10-)$							
2^{13}	$(2,13\pm)$	$(3,11-)$	$(3,6+)$	$(4,5-)$	$(4,4+)$	$(5,4-)$	$(6,2+)$	$(7,2-)$	
2^{14}	$(2,14\pm)$	$(3,12-)$	$(6,3-)$						
2^{15}	$(2,15\pm)$	$(3,13-)$	$(3,7+)$	$(4,6-)$	$(5,5-)$	$(5,3+)$			
2^{16}	$(2,16\pm)$	$(3,14-)$	$(4,5+)$	$(7,3-)$	$(7,2+)$				
2^{17}	$(2,17\pm)$	$(3,15-)$	$(3,8+)$	$(4,7-)$	$(5,6-)$	$(6,4-)$	$(8,2-)$		
2^{18}	$(2,18\pm)$	$(3,16-)$	$(6,3+)$						
2^{19}	$(2,19\pm)$ $(9,2-)$	$(3,17-)$	$(3,9+)$	$(4,8-)$	$(4,6+)$	$(5,7-)$	$(5,4+)$	$(7,4-)$	$(8,2+)$
2^{20}	$(2,20\pm)$	$(3,18-)$	$(6,5-)$						
2^{21}	$(2,21\pm)$	$(3,19-)$	$(3,10+)$	$(4,9-)$	$(5,8-)$	$(8,3-)$	$(10,2-)$		
2^{22}	$(2,22\pm)$	$(3,20-)$	$(4,7+)$	$(7,5-)$	$(7,3+)$				
2^{23}	$(2,23\pm)$ $(9,2+)$	$(3,21-)$ $(11,2-)$	$(3,11+)$	$(4,10-)$	$(5,9-)$	$(5,5+)$	$(6,6-)$	$(6,4+)$	$(9,3-)$
2^{24}	$(2,24\pm)$	$(3,22-)$							
2^{25}	$(2,25\pm)$ $(10,2+)$	$(3,23-)$	$(3,12+)$	$(4,11-)$	$(4,8+)$	$(5,10-)$	$(7,6-)$	$(8,4-)$	$(8,3+)$
2^{26}	$(2,26\pm)$	$(3,24-)$	$(6,7-)$	$(10,3-)$	$(12,2-)$				
2^{27}	$(2,27\pm)$	$(3,25-)$	$(3,13+)$	$(4,12-)$	$(5,11-)$	$(5,6+)$	$(9,4-)$		
2^{28}	$(2,28\pm)$	$(3,26-)$	$(4,9+)$	$(6,5+)$	$(7,7-)$	$(7,4+)$	$(11,3-)$	$(11,2+)$	$(13,2-)$
2^{29}	$(2,29\pm)$	$(3,27-)$	$(3,14+)$	$(4,13-)$	$(5,12-)$	$(6,8-)$	$(8,5-)$	$(12,2+)$	
2^{30}	$(2,30\pm)$	$(3,28-)$	$(14,2-)$						
2^{31}	$(2,31\pm)$ $(9,3+)$	$(3,29-)$ $(10,4-)$	$(3,15+)$	$(4,14-)$	$(4,10+)$	$(5,13-)$	$(5,7+)$	$(7,8-)$	$(9,5-)$
2^{32}	$(2,32\pm)$	$(3,30-)$	$(6,9-)$	$(8,4+)$	$(12,3-)$	$(15,2-)$			
2^{33}	$(2,33\pm)$	$(3,31-)$	$(3,16+)$	$(4,15-)$	$(5,14-)$	$(6,6+)$	$(8,6-)$	$(11,4-)$	
2^{34}	$(2,34\pm)$	$(3,32-)$	$(4,11+)$	$(7,9-)$	$(7,5+)$	$(10,3+)$	$(13,3-)$	$(13,2+)$	
2^{35}	$(2,35\pm)$	$(3,33-)$	$(3,17+)$	$(4,16-)$	$(5,15-)$	$(5,8+)$	$(6,10-)$	$(9,6-)$	
2^{36}	$(2,36\pm)$	$(3,34-)$	$(10,5-)$	$(14,2+)$					
2^{37}	$(2,37\pm)$ $(16,2-)$	$(3,35-)$	$(3,18+)$	$(4,17-)$	$(4,12+)$	$(5,16-)$	$(7,10-)$	$(8,7-)$	$(14,3-)$
2^{38}	$(2,38\pm)$	$(3,36-)$	$(6,11-)$	$(6,7+)$	$(11,5-)$	$(11,3+)$	$(12,4-)$		
2^{39}	$(2,39\pm)$ $(15,3-)$	$(3,37-)$ $(15,2+)$	$(3,19+)$ $(17,2-)$	$(4,18-)$	$(5,17-)$	$(5,9+)$	$(8,5+)$	$(9,7-)$	$(9,4+)$
2^{40}	$(2,40\pm)$	$(3,38-)$	$(4,13+)$	$(7,11-)$	$(7,6+)$	$(12,3+)$	$(13,4-)$		
2^{41}	$(2,41\pm)$	$(3,39-)$	$(3,20+)$	$(4,19-)$	$(5,18-)$	$(6,12-)$	$(8,8-)$	$(10,6-)$	$(18,2-)$
2^{42}	$(2,42\pm)$	$(3,40-)$							
2^{43}	$(2,43\pm)$ $(9,8-)$	$(3,41-)$ $(10,4+)$	$(3,21+)$ $(11,6-)$	$(4,21-)$ $(16,2+)$	$(4,14+)$ $(19,2-)$	$(5,19-)$	$(5,10+)$	$(6,8+)$	$(7,12-)$
2^{44}	$(2,44\pm)$	$(3,42-)$	$(6,13-)$	$(12,5-)$	$(14,4-)$				
2^{45}	$(2,45\pm)$	$(3,43-)$	$(3,22+)$	$(4,22-)$	$(5,20-)$	$(8,9-)$	$(16,3-)$		
2^{46}	$(2,46\pm)$ $(15,4-)$	$(3,44-)$ $(20,2-)$	$(4,15+)$	$(7,13-)$	$(7,7+)$	$(8,6+)$	$(10,7-)$	$(13,5-)$	$(13,3+)$

(i) $(a,b\pm) = L_a(q)$, where q is a power of a prime such that $q \equiv 2^b \pm 1 \pmod{2^{b+1}}$,

(ii) $(a,b-) = L_a(q)$, where q is a power of a prime such that $q \equiv 2^b - 1 \pmod{2^{b+1}}$,

(iii) $(a,b+) = L_a(q)$, where q is a power of a prime such that $q \equiv 2^b + 1 \pmod{2^{b+1}}$.

A4.2. $U_n(q)$. We list in this section the groups $U_n(q)$ such that $\mathrm{ord}_2(U_n(q)) = m$, $m \leq 46$. In the case $q = 2^r$, the order of a Sylow 2-subgroup of $U_n(q)$ is $2^{n(n-1)r/2}$. In the case q is a power of an odd prime, a complete list of $U_n(q)$ such that $\mathrm{ord}_2(U_n(q)) = m$ $(m \leq 46)$ can be obtained from the table in section A4.1, where

(i) $(a,b\pm) = U_a(q)$, where q is a power of a prime such that $q \equiv 2^b \mp 1 \pmod{2^{b+1}}$,

(ii) $(a,b-) = U_a(q)$, where q is a power of a prime such that $q \equiv 2^b + 1 \pmod{2^{b+1}}$,

(iii) $(a,b+) = U_a(q)$, where q is a power of a prime such that $q \equiv 2^b - 1 \pmod{}$

2^{b+1}).

Remark. Note that the interpretation of the symbol (a, b) in A4.1 and A4.2 is different.

A4.3. $O_{2n+1}(q)$, $S_{2n}(q)$. We list in this section the groups $O_{2n+1}(q)$ such that $\mathrm{ord}_2(O_{2n+1}(q)) = m$, $m \leq 46$. In the case $q = 2^r$, the order of a Sylow 2-subgroup of $O_{2n+1}(q)$ is $2^{n^2 r}$. In the case q is a power of an odd prime, the following table gives all the $O_{2n+1}(q)$ such that $\mathrm{ord}_2(O_{2n+1}(q)) = m$, $m \leq 46$. Note that the 2-parts of $O_{2n+1}(q)$ and $S_{2n}(q)$ are the same.

2^m	G					
2^2	(3, 2)					
2^3	(3, 3)					
2^4	(3, 4)					
2^5	(3, 5)					
2^6	(3, 6)	(5, 2)				
2^7	(3, 7)					
2^8	(3, 8)	(5, 3)				
2^9	(3, 9)	(7, 2)				
2^{10}	(3, 10)	(5, 4)				
2^{11}	(3, 11)					
2^{12}	(3, 12)	(5, 5)	(7, 3)			
2^{13}	(3, 13)					
2^{14}	(3, 14)	(5, 6)	(9, 2)			
2^{15}	(3, 15)	(7, 4)				
2^{16}	(3, 16)	(5, 7)				
2^{17}	(3, 17)	(11, 2)				
2^{18}	(3, 18)	(5, 8)	(7, 5)	(9, 3)		
2^{19}	(3, 19)					
2^{20}	(3, 20)	(5, 9)				
2^{21}	(3, 21)	(7, 6)	(13, 2)			
2^{22}	(3, 22)	(5, 10)	(9, 4)	(11, 3)		
2^{23}	(3, 23)					
2^{24}	(3, 24)	(5, 11)	(7, 7)	(15, 2)		
2^{25}	(3, 25)					
2^{26}	(3, 26)	(5, 12)	(9, 5)			
2^{27}	(3, 27)	(7, 8)	(11, 4)	(13, 3)		
2^{28}	(3, 28)	(5, 13)				
2^{29}	(3, 29)					
2^{30}	(3, 30)	(5, 14)	(7, 9)	(9, 6)	(17, 2)	
2^{31}	(3, 31)	(15, 3)				
2^{32}	(3, 32)	(5, 15)	(11, 5)			
2^{33}	(3, 33)	(7, 10)	(13, 4)	(19, 2)		
2^{34}	(3, 34)	(5, 16)	(9, 7)			
2^{35}	(3, 35)					
2^{36}	(3, 36)	(5, 17)	(7, 11)			
2^{37}	(3, 37)	(11, 6)	(21, 2)			
2^{38}	(3, 38)	(5, 18)	(9, 8)	(15, 4)	(17, 3)	
2^{39}	(3, 39)	(7, 12)	(13, 5)			
2^{40}	(3, 40)	(5, 19)	(23, 2)			
2^{41}	(3, 41)					
2^{42}	(3, 42)	(5, 20)	(7, 13)	(9, 9)	(11, 7)	(19, 3)
2^{43}	(3, 43)					
2^{44}	(3, 44)	(5, 21)				
2^{45}	(3, 45)	(7, 14)	(13, 6)	(15, 5)	(25, 2)	
2^{46}	(3, 46)	(5, 22)	(9, 10)	(17, 4)		

Note that (a, b) is the group $O_a(q)$, where q is a power of a prime such that $q \equiv 2^b \pm 1 \pmod{2^{b+1}}$.

A4.4. $O^+_{2n}(q)$. We list in this section the groups $O^+_{2n}(q)$ such that $\mathrm{ord}_2(O^+_{2n}(q)) = m$, $m \leq 46$. In the case $q = 2^r$, the order of a Sylow 2-subgroup of $O^+_{2n}(q)$ is $2^{n(n-1)r}$. In the case q is a power of an odd prime, the following table gives all the $O^+_{2n}(q)$ such that $\mathrm{ord}_2(O^+_{2n}(q)) = m$, $m \leq 46$.

2^m	G					
2^2						
2^3						
2^4	$(4, 2\pm)$					
2^5						
2^6	$(4, 3\pm)$					
2^7	$(6, 2\pm)$					
2^8	$(4, 4\pm)$					
2^9	$(6, 3-)$					
2^{10}	$(4, 5\pm)$	$(6, 3+)$				
2^{11}	$(6, 4-)$					
2^{12}	$(4, 6\pm)$	$(8, 2\pm)$				
2^{13}	$(6, 4+)$	$(6, 5-)$				
2^{14}	$(4, 7\pm)$					
2^{15}	$(6, 6-)$	$(10, 2\pm)$				
2^{16}	$(4, 8\pm)$	$(6, 5+)$	$(8, 3\pm)$			
2^{17}	$(6, 7-)$					
2^{18}	$(4, 9\pm)$					
2^{19}	$(6, 6+)$	$(6, 8-)$	$(10, 3-)$	$(12, 2\pm)$		
2^{20}	$(4, 10\pm)$	$(8, 4\pm)$	$(10, 3+)$			
2^{21}	$(6, 9-)$					
2^{22}	$(4, 11\pm)$	$(6, 7+)$	$(14, 2\pm)$			
2^{23}	$(6, 10-)$	$(10, 4-)$				
2^{24}	$(4, 12\pm)$	$(8, 5\pm)$				
2^{25}	$(6, 8+)$	$(6, 11-)$	$(10, 4+)$	$(12, 3\pm)$		
2^{26}	$(4, 13\pm)$					
2^{27}	$(6, 12-)$	$(10, 5-)$				
2^{28}	$(4, 14\pm)$	$(6, 9+)$	$(8, 6\pm)$	$(14, 3-)$	$(16, 2\pm)$	
2^{29}	$(6, 13-)$	$(14, 3+)$				
2^{30}	$(4, 15\pm)$	$(10, 5+)$				
2^{31}	$(6, 10+)$	$(6, 14-)$	$(10, 6-)$	$(12, 4\pm)$	$(18, 2\pm)$	
2^{32}	$(4, 16\pm)$	$(8, 7\pm)$				
2^{33}	$(6, 15-)$					
2^{34}	$(4, 17\pm)$	$(6, 11+)$	$(14, 4-)$			
2^{35}	$(6, 16-)$	$(10, 6+)$	$(10, 7-)$	$(20, 2\pm)$		
2^{36}	$(4, 18\pm)$	$(8, 8\pm)$	$(14, 4+)$	$(16, 3\pm)$		
2^{37}	$(6, 12+)$	$(6, 17-)$	$(12, 5\pm)$			
2^{38}	$(4, 19\pm)$	$(22, 2-)$	$(22, 2+)$			
2^{39}	$(6, 18-)$	$(10, 8-)$	$(18, 3-)$			
2^{40}	$(4, 20\pm)$	$(6, 13+)$	$(8, 9\pm)$	$(10, 7+)$	$(14, 5-)$	$(18, 3+)$
2^{41}	$(6, 19-)$					
2^{42}	$(4, 21\pm)$					
2^{43}	$(6, 14+)$	$(6, 20-)$	$(10, 9-)$	$(12, 6\pm)$	$(14, 5+)$	$(24, 2\pm)$
2^{44}	$(4, 22\pm)$	$(8, 10\pm)$	$(16, 4\pm)$			
2^{45}	$(6, 21-)$	$(10, 8+)$	$(20, 3\pm)$			
2^{46}	$(4, 23\pm)$	$(6, 15+)$	$(14, 6-)$	$(26, 2\pm)$		

(i) $(a, b\pm) = O_a^+(q)$, where q is a power of a prime such that $q \equiv 2^b \pm 1 \pmod{2^{b+1}}$,

(ii) $(a, b-) = O_a^+(q)$, where q is a power of a prime such that $q \equiv 2^b - 1 \pmod{2^{b+1}}$,

(iii) $(a, b+) = O_a^+(q)$, where q is a power of a prime such that $q \equiv 2^b + 1 \pmod{2^{b+1}}$.

A4.5. $O_{2n}^-(q)$. We list in this section the groups $O_{2n}^-(q)$ such that $\mathrm{ord}_2(O_{2n}^-(q)) = m$, $m \leq 46$. In the case $q = 2^r$, the order of a Sylow 2-subgroup of $O_{2n}^-(q)$ is $2^{n(n-1)r}$. In the case q is a power of an odd prime, the following table gives all the $O_{2n}^-(q)$ such that $\mathrm{ord}_2(O_{2n}^-(q)) = m$, $m \leq 46$.

2^m	G							
2^2								
2^3	$(4, 2\pm)$							
2^4	$(4, 3\pm)$							
2^5	$(4, 4\pm)$							
2^6	$(4, 5\pm)$							
2^7	$(4, 6\pm)$	$(6, 2\pm)$						
2^8	$(4, 7\pm)$							
2^9	$(4, 8\pm)$	$(6, 3+)$						
2^{10}	$(4, 9\pm)$	$(6, 3-)$	$(8, 2\pm)$					
2^{11}	$(4, 10\pm)$	$(6, 4+)$						
2^{12}	$(4, 11\pm)$							
2^{13}	$(4, 12\pm)$	$(6, 5+)$	$(6, 4-)$	$(8, 3\pm)$				
2^{14}	$(4, 13\pm)$							
2^{15}	$(4, 14\pm)$	$(6, 6+)$	$(10, 2\pm)$					
2^{16}	$(4, 15\pm)$	$(6, 5-)$	$(8, 4\pm)$					
2^{17}	$(4, 16\pm)$	$(6, 7+)$						
2^{18}	$(4, 17\pm)$	$(12, 2\pm)$						
2^{19}	$(4, 18\pm)$	$(6, 8+)$	$(6, 6-)$	$(8, 5\pm)$	$(10, 3+)$			
2^{20}	$(4, 19\pm)$	$(10, 3-)$						
2^{21}	$(4, 20\pm)$	$(6, 9+)$						
2^{22}	$(4, 21\pm)$	$(6, 7-)$	$(8, 6\pm)$	$(14, 2\pm)$				
2^{23}	$(4, 22\pm)$	$(6, 10+)$	$(10, 4+)$	$(12, 3\pm)$				
2^{24}	$(4, 23\pm)$							
2^{25}	$(4, 24\pm)$	$(6, 11+)$	$(6, 8-)$	$(8, 7\pm)$	$(10, 4-)$	$(16, 2\pm)$		
2^{26}	$(4, 25\pm)$							
2^{27}	$(4, 26\pm)$	$(6, 12+)$	$(10, 5+)$					
2^{28}	$(4, 27\pm)$	$(6, 9-)$	$(8, 8\pm)$	$(12, 4\pm)$	$(14, 3+)$			
2^{29}	$(4, 28\pm)$	$(6, 13+)$	$(14, 3-)$					
2^{30}	$(4, 29\pm)$	$(10, 5-)$						
2^{31}	$(4, 30\pm)$	$(6, 14+)$	$(6, 10-)$	$(8, 9\pm)$	$(10, 6+)$	$(18, 2\pm)$		
2^{32}	$(4, 31\pm)$	$(16, 3\pm)$						
2^{33}	$(4, 32\pm)$	$(6, 15+)$	$(12, 5\pm)$					
2^{34}	$(4, 33\pm)$	$(6, 11-)$	$(8, 10\pm)$	$(14, 4+)$	$(20, 2\pm)$			
2^{35}	$(4, 34\pm)$	$(6, 16+)$	$(10, 7+)$	$(10, 6-)$				
2^{36}	$(4, 35\pm)$	$(14, 4-)$						
2^{37}	$(4, 36\pm)$	$(6, 17+)$	$(6, 12-)$	$(8, 11\pm)$				
2^{38}	$(4, 37\pm)$	$(12, 6\pm)$	$(22, 2\pm)$					
2^{39}	$(4, 38\pm)$	$(6, 18+)$	$(10, 8+)$	$(16, 4\pm)$	$(18, 3+)$			
2^{40}	$(4, 39\pm)$	$(6, 13-)$	$(8, 12\pm)$	$(10, 7-)$	$(14, 5+)$	$(18, 3-)$		
2^{41}	$(4, 40\pm)$	$(6, 19+)$	$(24, 2\pm)$					
2^{42}	$(4, 41\pm)$							
2^{43}	$(4, 42\pm)$	$(6, 20+)$	$(6, 14-)$	$(8, 13\pm)$	$(10, 9+)$	$(12, 7\pm)$	$(14, 5-)$	$(20, 3\pm)$
2^{44}	$(4, 43\pm)$							
2^{45}	$(4, 44\pm)$	$(6, 21+)$	$(10, 8-)$					
2^{46}	$(4, 45\pm)$	$(6, 15-)$	$(8, 14\pm)$	$(14, 6+)$	$(16, 5\pm)$	$(26, 2\pm)$		

(i) $(a, b\pm) = O_a^-(q)$, where q is a power of a prime such that $q \equiv 2^b \pm 1 \pmod{2^{b+1}}$,

(ii) $(a, b-) = O_a^-(q)$, where q is a power of a prime such that $q \equiv 2^b - 1 \pmod{2^{b+1}}$,

(iii) $(a, b+) = O_a^-(q)$, where q is a power of a prime such that $q \equiv 2^b + 1 \pmod{2^{b+1}}$.

A4.6. Lie Groups of Exceptional Type. We list in this subsection the groups G (of exceptional type) such that $\mathrm{ord}_2(G) = m$, $m \leq 46$. In the case $q = 2^r$, the order of a Sylow 2-subgroup of G is listed in Section A2. In the case q is a power of an odd prime, the following table gives all the G such that $\mathrm{ord}_2(G) = m$, $m \leq 46$.

2^m	$E_6(q)$	${}^2E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$ $({}^3D_4(q))$
2^2						
2^3						
2^4						
2^5						
2^6						2±
2^7						
2^8						3±
2^9						
2^{10}						4±
2^{11}						
2^{12}						5±
2^{13}						
2^{14}						6±
2^{15}					2±	
2^{16}						7±
2^{17}	2−	2+				
2^{18}						8±
2^{19}	2+	2−			3±	
2^{20}						9±
2^{21}	3−	3+				
2^{22}						10±
2^{23}			2±		4±	
2^{24}						11±
2^{25}	3+	4− 3−	4+			
2^{26}						12±
2^{27}					5±	
2^{28}						13±
2^{29}	5−	5+				
2^{30}			3±	2±		14±
2^{31}	4+	4−			6±	
2^{32}						15±
2^{33}	6−	6+				
2^{34}						16±
2^{35}					7±	
2^{36}						17±
2^{37}	5+	7− 5−	7+ 4±			
2^{38}				3±		18±
2^{39}					8±	
2^{40}						19±
2^{41}	8−	8+				
2^{42}						20±
2^{43}	6+	6−			9±	
2^{44}			5±			21±
2^{45}	9−	9+				
2^{46}				4±		22±

A5. Simple groups G such that $\mathrm{ord}_2(G) \leq 46$

We list in this section all the simple groups G such that $\mathrm{ord}_2(G) = m$, where 2^m is the order of a Sylow 2-subgroup of some sporadic simple groups.

2^n	$\mathrm{ord}_2(G) = n$		
2^3	$L_2(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$ $L_3(2)$	$R(3^{2m+1})$, $m \geq 1$ A_6	$L_2(8)$ A_7
2^4	$L_3(q)$, $q \equiv 2^2 - 1 \pmod{2^3}$ $L_2(16)$	$L_2(q)$, $q \equiv 2^4 \pm 1 \pmod{2^5}$	$U_3(q)$, $q \equiv 2^2 + 1 \pmod{2^3}$
2^6	$L_2(q)$, $q \equiv 2^6 \pm 1 \pmod{2^7}$ $O_5(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^6)$ $U_3(4)$ A_8	$L_3(q)$, $q \equiv 2^4 - 1 \pmod{2^5}$ $G_2(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_3(4)$ $U_4(2)$ A_9	$U_3(q)$, $q \equiv 2^4 + 1 \pmod{2^5}$ ${}^3D_4(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_4(2)$ $Sz(8)$
2^7	$L_2(q)$, $q \equiv 2^7 \pm 1 \pmod{2^8}$ $L_4(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $U_4(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ A_{11}	$L_3(q)$, $q \equiv 2^5 - 1 \pmod{2^6}$ $U_3(q)$, $q \equiv 2^5 + 1 \pmod{2^6}$ $L_2(2^7)$	$L_3(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $U_3(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ A_{10}
2^8	$L_2(q)$, $q \equiv 2^8 \pm 1 \pmod{2^9}$ $O_5(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$ $L_2(2^8)$	$L_3(q)$, $q \equiv 2^6 - 1 \pmod{2^7}$ $G_2(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$ $O_5(4)$	$U_3(q)$, $q \equiv 2^6 + 1 \pmod{2^7}$ ${}^3D_4(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$

2^9	$L_2(q)$, $q \equiv 2^9 \pm 1 \pmod{2^{10}}$ $L_4(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $U_3(q)$, $q \equiv 2^4 - 1 \pmod{2^5}$ $O_7(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_3(8)$ $S_6(2)$	$L_3(q)$, $q \equiv 2^7 - 1 \pmod{2^8}$ $L_5(q)$, $q \equiv 2^2 - 1 \pmod{2^3}$ $U_4(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $S_6(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $U_3(8)$ A_{12}	$L_3(q)$, $q \equiv 2^4 + 1 \pmod{2^5}$ $U_3(q)$, $q \equiv 2^7 + 1 \pmod{2^8}$ $U_5(q)$, $q \equiv 2^2 + 1 \pmod{2^3}$ $L_2(2^9)$ $O_7(2)$ A_{13}
2^{10}	$L_2(q)$, $q \equiv 2^{10} \pm 1 \pmod{2^{11}}$ $U_3(q)$, $q \equiv 2^8 + 1 \pmod{2^9}$ $O_8^-(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{10})$ $Sz(2^5)$	$L_3(q)$, $q \equiv 2^8 - 1 \pmod{2^9}$ $U_4(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $G_2(q)$, $q \equiv 2^4 \pm 1 \pmod{2^5}$ $L_5(2)$ A_{14}	$L_4(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $O_5(q)$, $q \equiv 2^4 \pm 1 \pmod{2^5}$ ${}^3D_4(q)$, $q \equiv 2^4 \pm 1 \pmod{2^5}$ $U_5(2)$ A_{15}
2^{13}	$L_2(q)$, $q \equiv 2^{13} \pm 1 \pmod{2^{14}}$ $L_4(q)$, $q \equiv 2^5 - 1 \pmod{2^6}$ $L_6(q)$, $q \equiv 2^2 + 1 \pmod{2^3}$ $U_3(q)$, $q \equiv 2^6 - 1 \pmod{2^7}$ $U_5(q)$, $q \equiv 2^4 + 1 \pmod{2^5}$ $O_8^-(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$	$L_3(q)$, $q \equiv 2^{11} - 1 \pmod{2^{12}}$ $L_4(q)$, $q \equiv 2^4 + 1 \pmod{2^5}$ $L_7(q)$, $q \equiv 2^2 - 1 \pmod{2^3}$ $U_4(q)$, $q \equiv 2^5 + 1 \pmod{2^6}$ $U_6(q)$, $q \equiv 3 \pmod{2^3}$ $L_2(2^{13})$	$L_3(q)$, $q \equiv 2^6 + 1 \pmod{2^7}$ $L_5(q)$, $q \equiv 2^4 - 1 \pmod{2^5}$ $U_3(q)$, $q \equiv 2^{11} + 1 \pmod{2^{12}}$ $U_4(q)$, $q \equiv 2^4 - 1 \pmod{2^5}$ $U_7(q)$, $q \equiv 5 \pmod{2^3}$
2^{14}	$L_2(q)$, $q \equiv 2^{14} \pm 1 \pmod{2^{15}}$ $U_3(q)$, $q \equiv 2^{12} + 1 \pmod{2^{13}}$ $O_9(q)$, $q \equiv 2^2 \pm 2 \pmod{2^3}$ ${}^3D_4(q)$, $q \equiv 2^6 \pm 1 \pmod{2^7}$ A_{16}	$L_3(q)$, $q \equiv 2^{12} - 1 \pmod{2^{13}}$ $U_6(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $S_8(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{14})$ A_{17}	$L_6(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $O_5(q)$, $q \equiv 2^6 \pm 1 \pmod{2^7}$ $G_2(q)$, $q \equiv 2^6 \pm 1 \pmod{2^7}$ $Sz(2^7)$
2^{15}	$L_2(q)$, $q \equiv 2^{15} \pm 11 \pmod{2^{16}}$ $L_4(q)$, $q \equiv 2^6 - 1 \pmod{2^7}$ $U_3(q)$, $q \equiv 2^{13} + 1 \pmod{2^{14}}$ $U_5(q)$, $q \equiv 2^5 + 1 \pmod{2^6}$ $S_6(q)$, $q \equiv 2^4 \pm 1 \pmod{2^5}$ $F_4(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_6(2)$ A_{18}	$L_3(q)$, $q \equiv 2^{13} - 1 \pmod{2^{14}}$ $L_5(q)$, $q \equiv 2^5 - 1 \pmod{2^6}$ $U_3(q)$, $q \equiv 2^7 - 1 \pmod{2^8}$ $U_5(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $O_{10}^-(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{15})$ $U_3(2^5)$ A_{19}	$L_3(q)$, $q \equiv 2^7 + 1 \pmod{2^8}$ $L_5(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $U_4(q)$, $q \equiv 2^6 + 1 \pmod{2^7}$ $O_7(q)$, $q \equiv 2^4 \pm 1 \pmod{2^5}$ $O_{10}^+(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_3(2^5)$ $U_6(2)$
2^{17}	$L_2(q)$, $q \equiv 2^{17} \pm 1 \pmod{2^{18}}$ $L_4(q)$, $q \equiv 2^7 - 1 \pmod{2^8}$ $L_8(q)$, $q \equiv 2^2 - 1 \pmod{2^3}$ $U_4(q)$, $q \equiv 2^7 + 1 \pmod{2^8}$ $U_8(q)$, $q \equiv 2^2 + 1 \pmod{2^3}$ $E_6(q)$, $q \equiv 3 \pmod{2^3}$ A_{20}	$L_3(q)$, $q \equiv 2^{15} - 1 \pmod{2^{16}}$ $L_5(q)$, $q \equiv 2^6 - 1 \pmod{2^7}$ $U_3(q)$, $q \equiv 2^{15} + 1 \pmod{2^{16}}$ $U_5(q)$, $q \equiv 2^6 + 1 \pmod{2^7}$ $O_{11}(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ ${}^2E_6(q)$, $q \equiv 5 \pmod{2^3}$ A_{21}	$L_3(q)$, $q \equiv 2^8 + 1 \pmod{2^9}$ $L_6(q)$, $q \equiv 2^4 - 1 \pmod{2^5}$ $U_3(q)$, $q \equiv 2^8 - 1 \pmod{2^9}$ $U_6(q)$, $q \equiv 2^4 + 1 \pmod{2^5}$ $S_{10}(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{17})$
2^{18}	$L_2(q)$, $q \equiv 2^{18} \pm 1 \pmod{2^{19}}$ $U_3(q)$, $q \equiv 2^{16} + 1 \pmod{2^{17}}$ $O_7(q)$, $q \equiv 2^5 \pm 1 \pmod{2^6}$ $S_8(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$ ${}^3D_4(q)$, $q \equiv 2^8 \pm 1 \pmod{2^9}$ $L_4(8)$ $O_7(4)$ $Sz(2^9)$	$L_3(q)$, $q \equiv 2^{16} - 1 \pmod{2^{17}}$ $U_6(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $O_9(q)$, $q \equiv 2^3 \pm 1 \pmod{2^4}$ $O_{12}^-(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{18})$ $U_3(2^6)$ $S_6(4)$ A_{22}	$L_6(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $O_5(q)$, $q \equiv 2^8 \pm 1 \pmod{2^9}$ $S_6(q)$, $q \equiv 2^5 \pm 1 \pmod{2^6}$ $G_2(q)$, $q \equiv 2^8 \pm 1 \pmod{2^9}$ $L_3(2^6)$ $U_4(8)$ $G_2(8)$ A_{23}
2^{21}	$L_2(q)$, $q \equiv 2^{21} \pm 1 \pmod{2^{22}}$ $L_4(q)$, $q \equiv 2^9 - 1 \pmod{2^{10}}$ $L_{10}(q)$, $q \equiv 2^2 - 1 \pmod{2^3}$ $U_4(q)$, $q \equiv 2^9 + 1 \pmod{2^{10}}$ $U_{10}(q)$, $q \equiv 2^2 + 1 \pmod{2^3}$ $S_6(q)$, $q \equiv 2^6 \pm 1 \pmod{2^7}$ ${}^2E_6(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $L_7(2)$ A_{24}	$L_3(q)$, $q \equiv 2^{19} - 1 \pmod{2^{20}}$ $L_5(q)$, $q \equiv 2^8 - 1 \pmod{2^9}$ $U_3(q)$, $q \equiv 2^{19} + 1 \pmod{2^{20}}$ $U_5(q)$, $q \equiv 2^8 + 1 \pmod{2^9}$ $O_7(q)$, $q \equiv 2^6 \pm 1 \pmod{2^7}$ $S_{12}(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{21})$ $U_3(2^7)$ A_{25}	$L_3(q)$, $q \equiv 2^{10} + 1 \pmod{2^{11}}$ $L_8(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $U_3(q)$, $q \equiv 2^{10} - 1 \pmod{2^{11}}$ $U_8(q)$, $q \equiv 2^3 + 1 \pmod{2^4}$ $O_{13}(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $E_6(q)$, $q \equiv 2^3 - 1 \pmod{2^4}$ $L_3(2^7)$ $U_7(2)$
2^{41}	$L_2(q)$, $q \equiv 2^{41} \pm 1 \pmod{2^{42}}$ $L_4(q)$, $q \equiv 2^{19} - 1 \pmod{2^{20}}$ $L_8(q)$, $q \equiv 2^8 - 1 \pmod{2^9}$ $U_3(q)$, $q \equiv 2^{39} + 1 \pmod{2^{40}}$ $U_5(q)$, $q \equiv 2^{18} + 1 \pmod{2^{19}}$ $U_{10}(q)$, $q \equiv 2^6 + 1 \pmod{2^7}$ $E_6(q)$, $q \equiv 2^8 - 1 \pmod{2^9}$ A_{46}	$L_3(q)$, $q \equiv 2^{39} - 1 \pmod{2^{40}}$ $L_5(q)$, $q \equiv 2^{18} - 1 \pmod{2^{19}}$ $L_{10}(q)$, $q \equiv 2^6 - 1 \pmod{2^7}$ $U_3(q)$, $q \equiv 2^{20} - 1 \pmod{2^{21}}$ $U_6(q)$, $q \equiv 2^{12} + 1 \pmod{2^{13}}$ $U_{18}(q)$, $q \equiv 2^2 + 1 \pmod{2^3}$ ${}^2E_6(q)$, $q \equiv 2^8 + 1 \pmod{2^9}$ A_{47}	$L_3(q)$, $q \equiv 2^{20} + 1 \pmod{2^{21}}$ $L_6(q)$, $q \equiv 2^{12} - 1 \pmod{2^{13}}$ $L_{18}(q)$, $q \equiv 2^2 - 1 \pmod{2^3}$ $U_4(q)$, $q \equiv 2^{19} + 1 \pmod{2^{20}}$ $U_8(q)$, $q \equiv 2^8 + 1 \pmod{2^9}$ $O_{24}^-(q)$, $q \equiv 2^2 \pm 1 \pmod{2^3}$ $L_2(2^{41})$

2^{46}	$L_2(q), q \equiv 2^{46} \pm 1 \pmod{2^{47}}$	$L_3(q), q \equiv 2^{44} - 1 \pmod{2^{45}}$	$L_4(q), q \equiv 2^{15} + 1 \pmod{2^{16}}$
	$L_7(q), q \equiv 2^{13} - 1 \pmod{2^{14}}$	$L_7(q), q \equiv 2^7 + 1 \pmod{2^8}$	$L_8(q), q \equiv 2^6 + 1 \pmod{2^7}$
	$L_{10}(q), q \equiv 2^7 - 1 \pmod{2^8}$	$L_{13}(q), q \equiv 2^5 - 1 \pmod{2^6}$	$L_{13}(q), q \equiv 2^3 + 1 \pmod{2^4}$
	$L_{15}(q), q \equiv 2^4 - 1 \pmod{2^5}$	$L_{20}(q), q \equiv 2^2 - 1 \pmod{2^3}$	$U_3(q), q \equiv 2^{44} + 1 \pmod{2^{45}}$
	$U_4(q), q \equiv 2^{15} - 1 \pmod{2^{16}}$	$U_7(q), q \equiv 2^{13} + 1 \pmod{2^{14}}$	$U_7(q), q \equiv 2^7 - 1 \pmod{2^8}$
	$U_8(q), q \equiv 2^6 - 1 \pmod{2^7}$	$U_{10}(q), q \equiv 2^7 + 1 \pmod{2^8}$	$U_{13}(q), q \equiv 2^5 + 1 \pmod{2^6}$
	$U_{13}(q), q \equiv 2^3 - 1 \pmod{2^4}$	$U_{15}(q), q \equiv 2^4 + 1 \pmod{2^5}$	$U_{20}(q), q \equiv 2^2 + 1 \pmod{2^3}$
	$O_5(q), q \equiv 2^{22} \pm 1 \pmod{2^{23}}$	$O_9(q), q \equiv 2^{10} \pm 1 \pmod{2^{11}}$	$O_{17}(q), q \equiv 2^4 \pm 1 \pmod{2^5}$
	$S_8(q), q \equiv 2^{10} \pm 1 \pmod{2^{11}}$	$S_{16}(q), q \equiv 2^4 \pm 1 \pmod{2^5}$	$O^+_{14}(q), q \equiv 2^6 - 1 \pmod{2^7}$
	$O^+_{26}(q), q \equiv 2^2 \pm 1 \pmod{2^3}$	$O^-_8(q), q \equiv 2^{14} \pm 1 \pmod{2^{15}}$	$O^-_{16}(q), q \equiv 2^5 \pm 1 \pmod{2^6}$
	$O^-_{14}(q), q \equiv 2^6 + 1 \pmod{2^7}$	$O^-_{26}(q), q \equiv 2^2 \pm 1 \pmod{2^3}$	$E_8(q), q \equiv 2^4 \pm 1 \pmod{2^5}$
	$G_2(q), q \equiv 2^{22} \pm 1 \pmod{2^{23}}$	${}^3D_4(q), q \equiv 2^{22} \pm 1 \pmod{2^{23}}$	$L_2(2^{46})$
	$Sz(2^{23})$	A_{50}	A_{51}

The following gives the sublist when $q = 2^m$, 3, 5, 7.

2^m	G	$q = 2^r$
2^3	*Janko*$_1$	$L_2(8), L_3(2)$
2^4	*Mathieu*$_1$	$L_2(2^4)$
2^6	*Mathieu*$_2$	$L_2(2^6), L_3(4), L_4(2), U_3(4), U_4(2), Sz(8)$
2^7	*Janko*$_2$, *Janko*$_3$, *Mathieu*$_3$, *Mathieu*$_4$, *McLaughlin*	$L_2(2^7)$
2^8	*Lyons*	$L_2(2^8), O_5(4)$
2^9	*Higman-Sims*	$L_2(2^9), L_3(8), U_3(8), O_7(2), S_6(2)$
2^{10}	*Conway*$_3$, *Held*, *Mathieu*$_5$	$L_2(2^{10}), L_5(2), U_5(2), Sz(2^5)$
2^{13}	*Suzuki*	$L_2(2^{13})$
2^{14}	*Harada*, *Rudvalis*	$L_2(2^{14}), Sz(2^7)$
2^{15}	*Thompson*	$L_2(2^{15}), L_3(2^5), L_6(2), U_3(2^5), U_6(2)$
2^{17}	*Fischer*$_1$	$L_2(2^{17})$
2^{18}	*Conway*$_2$	$L_2(2^{18}), L_3(2^6), L_4(8), U_3(2^6), U_4(8), O_7(4), S_6(4), G_2(8), Sz(2^9)$
2^{21}	*Conway*$_1$, *Fischer*$_3$, *Janko*$_4$	$L_2(2^{21}), L_3(2^7), L_7(2), U_3(2^7), U_7(2)$
2^{41}	*Fischer*$_4$	$L_2(2^{41})$
2^{46}	*Monster*	$L_2(2^{46}), Sz(2^{23})$

2^m	G	$q = 3$	$q = 5$	$q = 7$
2^3	*Janko*$_1$		$L_2(7)$	
2^4	*Mathieu*$_1$	$L_3(3)$	$U_3(5)$	
2^6	*Mathieu*$_2$	$O_5(3), G_2(3)$ ${}^3D_4(3)$	$O_5(5), G_2(5)$ ${}^3D_4(5)$	
2^7	*Janko*$_2$, *Janko*$_3$, *Mathieu*$_3$, *Mathieu*$_4$, *McLaughlin*	$L_4(3)$, $U_4(3)$,	$L_4(5), U_4(5)$	$U_3(7)$
2^8	*Lyons*			$O_5(7), G_2(7)$ ${}^3D_4(7)$
2^9	*Higman-Sims*, *O'Nan*	$L_5(3), O_7(3)$ $S_6(3)$	$U_5(5), S_6(5)$ $O_7(5)$	$L_4(7)$
2^{10}	*Conway*$_3$, *Held*, *Mathieu*$_5$	$O^-_8(3)$	$O^-_8(5)$	$U_4(7)$
2^{13}	*Suzuki*	$L_7(3), U_6(3)$	$U_7(5), L_6(5)$	$O^-_8(7)$
2^{14}	*Harada*, *Rudvalis*	$O_9(3), S_8(3)$	$S_8(5), O_9(5)$	$L_6(7)$
2^{15}	*Thompson*	$O^+_{10}(3), F_4(3)$ $O^-_{10}(3)$	$O^+_{10}(5), F_4(5)$	$U_5(7)$
2^{17}	*Fischer*$_1$	$L_8(3), O_{11}(3)$ $S_{10}(3), E_6(3)$	$U_8(5), S_{10}(5)$ $O_{11}(5), {}^2E_6(5)$	
2^{18}	*Conway*$_2$, *Fischer*$_2$	$O^-_{12}(3)$	$O^-_{12}(5)$	$U_6(7), S_8(7)$ $O_9(7)$
2^{21}	*Conway*$_1$, *Fischer*$_3$, *Janko*$_4$	$L_{10}(3), O_{13}(3)$ $S_{12}(3)$	$U_{10}(5), O_{13}(5)$ $S_{12}(5)$	$L_8(7)$
2^{41}	*Fischer*$_4$	$L_{18}(3), O^-_{24}(3)$	$U_{18}(5), O^-_{24}(5)$	
2^{46}	*Monster*	$L_{20}(3), O^+_{26}(3)$ $O^-_{26}(3)$	$U_{20}(5), O^+_{26}(5)$ $O^-_{26}(5)$,	$U_{13}(7)$

Department of Mathematics, The Ohio State University, Columbus, Ohio 43210, USA.

E-mail address : **haradako@math.ohio-state.edu**

27-dimensional representations of $3.O(7,3), 3.F_{22}, 3.{}^2E_6(2)$.

北詰 正顕 (Masaaki Kitazume)

千葉大 理学部 数学・情報数理学科

いつも24次元の話（Mathieu群やConway群）の話ばかりしているので，今回は気分を変えて27次元の話をしようと思う。表題の３つの群には，包含関係

$$3.O(7,3) < 3.F_{22} < 3.{}^2E_6(2)$$

が良く知られており，これらが $\mathbb{F}_4$ 上の27次元既約表現を持つことと合わせて，ATLASに事実だけ記されている。${}^2E_6(2)$ はBaby Monster BM の位数２の元の中心化群に現れる群で，その重要性も高いと思われる。（ただし，その場合は位数３の中心は出てこないので，今回の話が直接関わるわけではない。）いくつかの重要な仕事もすでに残っていて，$3.{}^2E_6(2)$ についてはAschbacher [1] の仕事がその中核であり，歴史的にはDickson [6] の２０世紀初頭の仕事にさかのぼる。筆者も以前から少し関わっていて，$3.\Omega(7,3)$ に対するConway-Norton代数に関する結果[9]の他，今回の話の第１歩が代数的組合せ論研究集会の報告集[10]に残っている。その第１歩のきっかけとなったのは，Griessの仕事[8]である。

さて，のっけから言い訳めいた話を書くが，今回の講演の申し込みをした頃には，前述の文献に現れてこない F_{22} を主体にして話をするつもりであった。そこに計算ミスが存在することに気付いたのは集会の直前になってからで，従って，話の内容は修正されて F_{22} が出てこない話になってしまったのであるが，それでもなお「２７次元の有限群論」は面白い内容を含んでいると言って良いと思うので，その概要を記録しておこうと思う。詳しくは文献[11]をごらん戴きたい。

1 $W(E_6)$ $(27 = 63 - 36)$

表題のかっこの中の等式が，27という数字の意味をよく表している。63,36は，それぞれ E_7, E_6 型のルート系に含まれる positive roots の個数である。ルートの ± 1 倍を同一視して数えたものと言っても良い。このとき27は $E_7 \setminus E_6$ の positive roots の個数となって，ワイル群 $W(E_6)$ が置換群として作用することがよくわかる。

ここには，ルートが直交しないときに結ぶという定義によって，グラフの構造が入る。これは Schläfli graph として知られている。このグラフには3点からなる三角形が存在し，それも任意の結ばれた2点に対してただ一つ存在（x, y に対し $\{x, y, x+y\}$）するからそれを "line" として構造をとらえた方が分かり易い。純組合せ論的に表現すると，27 点を

$$a_i, b_j, c_{kl}\ (1 \leq i, j, k, l \leq 6, k < l)$$

として与えれことにすれば $(27 = 6 + 6 + 15)$，全ての lines は

$$\{a_i, b_j, c_{ij}\},\ \{c_{ij}, c_{kl}, c_{mn}\}$$

という集合全体となる。ただし，ここで用いた添え字は全て相異なるものとする。

2 Dickson's trilinear form

前節で述べた，$W(E_6)$ の 27 次置換表現から，より代数的な構造を作り出すと，さらに大きな群が作用するものになる。Dickson [6] の trilinear form として知られているもので，近年になって Aschbacher [1] によって詳しく調べられている。一般の体で定義出来るのだが，ここでは簡単のため 4 元体 $\mathbb{F}_4$ で述べることにする。以下，$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ という記号を用いる。

前節の 27 点で生成される $\mathbb{F}_4$ 上の 27 次元ベクトル空間 V を考える。V 上の対称な trilinear form を

$$\begin{aligned} f(a_i, b_j, c_{ij}) &= 1, \\ f(c_{ij}, c_{kl}, c_{mn}) &= 1. \end{aligned}$$

で定める。上記以外の基底の組み合わせでは f の値は 0 とし，V 全体へは線型に拡張するのである。このとき，自己同型群 $\mathrm{Aut}(V, f)$ (V の線型変換で f を不変にするもの全体) について次が成り立つ。

$$\mathrm{Aut}(V, f) \cong 3.E_6(2^2).2.$$

さらに，基底 a_i, b_j, c_{kl} たちを正規直交基底とするような hermitian form を h と表すとき，f に加えて h をも不変にする自己同型群として twisted type の群が得られる。

$$\mathrm{Aut}(V, f, h) \cong 3.{}^2E_6(2).$$

以上については Aschbacher [1] を参照いただきたい。

なお，一般の体の場合は V の基底について

$$c_{ij} = -c_{ji}$$

と定める必要がある。標数 2 ならば，この符号の問題が起こらずに記述が簡単になるのである。

3 Griess による記述 $(27 = 3^3)$

先に 27 という数字の解釈を示したが，明らかに 3^3 と見ることが自然であろう。実際そうであることを示したのが Griess [8] である。

3 元体 $\mathbb{F}_3$ 上の 3 次元ベクトル空間 $\mathbb{F}_3{}^3$ を考え，ベクトル $x = (x_1, x_2, x_3)$，$y = (y_1, y_2, y_3)$ に対し $g(x, y)$ を，

$$g(x, y) = (x_1 - y_1)(x_2y_3 - x_3y_2) \ (\in \mathbb{F}_3).$$

と定義する。このとき，$\mathbb{F}_4$ 上の 27 次元のベクトル空間 V の基底として $\mathbb{F}_3{}^3$ を index にもつもの，$\{v_x | x \in \mathbb{F}_3{}^3\}$ がとれて f は

$$f(v_x, v_y, v_z) = \begin{cases} \omega^{g(x,y)} & (\text{if } x + y + z = 0) \\ 0 & (\text{if } x + y + z \neq 0) \end{cases}$$

と表される，というのである。基底の変換を実際に書き下しておこう。以下では，$-1 \in \mathbb{F}_3$ を $\bar{1}$ で表している。

$$\begin{array}{lll}
v_{(000)} = a_1 + b_2 + c_{12} & v_{(001)} = a_4 + b_5 + c_{45} & v_{(00\bar{1})} = c_{15} + c_{24} + c_{36} \\
v_{(010)} = a_2 + b_3 + c_{23} & v_{(011)} = a_5 + b_6 + c_{56} & v_{(01\bar{1})} = c_{14} + c_{26} + c_{35} \\
v_{(0\bar{1}0)} = a_3 + b_1 + c_{13} & v_{(0\bar{1}1)} = a_6 + b_4 + c_{46} & v_{(0\bar{1}\bar{1})} = c_{16} + c_{25} + c_{34} \\
v_{(100)} = \omega a_1 + \omega^2 b_2 + c_{12} & v_{(101)} = \omega^2 a_4 + \omega b_5 + c_{45} & v_{(10\bar{1})} = \omega c_{15} + \omega^2 c_{24} + c_{36} \\
v_{(110)} = a_2 + \omega b_3 + \omega^2 c_{23} & v_{(111)} = \omega^2 a_5 + \omega b_6 + c_{56} & v_{(11\bar{1})} = \omega c_{14} + \omega^2 c_{26} + c_{35} \\
v_{(1\bar{1}0)} = \omega^2 a_3 + b_1 + \omega c_{13} & v_{(1\bar{1}1)} = \omega^2 a_6 + \omega b_4 + c_{46} & v_{(1\bar{1}\bar{1})} = \omega c_{16} + \omega^2 c_{25} + c_{34} \\
v_{(\bar{1}00)} = \omega^2 a_1 + \omega b_2 + c_{12} & v_{(\bar{1}01)} = \omega a_4 + \omega^2 b_5 + c_{45} & v_{(\bar{1}0\bar{1})} = \omega^2 c_{15} + \omega c_{24} + c_{36} \\
v_{(\bar{1}10)} = a_2 + \omega^2 b_3 + \omega c_{23} & v_{(\bar{1}11)} = \omega a_5 + \omega^2 b_6 + c_{56} & v_{(\bar{1}1\bar{1})} = \omega^2 c_{14} + \omega c_{26} + c_{35} \\
v_{(\bar{1}\bar{1}0)} = \omega a_3 + b_1 + \omega^2 c_{13} & v_{(\bar{1}\bar{1}1)} = \omega a_6 + \omega^2 b_4 + c_{46} & v_{(\bar{1}\bar{1}\bar{1})} = \omega^2 c_{16} + \omega c_{25} + c_{34}
\end{array}$$

4 関数 $g(x, y)$

g に関する基本的な関係式として，以下が成り立つ。

(1) $g(x, o) = g(x, x) = g(x, -x) = 0$

(2) $g(x, y) = g(y, x) = g(x, -x - y) = -g(-x, -y)$

(3) $g(x, y) + g(x + y, z) - g(y, z) - g(x, y + z) = \det \begin{pmatrix} x \\ y \\ z \end{pmatrix}$

(4) $g(x, y) + g(x, z) + g(x + y, x + z) = g(y, z) + g(x, y + z) + g(x, x + y + z).$

この g を用いて，Moufang loop と呼ばれる代数系が定義できる。古くから調べられている対象のようで，６０年前の文献 [3] に g の記述があるようである。[2] には，さらに一般的な形で述べられている。

まず，$\mathcal{M} = \mathbb{F}_3 \times \mathbb{F}_3{}^3$ とおき $\mathcal{M}$ 上の演算を，

$$(\alpha, x)(\beta, y) = (\alpha + \beta + g(x, y), x + y)$$

と定義する。この演算は可換で，$(0,0)$ は単位元になり，各 (α, x) は逆元 $(-\alpha, -x)$ を持つが，結合法則は一般に成立しない。しかし，(4) 式は $(ab)(ca) = (a(bc))a$ という関係式を意味していて，$\mathcal{M}$ は commutative Moufang loop と呼ばれる代数構造になっている。

次に $\mathcal{M}$ から 3-transposition group を定義することができる。一般に 3-transposition group とは位数 2 の元で生成され，その異なる 2 つの元の積の位数が 2 または 3 であるような群のことをいうが，ここで現れるのは，積の位数が 2（すなわち，2 元が可換）である場合が起こらないものである。

各 $(\alpha, x) \in \mathcal{M}$ に対し $\mathcal{M}$ 上の置換 $t_{(\alpha,x)}$ を

$$\begin{aligned} t_{(\alpha,x)}(\beta, y) &= (\alpha, x)^{-1}(\beta, y)^{-1} \\ &= (-\alpha - \beta - g(x, y), -x - y) \end{aligned}$$

と定義する。このとき

$$t_{(\beta,y)}{}^{t_{(\alpha,x)}} = t_{\{t_{(\alpha,x)}(\beta,y)\}},$$

であり $\langle t_{\mathcal{M}} \rangle$ は 3-transposition group となる。その生成元 $t_{\mathcal{M}}$ は 81 個からなる。このあたりの Moufang loop から 3-transposition group へのより一般的な記述が [13] にある。

次の重要な関係式は，後で非分裂性の証明に用いられる ([11])。

$$(5)\quad \{t_{(\alpha,x)}t_{(\beta,y)}t_{(\gamma,z)}\}^2(\delta, u) = \left(\begin{vmatrix} x & 1 \\ y & 1 \\ z & 1 \\ u & 1 \end{vmatrix} + \delta,\ u \right).$$

証明は直接計算すればよい。

5 Conway-Norton 代数

Dickson の trilinear form と同様の構造定数で，27×2 次元の Conway-Norton 代数と呼ばれる非結合的可換代数を定義することができる。B を $\mathbb{C}$ 上の 27×2 次元のベクトル空間とするとき，B 上定義される可換代数とは，対称な bilinear map $\tau : B \times B \to B$ を（非結合的な）積と見なすものである。

B の基底は 2 通り考えることができて，それは

$$a_i, b_j, c_{ij}, \bar{a}_i, \bar{b}_j, \bar{c}_{ij},$$

及び

$$v_x, \bar{v}_x \ (x \in \mathbb{F}_3{}^3)$$

というものである。それぞれに対し，τ は，

$$\begin{cases} \tau(a_i,b_j) = \bar{c}_{ij}, & \tau(\bar{a}_i,\bar{b}_j) = c_{ij}, \\ \tau(a_i,c_{ij}) = \bar{b}_{ij}, & \tau(\bar{a}_i,\bar{c}_{ij}) = b_{ij}, \\ \tau(b_j,c_{ij}) = \bar{a}_i, & \tau(\bar{b}_j,\bar{c}_{ij}) = a_i, \\ \tau(c_{ij},c_{kl}) = \bar{c}_{mn}, & \tau(\bar{c}_{ij},\bar{c}_{kl}) = c_{mn}, \end{cases}$$

及び

$$\begin{cases} \tau(v_x,v_y) = \omega^{g(x,y)}\bar{v}_{(-x-y)} \\ \tau(\bar{v}_x,\bar{v}_y) = \omega^{2g(x,y)}v_{(-x-y)} \end{cases}$$

と表される。この二つの基底の関係は，前の場合と全く同様である。

全自己同型群 $G = \mathrm{Aut}(\mathcal{B},\tau)$ は $3.\Omega(7,3).2$ という形である。群構造についてもう少し詳しく書いておくと，

$$G' = G'', [G:G'] = 2, |Z(G')| = 3, |Z(G)| = 1$$

が成り立つ。特に中心拡大 $G' = 3.\Omega(7,3)$ は非分裂である。

この群の非分裂性を，先の (5) 式を用いて示すことができる。[10] の繰り返しになるが，その概略を記しておこう。

各 $x \in \mathbb{F}_3{}^3$ に対し，$\mathrm{Aut}(\mathcal{B},f)$ の元 e_x を

$$e_x(v_y) = \tau(v_x,v_y), \quad e_x(\bar{v}_y) = \tau(\bar{v}_x,\bar{v}_y).$$

と定義することができる。これは $G\backslash G'$ の位数2の元で，$\zeta^{e_x} = \zeta^{-1}$ ゆえ $e_x{}^{\zeta} = \zeta e_x$ となる。従って，

$$(\zeta^{\alpha}e_x)^{(\zeta^{\beta}e_y)} = \zeta^{-\alpha-\beta-g(x,y)}e_{(-x-y)}.$$

が成り立ち，(5) 式から

$$(\zeta^{\delta}e_u)^{\{(\zeta^{\gamma}e_z)(\zeta^{\beta}e_y)(\zeta^{\alpha}e_x)\}^2} = \zeta^{m+\delta}e_u,\ m = \begin{vmatrix} x & 1 \\ y & 1 \\ z & 1 \\ u & 1 \end{vmatrix}$$

を得る。

さて G が分裂するなら，その補群は各剰余類 $Z(G')e_x$ の元を丁度1つずつ含んでいることになるが x,y,z,u のとり方で $m \neq 0$ となるということは，そのような補群が存在しないことを意味している。従って G は分裂しない。

6 $3.\Omega(7,3) \subset 3.^2E_6(2)$

さて表題の2つの群を振り返ると，同じ様な形で27あるいは27×2次元の表現が構成されているわけである。そこから，この包含関係は見て取れないのだろうか。実は，それは難しいことではない。

$G = \mathrm{Aut}(B, \tau)$ の作用を詳しく調べてみると，作用の係数が $\mathbb{Z}[\omega, \frac{1}{3}]$ に入ることがわかる。従って，mod2 で考えることが出来て，この表現は $\mathbb{F}_4$ で実現されることがわかる。さらに，交換子群 $G' \cong 3.\Omega(7,3)$ は，

$$a_i, b_j, c_{ij}$$

で生成される27次元空間に作用することもわかっている。この空間を U とおく。U 上で定義される trilinear form f と hermitian form h を G' が不変にすることを示し，問題の包含関係を導こうというわけである。

G の B への作用においては，Smith [14] により，次のような symmetric bilinear form を不変にすることがわかっている。

$$\langle a_i, \bar{a}_i \rangle = \langle b_i, \bar{b}_i \rangle = \langle c_{ij}, \bar{c}_{ij} \rangle = 1, \tag{1}$$

これを用いて trilinear form f^* を

$$f^*(u, v, w) := \langle u, \tau(v, w) \rangle.$$

と定義すれば，G' は f^* を不変にする。そして，

$$\begin{aligned} f^*(a_i, b_j, c_{ij}) &= \langle a_i, \tau(b_j, c_{ij}) \rangle = \langle a_i, \bar{a}_i \rangle = 1, \\ f^*(c_{ij}, c_{kl}, c_{mn}) &= \langle c_{ij}, \tau(c_{kl}, c_{mn}) \rangle = \langle c_{ij}, \bar{c}_{ij} \rangle = 1. \end{aligned}$$

という計算から $f^* = f$ が示される。なお

$$f^*(a_i, a_i, a_i) = f^*(b_i, b_i, b_i) = f^*(c_{ij}, c_{ij}, c_{ij}) = 2$$

であるから，標数が2であることが効いている。

最後に hermitian form h を $\langle \cdot, \cdot \rangle$ を用いて，

$$h(u, v) := \langle u, \bar{v} \rangle$$

と定義する。ただし，$\bar{v}$ とは，U の基底 a_i, b_j, c_{ij} を $\bar{a}_i, \bar{b}_j, \bar{c}_{ij}$ にそれぞれ替え，係数を $\mathbb{F}_4$ の自己同型 $(\omega \leftrightarrow \omega^2)$ で移すことで得られる B の元である。これが G' 不変であることも容易に示される。以上で，

$$3 \cdot \Omega(7,3) \subset 3 \cdot {}^2E_6(2)$$

が示された。この包含関係については，[4] にも記述がある。

さて，この節で最初に述べたことによれば，(B,τ) を $\mathbb{F}_4$ 上で考えることが出来る。その自己同型群は，何になるのだろうか。冒頭で言い訳を書いた「計算ミス」は，ここに起こっていたのであり，自己同型群が $3.F_{22}$ であると期待する余り，そうであるという間違いを信じてしまったのであった。間違いを修正した結果，自己同型群はもっと大きくなることがわかったが，正確な決定はまだしていない。

7 非分裂拡大 $3^7.\Omega(7,3).2$

今回の話の流れの一つとして，表題の群の構成がある。これは，Fischer の最大の 3-transposition group F_{24} に極大部分群として含まれる群である。講演時には一言ふれることしかできなかったが，この機会に紹介しておこう。

本節の最後に $g(x,y)$ が再び登場し，全てが解決するところにご注目いただければ幸いである。

7.1 直交群 $\Omega(7,3):2$

ここで，改めて直交群 $\Omega(7,3):2$ について述べておくことにする。

V を3元体 $\mathbb{F}_3$ 上の7次元ベクトル空間とする。V 上の内積を

$$\langle x,y\rangle = x_1y_1 + \cdots + x_7y_7,\ x=(x_1,\ldots,x_7), y=(y_1,\ldots,y_7)$$

と定め，各 $x\in V$ に対し，鏡映 r_x を

$$r_x(y) := y - \frac{2\langle x,y\rangle}{\langle x,x\rangle}x$$

と定義する。($r_x = r_y \Leftrightarrow y\in\{x,-x\}$ に注意されたい。) 特に，ノルム -1 の元に関する鏡映だけを考えることにして，

$$V^- = \{x\in V \mid \langle x,x\rangle = -1\},\ C = \{r_x \mid x\in V, \langle x,x\rangle = -1\}.$$

とおく。このとき，C で生成される群を G とおけば，

$$|G:G'| = 2, G'\cong\Omega(7,3)$$

が成立する。ベクトル x が V^- に入るということは，その0でない成分が2つか5つであることを意味し，$|C| = 378$ であることも容易にわかる。C は G の 3-transpositions の共役類になる。すなわち，

$$|r_xr_y| = \begin{cases} 1 & \text{if } x=\pm y \\ 2 & \text{if } \langle x,y\rangle = 0 \\ 3 & \text{if } \langle x,y\rangle\neq 0, x\neq\pm y. \end{cases}$$

が成立する。

7.2 関数 φ

次に重要な関数 φ を定義する。定義自体は単純で，$x, y \in V^-$ に対し

$$\varphi(x,y) := \begin{cases} 0 & \text{if } \langle x,y\rangle = 0, \\ \prod_{y_i=0} x_i \prod_{y_j \neq 0} y_j & \text{if } \langle x,y\rangle \neq 0. \end{cases}$$

とするだけである。

実を言うと，これが何なのかがよくわからない。以下では，いくつかの補題をつないで目的の群の構成ができるのだが，補題の証明は case-by-case で，理屈がわかるわけではないのである。

ただ，φ の値は座標の置換と，偶数個の符号 $(\pm)$ の変換（これらは Weyl 群 $W(D_7)$ を生成する）に関して不変なので，これを用いて場合分けを少なくすることはできる。また定義から，x, y が直交している場合と，共通して 0 となる座標が存在するなら $\varphi(x,y) = 0$ である。従って，x, y の一方でもその 0 でない成分が 2 個であるなら，$\varphi(x,y) = 0$ である。このことは，先にも注意した $x \in V^-$ の 0 でない成分は 2 つか 5 つであることから容易にわかる。このことからも φ が 7 という次元に深く依存していることがわかると思う。

以下 φ に関する基本性質を並べておこう。

補題 7.1. $x, y \in V^-$ に対し，

(1) $\varphi(x,y) = \varphi(-x,y) = -\varphi(x,-y) = -\langle x,y\rangle\varphi(y,x)$

(2) $\varphi(x,y) = -\varphi(x, r_x(y)) = -\varphi(y, r_y(x))$

(証明) $W(D_7)$ の作用を用いると，$x = (1,1,1,1,1,0,0), y = (1,\bar{1},\bar{1},0,0,1,\pm 1)$ として良い。以下は容易な計算。 □

補題 7.2. $x, y, z \in V^-$ が $\langle x,y\rangle = \langle y,z\rangle = -1$, $\langle x,z\rangle = 0$ をみたすとき，

$$\varphi(x,y) + \varphi(x+y,z) = \varphi(y,z) + \varphi(x,y+z).$$

が成り立つ。

(証明) これも，具体的に計算するのだが，少し複雑なので詳細は省く。

$$x = (1,1,1,1,1,0,0), y = (1,\bar{1},\bar{1},0,0,1,\pm 1).$$

としてよく，例えば $y = (1,\bar{1},\bar{1},0,0,1,1)$ の場合，$z = (z_1, \ldots, z_7)$ とおけば，示すべき式は

$$z_2 z_3 + z_4 z_5 + z_6 z_7 + z_6 + z_7 = 0.$$

となり，可能な z (81 通り) に対して，これを確かめれば良い。一例として $z = (0,1,\bar{1},\bar{1},1,\bar{1},0)$ として計算されたい。 □

7.3 $3^7 \cdot \Omega(7,3) : 2$ の構成

集合 $V^- \times \mathbb{F}_3$ を考える。ただし，同値関係 $\sim$ を

$$(x,\alpha) \sim (-x,-\alpha) \quad (x \in V^-, \alpha \in \mathbb{F}_3)$$

と定めて，このふたつを同一視し，

$$D := (V^- \times \mathbb{F}_3)/\sim$$

と定義する。ただし簡単のため，その同値類を表すのに特別な記号は用いず D の元を単に (x,α) と表す。

目的の群は D 上の置換群として構成される。その生成元は D を index に持つように定義される。すなわち，$(x,\alpha) \in D$ に対し D 上の置換を

$$p(x,\alpha) : (y,\beta) \mapsto (y,\beta)^{p(x,\alpha)} := (r_x(y), \varphi(x,y) - \langle x,y\rangle\alpha + \beta).$$

と定める。ここで $p(x,\alpha)$ は well-defined （すなわち $p(-x,-\alpha) = p(x,\alpha)$ ）であることが，

$$\begin{aligned}(y,\beta)^{p(-x,-\alpha)} &= (r_{-x}(y), \varphi(-x,y) - \langle -x,y\rangle(-\alpha) + \beta) \\ &= (y,\beta)^{p(x,\alpha)}.\end{aligned}$$

によりわかる。さらに，補題 7.1 を用いた簡単な計算

$$\begin{aligned}(y,\beta)^{p(x,\alpha)^2} &= (r_x(y), \varphi(x,y) - \langle x,y\rangle\alpha + \beta)^{p(x,\alpha)} \\ &= ({r_x}^2(y), \varphi(x, r_x(y)) - \langle x, r_x(y)\rangle\alpha + \varphi(x,y) - \langle x,y\rangle\alpha + \beta) \\ &= (y,\beta),\end{aligned}$$

から $p(x,\alpha)$ が位数 2 であることも示される。

目的の群 G^* を

$$G^* := \langle\, p(x,\alpha) \,|\, (x,\alpha) \in D \,\rangle$$

として定義する。目標は

定理 7.3. *$G^* \cong 3^7.\Omega(7,3).2$ (non-split).*

を示すことである。

G^* の位数 3^7 の（基本可換）正規部分部分群の定義は難しくない。$v \in V$ に対し D 上の置換を

$$\Delta(v) : (y,\beta) \mapsto (y, \beta + \langle y,v\rangle)$$

と定義して

$$X := \langle \Delta(v) \,|\, v \in V \,\rangle$$

とおく。$\Delta(v)$ 達は

$$\Delta(v)\Delta(u) = \Delta(v+u)$$

を満たすことが容易にわかるので，X はベクトル空間 V と同型な基本可換群を生成する。この群 X が G^* に含まれることは次節の補題から示されることである。

次節において，主定理の証明の概略を述べようと思う。

7.4 証明の概略

証明は以下のような補題の積み重ねによる。

補題 7.4. $(x,\alpha),(y,\beta) \in D$ に対し

$$(y,\beta)^{p(x,\alpha)} = \begin{cases} (y,\beta) & (\text{if } \langle x,y\rangle = 0) \\ (x,\alpha)^{p(y,\beta)} & (\text{if } \langle x,y\rangle \neq 0) \end{cases}.$$

(証明) x,y が直交する場合は易しい。そうでないときは，$\langle x,y\rangle = -1$ としてよく，このとき両辺は

$$(y,\beta)^{p(x,\alpha)} = (r_x(y), \varphi(x,y) + \alpha + \beta)$$

と

$$\begin{aligned} (x,\alpha)^{p(y,\beta)} &= (r_y(x), \varphi(y,x) + \beta + \alpha) \\ &= (r_x(y), \varphi(x,y) + \beta + \alpha), \end{aligned}$$

となって一致する。 □

補題 7.5. $(x,\alpha) \in D$ に対し

$$\Delta(x) = p(x,\alpha)p(x,\alpha+1)$$

が成り立つ。特に X は G^* の部分群である。

(証明) 上の補題を用いて，

$$\begin{aligned} (y,\beta)^{p(x,\alpha)p(x,\alpha+1)} &= (r_x(y), \varphi(x,y) - \langle x,y\rangle\alpha + \beta)^{p(x,\alpha+1)} \\ &= (r_x{}^2(y), \varphi(x,r_x(y)) - \langle x,r_x(y)\rangle(\alpha+1) + \varphi(x,y) - \langle x,y\rangle\alpha + \beta) \\ &= (y, -\langle x,r_x(y)\rangle + \beta) \\ &= (y, \langle x,y\rangle + \beta), \end{aligned}$$

となる。 □

補題 7.6. $p(y,\beta)^{p(x,\alpha)} = p((y,\beta)^{p(x,\alpha)})$.

この補題がいわゆる Key Lamma である。ところが，この証明は難しい。この補題さえ得られれば，次の補題は容易に得られる。

補題 7.7. $\Delta(y)^{p(x,\alpha)} = \Delta(r_x(y))$.

(証明) $\langle x, y\rangle = -1$ と仮定して良く，そのとき

$$\begin{aligned}\Delta(y)^{p(x,\alpha)} &= \{p(y,0)p(y,1)\}^{p(x,\alpha)} \\ &= p(x+y, \varphi(x+y)+\alpha)p(x+y, \varphi(x+y)+\alpha+1) \\ &= \Delta(x+y) = \Delta(r_x(y)),\end{aligned}$$

が得られる。 □

この補題により，$p(x,\alpha)$ たちの X への作用は reflection としてのものであると考えて良いことがわかる。詳細は省略するが，このことから

$$G^*/X \cong \Omega(7,3).2$$

であることが導かれるのである。

補題 7.6 の証明は，両辺の (z,γ) への作用が等しいこと

$$(z,\gamma)^{p(y,\beta)p(x,\alpha)} = (z,\gamma)^{p((y,\beta)p(x,\alpha))}. \tag{2}$$

を示すことを目標にする。当然 x, y, z の関係による場合分けが必要になる。例えば $\langle x, y\rangle = 0$ と仮定した場合は比較的簡単にすむ。多くの場合，補題 7.2 に帰着される。最も複雑かつ重要なのは，

$$\langle x, y\rangle = \langle x, z\rangle = \langle y, z\rangle = -1$$

という場合である。この場合，$x-y, x-z$ が 2 次元の totally isotropic subspace を張る。それらを含む極大（3 次元）な totally isotropic subspace W をとる。これは，例えば

$$a = (1,1,1,0,0,0,0), b = (0,0,0,1,1,1,0), c = (0,0,0,0,1,\bar{1},1),$$

$$x = (1,\bar{1},0,0,0,0,0), y = x+a, z = x+b$$

として良い。このとき

$$\{v \in V \mid \langle v, v\rangle = -1, \langle v, w\rangle = 0\,(\forall w \in W)\} = \{\pm x + w_1 a + w_2 b + w_3 c \mid w_i \in \mathbb{F}_3\}.$$

となる。

ここで，3 節に現れた関数 g に再登場を願うのである。すなわち，$w = w_1 a + w_2 b + w_3 c, v = v_1 a + v_2 b + v_3 c$ に対し

$$g^*(w,v) := g((w_1,w_2,w_3),(v_1,v_2,v_3)) = (w_1 - v_1)(w_2 v_3 - w_3 v_2).$$

と定義する。

補題 7.8. 任意の $w, v \in W$ に対し

$$\varphi(x+w, x+v) = g^*(w, v).$$

特に

$$(x+v, \beta)^{p(x+w,\alpha)} = (x-w-v, -g^*(w,v) - \alpha - \beta).$$

(証明) この証明もまた，全ての場合を尽くして等式を確かめるのである。例えば，

$$x+a+b = (\bar{1}, 0, 1, 1, 1, 1, 0), x+c = (1, \bar{1}, 0, 0, 1, \bar{1}, 1),$$

については，

$$\varphi(x+a+b, x+c) = 1,$$

であり

$$g^*(a+b, c) = (1-0)(1 \times 1 - 0 \times 0) = 1,$$

であるから両者は確かに一致している。 □

この補題により，問題の補題 7.6 は容易に示される。

このように議論は十分整理されていると思うのだが，証明は直接計算の繰り返しで，φ が何であるのか全くわからないのである。

この段階で，G^* が非分裂であることも，5節と同様に示される。ちょうど今使った記号 W, a, b, c, x を用いる。このとき，$w = w_1a + w_2b + w_3c, v = v_1a + v_2b + v_3c$, $u = u_1a + u_2b + u_3c, t = t_1a + t_2b + t_3c$. とすれば，補題 7.8 により，

補題 7.9. $$(t, \delta)^{\{p(w,\alpha)p(v,\beta)p(u,\gamma)\}^2} = \left(t, \begin{vmatrix} w_1 & w_2 & w_3 & 1 \\ v_1 & v_2 & v_3 & 1 \\ u_1 & u_2 & u_3 & 1 \\ t_1 & t_2 & t_3 & 1 \end{vmatrix} + \delta \right).$$ □

が得られる。

もし，G^* における X の補群 K が存在するならば，K は各 x に対し $p(x, \alpha), \alpha = 0, 1, -1$ のいずれかひとつを含むはずである。補題 7.9 は，それが不可能なことを示している。

参考文献

[1] M. ASCHBACHER, The 27-dimensional module for E_6, I, *Invent. Math.* **89** (1987), 159–195.

[2] L. BÉNÉTEAU, Commutative Moufang loops and related groupoids, in "Quasigroups and Loops: Theory and Applications" (O. Chein, H. O. Pflugfelder and J. D. H. Smith, ed.), Heldermann, Berlin, 1991, 115–142.

[3] G. BOL, Gewebe und Gruppen, *Math. Ann.* **114** (1937) 414–431.

[4] V.P.BURICHENKO, On a special loop, the Dickson form, and the lattice connected with $O_7(3)$, *Math. USSR Sbornik*, **74** (1993), No.1, 145–167.

[5] O. CHEIN, Examples and methods of construction, in "Quasigroups and Loops: Theory and Applications" (O. Chein, H. O. Pflugfelder and J. D. H. Smith, ed.), Heldermann, Berlin, 1991, 27–93.

[6] L. DICKSON, A class of groups in arbitrary realm connected with the configuration of the 27 lines on a cubic surface, *Quarterly J. Math.* **33** (1901), 145–173.

[7] R.L.GRIESS, The Friendly Giant, *Invent. Math.* **69** (1982), 1–102.

[8] R.L.GRIESS, A Moufang loop, the Exceptional Jordan Algebra and a Cubic form in 27 Variables, *J. Algebra* **131-1** (1990),281–293.

[9] M.KITAZUME, The Conway-Norton algebras for $\Omega^-(6,3), \Omega(7,3), F'_{24}$, and their full automorphism groups, *Invent. Math.* **88** (1987), 277–318.

[10] 北詰正顕, Griess の関数と直交群の非分裂拡大, 1992 年 6 月, 代数的組合せ論シンポジウム (岐阜大学教養部)

[11] M.KITAZUME, Some Non-split Extensions of the Orthogonal Group $\Omega(7,3)$, to appear in *Journal of Algebra.*

[12] A.S.KÜSEFOGLU, The second cohomology of finite orthogonal groups, I, *J. Algebra* **56**(1979), 207–220.

[13] YU.I.MANIN, Cubic forms, North-Holland, Amsterdam, 1973.

[14] S.D.SMITH, Nonassociative commutative algebras for triple covers of 3-transposition groups, *Michigan J. Math.* **24** (1977), 273–287.

DEFORMING THE CATEGORIES OF REPRESENTATIONS OF SOME SEMI-DIRECT PRODUCT GROUPS

D. TAMBARA

Department of Mathematical System Science,
Hirosaki University, Hirosaki 036-8561, Japan

1. 3-COCYCLE DEFORMATION

Let k be the complex field. With a finite group G associated are two algebras: the group algebra $k[G]$ and the function algebra $k(G) := \mathrm{Map}(G, k)$. These are Hopf algebras dual to each other. Modules over each of the algebras can be tensored so that they form a tensor category. Denote the category of $k[G]$-modules by $\mathrm{Rep}(G)$ and the category of $k(G)$-modules by $\mathrm{Vect}[G]$. We are concerned about deformations of these tensor categories.

Look at $\mathrm{Vect}[G]$ first. A $k(G)$-module is a G-graded vector space $V = \bigoplus_{\sigma \in G} V_\sigma$, and the tensor product $W = U \otimes V$ of two modules U and V is graded as

$$W_\sigma = \bigoplus_{\sigma = \tau\rho} U_\tau \otimes V_\rho.$$

Simple modules are one-dimensional. They are labeled as $[\sigma]$ for $\sigma \in G$ so that

$$[\sigma]_\tau = \begin{cases} k & \text{if } \sigma = \tau, \\ 0 & \text{if } \sigma \neq \tau. \end{cases}$$

Then $[\sigma] \otimes [\tau] = [\sigma\tau]$.

If $\alpha\colon G \times G \times G \to k^\times$ is a 3-cocycle, $\mathrm{Vect}[G]$ is deformed to a tensor category $\mathrm{Vect}[G, \alpha]$. This has the same objects, morphisms, and tensor products as $\mathrm{Vect}[G]$. The only difference is in the associativity isomorphisms $(X \otimes Y) \otimes Z \to X \otimes (Y \otimes Z)$, which are a part of the structure of a tensor category. In $\mathrm{Vect}[G]$, the associativity $([\sigma] \otimes [\tau]) \otimes [\rho] \to [\sigma] \otimes ([\tau] \otimes [\rho])$ is the identity map on $[\sigma\tau\rho]$, while in $\mathrm{Vect}[G, \alpha]$ it is multiplication by the scalar $\alpha(\sigma, \tau, \rho)$. The pentagon axiom that the results of two ways of composition of associativity isomorphisms from $((X \otimes Y) \otimes Z) \otimes W$ to $X \otimes (Y \otimes (Z \otimes W))$ should be equal amounts to the cocycle condition for α.

Conversely, any tensor category with the same underlying category and the same tensor product operation as $\mathrm{Vect}[G]$ is of the form $\mathrm{Vect}[G, \alpha]$. Thus deformations of $\mathrm{Vect}[G]$ in such a sense are classified by the group $H^3(G, k^\times)$.

Our interest here is

Problem. How one can obtain deformations of $\mathrm{Rep}(G)$?

If G is abelian, then $\mathrm{Rep}(G) = \mathrm{Vect}[\hat{G}]$ with $\hat{G} = \mathrm{Hom}(G, k^\times)$, so we have the answer. For non-abelian groups, no general procedure of deformation seems to be known. Some constructions are dealt with by Yamagami [Y]. In the next section, we will give deformations for groups having abelian normal subgroups.

2. CENTRAL EXTENSIONS AND SEMI-DIRECT PRODUCTS

If K is a central subgroup of G, the irreducible characters of G are partitioned according to their restrictions to K. So the category $\mathcal{C} = \mathrm{Rep}(G)$ has a decomposition

$$\mathcal{C} = \bigoplus_{\lambda \in \hat{K}} \mathcal{C}_\lambda,$$

where $\hat{K} = \mathrm{Hom}(K, k^\times)$ and for $\lambda \in \hat{K}$

$$\mathcal{C}_\lambda = \{G\text{-modules on which } K \text{ acts through } \lambda\}.$$

If $X \in \mathcal{C}_\lambda$ and $Y \in \mathcal{C}_\mu$, then $X \otimes Y \in \mathcal{C}_{\lambda\mu}$. Thus we may say $\mathcal{C}$ has a $\hat{K}$-grading.

If $\alpha\colon \hat{K}^3 \to k^\times$ is a 3-cocycle, $\mathcal{C}$ is deformed to a tensor category $\mathcal{C}^\alpha$ in a similar manner to the case of Vect[G]. Namely, we let the associativity isomorphism $(X \otimes Y) \otimes Z \to X \otimes (Y \otimes Z)$ in $\mathcal{C}^\alpha$ for $X \in \mathcal{C}_\lambda$, $Y \in \mathcal{C}_\mu$, $Z \in \mathcal{C}_\nu$ to be the scalar multiplication by $\alpha(\lambda, \mu, \nu)$.

Example 2.1. Let $G = D_8$, the dihedral group of order 8, and $K = Z(G) = Z_2$. Then $H^3(\hat{K}, k^\times) \cong Z_2$. Take a non-coboundary 3-cocycle α of $\hat{K}$. Then it turns out that $\mathcal{C}^\alpha \cong \mathrm{Rep}(Q_8)$.

Example 2.2. Let $G = SL(2, q)$ with q odd and $K = Z(G) = \{\pm 1\}$. Let α be as above. Then it can be shown that the twisted category $\mathcal{C}^\alpha$ is equivalent to the module category for a Hopf algebra different from group algebras.

Next we consider a situation in which a group G acts on a group L. Details are omitted here. Form the semi-direct product LG. Let ρ be a 3-cocycle of LG which restricts to a coboundary of G. Put $\theta = \rho|L$. We have the category Vect[L, θ] and ρ gives rise to an action of G on Vect[L, θ]. Then we have the tensor category Vect$[L, \theta]^G$ of G-invariant objects in Vect[L, θ]. If L is abelian and $|L|$, $|G|$ are coprime, Vect$[L, \theta]^G$ is a deformation of Rep($\hat{L}G$).

Example 2.3. Let $L = Z_3$, $G = Z_2$ and $LG \cong S_3$. We have $\mathrm{Ker}(H^3(LG) \to H^3(G)) \cong H^3(L)^G \cong Z_3$. Correspondingly three deformations of Rep(S_3) (including itself) are obtained. The two nontrivial ones are not representable as module categories over Hopf algebras. Moreover these are the only deformations of Rep(S_3).

Example 2.4. Let $L = Z_2 \times Z_2$, $G = Z_3$ and $LG \cong A_4$. Then $\mathrm{Ker}(H^3(LG) \to H^3(G)) \cong Z_2$. We have one nontrivial deformation of Rep(A_4). This does not come from a Hopf algebra and is the unique nontrivial deformation.

To see the non-representability by Hopf algebras in these examples we make use of the duality considered in [T].

3. EXTRASPECIAL 2-GROUPS

An extraspecial 2-group has a unique irreducible non-linear character m. Let A be the group of linear characters. Then

$$m^2 \cong \sum_{a \in A} a.$$

Tensor categories having such a fusion rule were classified in [TY]. They are parameterized by pairs of nondegenerate symmetric bicharacter $A \times A \to k^\times$ and signs $\pm$. The signs correspond to the two types of extraspecial 2-groups.

4. $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$

The next simplest will be the case where there is a unique non-linear character m and

$$m^2 = Nm + \sum_{a \in A} a$$

with A the group of linear characters and N a positive integer. Such is the group $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$ with $N = q - 2$ and $A = (\mathbb{F}_q^\times)\hat{}$. Stating formally,

Problem. Classify semi-simple tensor categories of which the set of simple objects is a disjoint union $A \cup \{m\}$ of a group A and a one-point set $\{m\}$, and the fusion rule is

$$a \otimes b \cong ab,$$
$$a \otimes m \cong m, \quad m \otimes a \cong m$$
$$m \otimes m \cong \underbrace{m \oplus \cdots \oplus m}_{N} \oplus \bigoplus_{a \in A} a$$

for $a, b \in A$ with $N \in \mathbb{N}$.

At present we have a few results for small values of N.

- If $N = 1$, there are just three such categories. They are $\mathrm{Rep}(S_3)$ and their twists in Example 2.3.
- If $N = 2$, there are just two such categories. They are $\mathrm{Rep}(A_4)$ and their twist in Example 2.4.
- If $N = 6$, there is such a category other than $\mathrm{Rep}(\mathbb{F}_8 \rtimes \mathbb{F}_8^\times)$.

In the course, we obtained a result on reconstruction of a finite field from its multiplicative group and the fractional transformation $x \mapsto 1 - 1/x$ (Theorem below).

Let us explain our approach in some detail. Let $\mathcal{C}$ be a tensor category as above. First look at the associativity

$$(a \otimes m) \otimes b \cong a \otimes (m \otimes b)$$

for $a, b \in A$. By the fusion rule the both sides are isomorphic to m. Thus we have an automorphism of the simple object m, which must be a nonzero scalar denoted by $\alpha(a, b)$. The pentagon identities for $a \otimes a' \otimes m \otimes b$ and $a \otimes m \otimes b \otimes b'$ tell us that $\alpha\colon A \times A \to k^\times$ is a bicharacter.

Secondly the associativity

$$(m \otimes a) \otimes m \cong m \otimes (a \otimes m)$$

for $a \in A$ yields an automorphism of the object

$$Vm \oplus \bigoplus_{a} a,$$

where $V = k^N$ and $Vm = m \oplus \cdots \oplus m$ (N-times). Taking the m-component, we have a linear automorphism of V, denoted by $a\cdot$. Considering the pentagon identity for $m \otimes a \otimes a' \otimes m$, we know the map $A \to GL(V)\colon a \mapsto a\cdot$ is a homomorphism. Thus we obtain a representation of A on the space V.

Thirdly the associativity

$$(m \otimes m) \otimes m \cong m \otimes (m \otimes m)$$

yields an automorphism of the object

$$(VV \oplus \bigoplus_{a \in A} k)m \oplus \bigoplus_{b \in A} Vb,$$

where we omit $\otimes$ for vector spaces. Taking its components, we obtain linear maps

$$\begin{aligned} \gamma(m,m)&: VV \to VV \\ \gamma(m,a')&: VV \to k \\ \gamma(a,m)&: k \to VV \\ \gamma(a,a')&: k \to k \\ \gamma(b)&: V \to V \end{aligned}$$

for $a, a', b \in A$.

In the case where $\mathcal{C} = \mathrm{Rep}(F \rtimes F^\times)$ with $F = \mathbb{F}_q$, we have $A = (F^\times)\hat{}$, $\alpha \equiv 1$ and the representation of A on V is the regular minus trivial. So V has a basis $\{(x) \mid x \in \hat{A} - \{1\} = F - \{0,1\}\}$ so that $a \cdot (x) = \langle a, x \rangle (x)$ for $a \in A$. With this basis the above maps are represented as

$$\gamma(m,m)\colon (x) \otimes (y) \mapsto \begin{cases} ((1-\frac{1}{x})y) \otimes (x+y-xy) & \text{if } \frac{1}{x}+\frac{1}{y} \neq 1 \\ 0 & \text{if } \frac{1}{x}+\frac{1}{y} = 1 \end{cases}$$

$$\gamma(m,1)\colon (x) \otimes (y) \mapsto \begin{cases} 1 & \text{if } \frac{1}{x}+\frac{1}{y} \neq 1 \\ 0 & \text{if } \frac{1}{x}+\frac{1}{y} = 1 \end{cases}$$

$$\gamma(1,m) : 1 \mapsto \frac{1}{q-1} \sum_{x+y=1} (x) \otimes (y)$$

$$\gamma(1,1) : 1 \mapsto \frac{1}{q-1}$$

$$\gamma(1)\colon (x) \mapsto (1-\tfrac{1}{x})$$

for $x, y \in F - \{0,1\}$. The pentagon diagram for $m \otimes m \otimes m \otimes m$ reflects the property for the partial map

$$\begin{aligned} \omega\colon F \times F &\to F \times F \\ (x,y) &\mapsto ((1-\tfrac{1}{x})y, x+y-xy) \end{aligned}$$

to make the commutative hexagon

$$\begin{array}{ccc} & F \times F \times F & \\ {\scriptstyle \omega \times 1}\swarrow & & \searrow{\scriptstyle 1 \times \omega} \\ F \times F \times F & & F \times F \times F \\ {\scriptstyle 1 \times \omega}\downarrow & & \downarrow{\scriptstyle T \times 1} \\ F \times F \times F & & F \times F \times F \\ {\scriptstyle \omega \times 1}\searrow & & \swarrow{\scriptstyle 1 \times \omega} \\ & F \times F \times F & \end{array}$$

where T: $(x,y) \mapsto (y,x)$.

Because of difficulty of carrying on classification in full generality, I make here the following assumptions, which are satisfied in the above case.

- A is abelian.
- $\alpha \equiv 1$.
- The representation of A on V is the sum of all nontrivial one-dimensional representations without multiplicity.
- $\gamma(1,1) \neq 0$.

Put $X = \hat{A} - \{1\}$. Then V has a basis $\{(x) \mid x \in X\}$ so that the action of $a \in A$ is given by $a \cdot (x) = \langle a, x \rangle (x)$. The maps $\gamma(m,m), \ldots$ will be expressed as

$$\gamma(m,m)\colon (x) \otimes (y) \mapsto \sum_{u,v \in X} p_{x,y}^{u,v}(u) \otimes (v)$$

$$\gamma(m,1)\colon (x) \otimes (y) \mapsto r_{x,y}$$

$$\gamma(1,m) : 1 \mapsto \sum_{x,y \in X} q_{x,y}(x) \otimes (y)$$

$$\gamma(1,1) : 1 \mapsto \frac{\epsilon}{|A|}$$

$$\gamma(1)\colon (x) \mapsto s_x(\sigma(x))$$

for some scalars $p_{x,y}^{u,v}, q_{x,y}, r_{x,y}, s_x, \epsilon \in k$ and a map $\sigma\colon X \to X$.

Let $\tau\colon X \to X$ be the map $x \mapsto x^{-1}$. Then the pentagon identity for $m \otimes m \otimes m \otimes m$ implies the following:

(1) $\sigma^3 = 1$.

(2) $\sigma\tau = \tau\sigma^{-1}$.

(3) The maps

$$\{(x,y) \in X \times X \mid \sigma^{-1}(x)\sigma^{-1}(y) \neq 1\} \rightleftarrows \{(u,v) \in X \times X \mid \sigma(u)\sigma(v) \neq 1\}$$
$$(x,y) \overset{\omega}{\rightarrow} (\sigma(x)y, \sigma(\sigma^{-1}(x)\sigma^{-1}(y)))$$
$$(\sigma^{-1}(u)v, \sigma^{-1}(\sigma(u)\sigma(v))) \leftarrow (u,v)$$

are well-defined and inverse to each other.

It turns out that there is no such pair (X,σ) other than those arising from $\mathrm{Rep}(F \rtimes F^\times)$:

Theorem. *Let B be a finite abelian group, $X = B - \{1\}$, and $\tau\colon X \to X$ the map $x \mapsto x^{-1}$. If a map $\sigma\colon X \to X$ satisfies (1), (2) and (3), then B is the multiplicative group of a field F and $\sigma(x) = 1 - \frac{1}{x}$ for all $x \in X$.*

So we have $\hat{A} = F^\times$ with F a finite field and $\sigma\colon x \mapsto 1 - \frac{1}{x}$. Moreover we have $\epsilon = \pm 1$. The case $|F| = 3$ being easy and treated separately, we assume $|F| > 3$. Replacing the vectors (x) suitably, we may assume $s_x = \epsilon$ for all x. The remaining equations then reduce to the following:

$$p_{x,y}^{u,v} \neq 0 \iff (x,y) \overset{\omega}{\rightarrow} (u,v) \tag{4}$$

$$q_{x,y} \neq 0 \iff \sigma(x)\sigma(y) = 1 \tag{5}$$

$$r_{x,y} \neq 0 \iff \sigma(x)^{-1}\sigma(y)^{-1} = 1 \tag{6}$$

$$q_{y,x} = \epsilon q_{x,y} \tag{7}$$

$$r_{y,x} = \epsilon r_{x,y} \tag{8}$$

$$q_{\sigma^{-1}(x),y} r_{x,y} = \frac{\epsilon}{|A|} \tag{9}$$

$$q_{\sigma(x),y} = q_{x,\sigma(y)} \tag{10}$$

$$r_{\sigma(x),y} = r_{x,\sigma(y)} \tag{11}$$

$$p_{x,y}^{u,v} = \frac{1}{p_{\sigma\tau(x),u}^{y,\sigma\tau(v)}} \frac{q_{v,\sigma\tau(v)}}{q_{x,\sigma\tau(x)}} = \frac{1}{p_{v,\tau\sigma(y)}^{\tau\sigma(u),x}} \frac{r_{y,\tau\sigma(y)}}{r_{u,\tau\sigma(u)}} = \frac{1}{p_{\tau\sigma(x),v}^{\sigma\tau(u),y}} \frac{r_{x,\tau\sigma(x)}}{r_{u,\tau\sigma(u)}} \tag{12}$$

and

$$p_{x,y}^{x',y'} p_{y',z}^{y'',z'} p_{x',y''}^{x'',y'''} = p_{y,z}^{x'',z''} p_{x,z''}^{y''',z'} \tag{13}$$

whenever

$$\begin{array}{ccc} & (x,y,z) & \\ {\scriptstyle \omega\times 1}\swarrow & & \searrow{\scriptstyle 1\times\omega} \\ (x',y',z) & & (x,x'',z'') \\ {\scriptstyle 1\times\omega}\downarrow & & \downarrow{\scriptstyle T\times 1} \\ (x',y'',z') & & (x'',x,z'') \\ {\scriptstyle \omega\times 1}\searrow & & \swarrow{\scriptstyle 1\times\omega} \\ & (x'',y''',z') & \end{array}$$

Note that if $C = \mathrm{Rep}(F \rtimes F^\times)$, then $\epsilon = 1$ and all nonzero $p_{x,y}^{u,v}, |A| q_{x,y}, r_{x,y}$ equal 1. This is the trivial solution for (4)–(13). For small finite fields F, we solve the equations with the aid of computer to find the following:

- If $|F| = 4$, there is a unique nontrivial solution up to equivalence. With α being a generator of $F^\times$, it is given by

$$\begin{gathered} \epsilon = -1, \\ p_{\alpha,\alpha}^{\alpha^2,\alpha^2} = 1, \quad p_{\alpha^2,\alpha^2}^{\alpha,\alpha} = -1, \\ q_{\alpha,\alpha^2} = -\tfrac{1}{|A|}, \quad q_{\alpha^2,\alpha} = \tfrac{1}{|A|}, \\ r_{\alpha,\alpha^2} = 1, \quad r_{\alpha^2,\alpha} = -1. \end{gathered}$$

- If $|F| = 8$, there is a unique nontrivial solution up to equivalence. Let $F^\times = \langle\alpha\rangle$ with $\alpha^3 + \alpha + 1 = 0$. It is given by

$$\epsilon = -1,$$

$$\begin{aligned} r_{\alpha^1,\alpha^5} &= r_{\alpha^2,\alpha^3} = r_{\alpha^4,\alpha^6} = 1, \\ r_{\alpha^5,\alpha^1} &= r_{\alpha^3,\alpha^2} = r_{\alpha^6,\alpha^4} = -1, \\ q_{\alpha^1,\alpha^3} &= q_{\alpha^2,\alpha^6} = q_{\alpha^4,\alpha^5} = -\tfrac{1}{|A|}, \\ q_{\alpha^3,\alpha^1} &= q_{\alpha^6,\alpha^2} = q_{\alpha^5,\alpha^4} = \tfrac{1}{|A|}, \end{aligned}$$

$$p_{x,y}^{u,v} = 1$$

for

$$\begin{aligned}(x,y,u,v) =&(\alpha^1,\alpha^1,\alpha^3,\alpha^2),\quad (\alpha^1,\alpha^2,\alpha^4,\alpha^6),\quad (\alpha^1,\alpha^4,\alpha^6,\alpha^3),\\ &(\alpha^2,\alpha^1,\alpha^5,\alpha^6),\quad (\alpha^2,\alpha^2,\alpha^6,\alpha^4),\quad (\alpha^2,\alpha^4,\alpha^1,\alpha^5),\\ &(\alpha^3,\alpha^3,\alpha^1,\alpha^6),\quad (\alpha^3,\alpha^5,\alpha^3,\alpha^4),\quad (\alpha^4,\alpha^1,\alpha^2,\alpha^3),\\ &(\alpha^4,\alpha^2,\alpha^3,\alpha^5),\quad (\alpha^4,\alpha^4,\alpha^5,\alpha^1),\quad (\alpha^5,\alpha^5,\alpha^4,\alpha^3),\\ &(\alpha^5,\alpha^6,\alpha^5,\alpha^2),\quad (\alpha^6,\alpha^3,\alpha^6,\alpha^1),\quad (\alpha^6,\alpha^6,\alpha^2,\alpha^5),\end{aligned}$$

and

$$p_{x,y}^{u,v} = -1$$

for

$$\begin{aligned}(x,y,u,v) =&(\alpha^1,\alpha^3,\alpha^5,\alpha^5),\quad (\alpha^1,\alpha^6,\alpha^1,\alpha^4),\quad (\alpha^2,\alpha^5,\alpha^2,\alpha^1),\\ &(\alpha^2,\alpha^6,\alpha^3,\alpha^3),\quad (\alpha^3,\alpha^1,\alpha^6,\alpha^5),\quad (\alpha^3,\alpha^4,\alpha^2,\alpha^2),\\ &(\alpha^3,\alpha^6,\alpha^4,\alpha^1),\quad (\alpha^4,\alpha^3,\alpha^4,\alpha^2),\quad (\alpha^4,\alpha^5,\alpha^6,\alpha^6),\\ &(\alpha^5,\alpha^2,\alpha^1,\alpha^1),\quad (\alpha^5,\alpha^3,\alpha^2,\alpha^4),\quad (\alpha^5,\alpha^4,\alpha^3,\alpha^6),\\ &(\alpha^6,\alpha^1,\alpha^4,\alpha^4),\quad (\alpha^6,\alpha^2,\alpha^5,\alpha^3),\quad (\alpha^6,\alpha^5,\alpha^1,\alpha^2).\end{aligned}$$

The other $p_{x,y}^{u,v}$, $q_{x,y}$ and $r_{x,y}$ are zero.

- If $|F| = 16$, there is no nontrivial solution.
- If $|F| = 32$, there is no nontrivial solution.

In the case of $|F| = 4$, we checked that there is no tensor category which does not satisfy our previous assumptions. So the above solution is the unique deformation of $\mathrm{Rep}(F \rtimes F^\times)$.

When $|F|$ is odd and $|F| > 3$, we have not yet found nontrivial solutions.

References

[T] D. Tambara, *A duality for modules over monoidal categories of representations of semisimple Hopf algebras*, preprint.

[TY] D. Tambara and S. Yamagami, *Tensor categories with fusion rules of self-duality for finite abelian groups*, J. Algebra **209** (1998), 692–707.

[Y] S. Yamagami, *Group symmetry in tensor categories*, preprint.

[8,4,4] 拡張 Hamming 符号に附随した頂点作用素代数の自己同型群と関連する話題

東京大学大学院数理科学研究科

松尾　厚・未佳†

本稿の主要な研究対象である二進線型符号に附随する頂点作用素代数は，筑波大学の宮本雅彦氏によって考案されたものである。宮本は，Frenkel-Lepowsky-Meurman [FLM] のムーンシャイン加群 $V^\natural$ 上に互いに可換な中心電荷 $\frac{1}{2}$ の Virasoro 代数の完全可約な作用が 48 個存在するという Dong-Mason-Zhu [DMZ] の発見に触発され，$V^\natural$ をこれらの Virasoro 代数のテンソル積の表現の直和として再構成するために，二進線型符号から標準的な手続で構成される頂点作用素代数を考え，その表現論を展開したのであった[1]。

一般に頂点作用素代数 (VOA) は構造が複雑であり，具体的な研究には非常な困難が伴う。特に $V^\natural$ はムーンシャイン現象との関連から良く調べられている対象であるが，その構造は非常に美しく，かつ極めて複雑である。

こういった VOA の複雑さの中に美しい対称性を見出すためのモデルとして，ここでは特に [8,4,4] 拡張 Hamming 符号に附随する VOA を調べてみようという訳である[2]。

拡張 Hamming 符号 H_8 は長さ 8 の唯一の重偶自己双対符号である。これに附随する VOA V_{H_8} は共形ウェイト 1 の部分空間が 0 で，共形ウェイト 2 の部分空間に非結合的可換代数 (Griess 代数) の構造が入る。その次元は 22 であって，$V^\natural$ の Griess 代数の次元 196884 と比べれば余りにも簡単であるが，実際に調べてみると V_{H_8} は (簡単ではあるが) 予想以上に面白い構造を持っていることがわかった。

本稿では，VOA V_{H_8} の Griess 代数の構造を調べ，V_{H_8} の自己同型群を決定する。また，自己同型群と Mathieu 群 M_{24} のトリオ安定化群との関係および自己同型群に含まれる対称群 S_3 と三対性 (triality) の関係について述べる。さらに，三対性による固定部分空間と関連して，位数 168 の単純群を自己同型群に持つ非結合的可換代数および VOA を構成する。詳細は論文 [Ma1]–[Ma3] を御覧頂きたい。

代数的組合せ論シンポジウムでの講演を薦めてくださった北詰正顕氏ならびに快く了承してくださった原田昌晃氏および宗政昭弘氏に感謝する。

† 現在は無所属

1. 文献 [Mi1]–[Mi4][Ko2][Ha2][Ha3] を参照。関連する研究として Dong-Griess-Höhn [DGH] がある。
2. その性質の一部は既に宮本 [Mi2][Mi4] によって調べられている。

1 頂点作用素代数の公理

頂点作用素超代数(VOSA)とは, $\mathbb{Z}/2\mathbb{Z}$ で次数付けされた $\mathbb{C}$ 上の[3]ベクトル空間 $V = V_{\bar{0}} \oplus V_{\bar{1}}$ とその元 $1, \omega \in V_{\bar{0}}$ および次数を保つ線型写像

$$Y : V \to (\mathrm{End}\, V)[[z, z^{-1}]], \quad Y(a,z) = \sum_{n \in \mathbb{Z}} a_{(n)} z^{-n-1}$$

が与えられていて, 以下の条件 (0)-(6) を満たすもののことである[4]。

(0) 任意の $a, b \in V$ に対して, ある n_0 が存在して $a_{(n)}b = 0$, $(n \geq n_0)$, が成立する。
(1) 任意の $a, b, c \in V$ と任意の $p, q, r \in \mathbb{Z}$ に対して次が成立する。

$$\sum_{i=0}^{\infty} \binom{p}{i} (a_{(r+i)}b)_{(p+q-i)}c = \sum_{i=0}^{\infty} (-1)^i \binom{r}{i} \left(a_{(p+r-i)}(b_{(q+i)}c) - (-1)^{r+p(a)p(b)} b_{(q+r-i)}(a_{(p+i)}c) \right)$$

ただし, $p(a), p(b)$ は a, b の偶奇を表す。
(2) 任意の $a \in V$ に対して次が成立する。

$$a_{(n)}1 = \begin{cases} 0 & (n \geq 0) \\ a & (n = -1) \end{cases}$$

(3) 作用素 $L_n = \omega_{(n+1)}$ は中心電荷 c の Virasoro 代数の表現を与える。すなわち

$$[L_m, L_n] = (m-n)L_{m+n} + \frac{m^3 - m}{12} \delta_{m+n,0} c$$

が成立する。
(4) 任意の $a \in V$ に対して $\omega_{(0)}a = a_{(-2)}1$ が成立する[5]。
(5) 作用素 $L_0 = \omega_{(1)}$ は半単純であって, V は

$$V_{\bar{0}} = \bigoplus_{m \in \mathbb{Z}} V^m, \quad V_{\bar{1}} = \bigoplus_{m \in \mathbb{Z}} V^{m+1/2}$$

と分解する。ただし V^d は固有値 (共形ウェイト) d の固有空間を表す[6]。
(6) 各固有空間 V^d は有限次元であり, ある d_0 が存在して $V^d = 0$, $(d < d_0)$, である。

本稿で考える VOSA はすべて次の性質も満たしている。

(7) $V^0 = \mathbb{C}1$ であり, $V^d = 0$, $(d < 0)$, である。

そこで, 本稿では (0)-(7) の性質を満たす組 $(V, 1, \omega, Y)$ を VOSA と呼ぶことにする。元 1 を真空ベクトル, 元 ω を共形ベクトル (conformal vector) [7]という。

---

3. 標数 0 の任意の体上で VOSA が考えられるが, 本稿では複素数体上に話を限ることとする。
4. 頂点代数の一般論については, 大阪大学の永友清和氏との共著 [MN] を参照していただきたい。
5. これは他の公理のもとで $Y(L_{-1}a, z) = \partial Y(a, z)$ と同値である。
6. 添字を下に付けて V_d と表すのが業界の標準であるが, 私は上に付けることにしている。
7. conformal vector は Borcherds の用語であり, Frenkel-Lepowsky-Meurman [FLM] は同じものを Virasoro element と呼んでいる。なお, 条件 (3) のみ満たすベクトルを本稿では Virasoro vector と呼ぶが, 宮本はそれを conformal vector と呼んでいる。

特に, $V_{\bar{1}} = 0$ のとき V は Boson 的であるといい, $(V, 1, \omega, Y)$ を頂点作用素代数 (VOA) という。

2 符号頂点作用素代数

集合 $\{\psi_n \mid n \in \mathbb{Z} + \frac{1}{2}\}$ を生成元の集合とし, $\psi_m\psi_n + \psi_n\psi_m = \delta_{m+n,0}$ を基本関係式とする $\mathbb{C}$ 上の Clifford 代数を $\mathcal{A}$ とする。その表現 M であって, $n > 0$ ならば $\psi_n|0\rangle = 0$ を満たす零でないベクトル $|0\rangle$ で生成されているものは同型を除いて一意的である。これを $\mathcal{A}$ の Fock 表現といい, その上の作用素 ψ_n の生成級数

$$\psi(z) = \sum_{n \in \mathbb{Z}+1/2} \psi_n z^{-n-1/2}$$

を (Neveu-Schwarz セクターにおける) Majorana Fermion 場という。

ここで, M 上の作用素

$$L_n = \frac{1}{2} \sum_{k > -n/2} (n + 2k)\psi_{-k}\psi_{n+k}, \quad (n \in \mathbb{Z})$$

は中心電荷 $\frac{1}{2}$ の Virasoro 代数の作用 $\mathcal{V}ir_{1/2}$ を与える。この作用に関する M の既約分解は, Fock 表現の標準的な偶奇による分解 $M = M_{\bar{0}} \oplus M_{\bar{1}}$ と一致し

$$M_{\bar{0}} \cong L(\tfrac{1}{2}, 0), \quad M_{\bar{1}} \cong L(\tfrac{1}{2}, \tfrac{1}{2})$$

となる[8]。その最高ウェイトベクトルはそれぞれ $|0\rangle$ および $|\frac{1}{2}\rangle = \psi_{-1/2}|0\rangle$ で与えられる。

このとき, $|0\rangle$ を真空ベクトルとし, $\omega_M = \frac{1}{2}\psi_{-3/2}\psi_{-1/2}|0\rangle$ を共形ベクトルとする M 上の VOSA の構造であって, $Y(|\frac{1}{2}\rangle, z) = \psi(z)$ なるものが一意的に存在する。なお $Y(\omega_M, z) = \sum_{n \in \mathbb{Z}} L_n z^{-n-2}$ の展開係数 L_n は上で与えたものと一致している。

次に, ベクトル空間 M の l 個のテンソル積 $M^{\otimes l}$ を考え,

$$1 = |0\rangle \otimes \cdots \otimes |0\rangle, \quad \omega = \omega^1 + \cdots + \omega^l$$

とする。ただし ω^i は第 i 番目の成分が ω_M でその他の成分が $|0\rangle$ であるような元である。空間 $M^{\otimes l}$ の元の偶奇を, 各成分の偶奇の和で与える。このとき $M^{\otimes l}$ には

$$Y(a_1 \otimes \cdots \otimes a_l, z)b_1 \otimes \cdots \otimes b_l = (-1)^{\sum_{i>j} p(a_i)p(b_j)} Y(a_1, z)b_1 \otimes \cdots \otimes Y(a_l, z)b_l$$

によって VOSA の構造が入る[9]。

---

8. 例えば文献 [KR] を参照。中心電荷 $\frac{1}{2}$ の Virasoro 代数のユニタリ性を満たす最高ウェイト既約表現は $L(\frac{1}{2}, 0)$, $L(\frac{1}{2}, \frac{1}{2})$, $L(\frac{1}{2}, \frac{1}{16})$ の 3 種類であり, これらを Ising 模型という。ここで, 最高ウェイトとは L_0 の最小固有値を意味する。本来 Ising 模型は可解格子模型の一種であるが, そのある種の極限が共形場理論になり, その正則・反正則部分それぞれがこれらの表現で記述されるという筋書きである。物理的な背景については例えば文献 [Gi] を参照。なお, ユニタリ性を用いずとも, $L(\frac{1}{2}, 0)$ が VOA 構造を持ち, その上の既約加群が上記のものに限るという形で最高ウェイト $0, \frac{1}{2}, \frac{1}{16}$ が特徴付けられることも知られている。
9. ここでは, 右辺の ± 1 の因子の入れ方は超代数のテンソル積の通常のルールに従っている。

さて, D を長さ l の二進線型符号とし, その符号語を 0 と 1 の列として $w = w_1 \cdots w_l$ と表す。宮本 [Mi2] に従い,

$$V_D = \bigoplus_{w \in D} M_w, \quad M_w = M_{\tilde{w}_1} \otimes \cdots \otimes M_{\tilde{w}_l}$$

とおく。このとき, D が加法で閉じていることから V_D は $M^{\otimes l}$ の部分代数となる。これを符号 D に附随した VOSA という[10]。ここで, $M_0^{\otimes l} \subset V_D$ であるから, $\omega^1, \ldots, \omega^l$ は V_D に属する。これらが生成する Virasoro 代数の作用 $\mathcal{V}ir_{1/2}$ のテンソル積に関して, 各直和因子 M_w は最高ウェイトベクトル

$$|w\rangle = |w_1/2\rangle \otimes \cdots \otimes |w_l/2\rangle$$

で生成された既約表現となる。

特に D が偶符号であれば $(V_D)_{\bar{1}} = 0$, すなわち V_D は Boson 的となる。これを, 符号 D に附随した VOA という。

さらに D が重偶符号であれば, V_D の共形ウェイト 1 の部分空間 V_D^1 は 0 となる。このような性質を持つ VOA を重 Boson 的 (doubly bosonic) と呼ぶことにしよう。このとき, 共形ウェイト 2 の部分空間を $B_D = V_D^2$ とおくと, B_D には

$$a \cdot b = \frac{1}{2} a_{(1)} b, \quad (a|b)1 = 2a_{(3)}b$$

によって, 不変な対称双線型形式を持つ非結合的可換代数の構造が入る。これを Frenkel-Lepowsky-Meurman の用語に従い, V_D の Griess 代数と呼ぶ。

ただし, 元 $e \in B_D$ が代数 B_D の巾等元であることと e が VOA V_D の Virasoro ベクトルであることが同値となるように Griess 代数の乗法を正規化した。ここで Virasoro ベクトルとは $Y(e,z)$ の展開係数が Virasoro 代数の作用を与えるような元 e のことである[11]。また, 双線型形式は, 巾等元 e の定める Virasoro 代数の表現の中心電荷が $(e|e)$ で与えられるように正規化した[12]。

なお, 符号が重偶な場合にはテンソル積で生じる ± 1 の因子を除いてよい[13]。

3 V_{H_8} の Griess 代数の記述

二元体 $\mathbb{F}_2$ 上の 2 次元射影平面 $\Omega' = \mathbb{P}^2(2)$ を考え, 直線の集合が

$$\mathcal{L} = \big\{\{1,2,3\}, \{1,4,5\}, \{1,6,7\}, \{2,4,7\}, \{2,5,6\}, \{3,4,7\}, \{3,5,6\}\big\}$$

10. 論文 [Mi2] では M を Boson 化した形で構成しているが, V_D の構成だけならここで述べたように Fermion を使うほうが手短だし, 計算も容易である。なお, Boson 化を含め M に関するいろいろな事実は以前から良く知られていることであって, 宮本は別の動機から再発見したといえる。
11. 既に述べたように, Virasoro ベクトル ω であって $\omega_{(0)}a = a_{(-2)}1$ となるものを本稿では共形ベクトルと呼んでいる。この用語の使い方は宮本と逆であるが, 本稿の使い方の方が良いと思う。
12. これらの正規化は必ずしも良い正規化ではないが, 伝統的な用語との兼ね合いで便利である。
13. テンソル積で生じる ± 1 の因子は符号 D の $\{\pm 1\}$ による中心拡大を定める余輪体とみなされる。符号が重偶であれば, 拡大が自明となって因子が除けるのである。この中心拡大は宮本理論の要点の一つであり, V_D の表現論 [Mi3] において積極的な役割を果たすが, 本稿ではこれ以上は用いない。

となるように番号を振って $\Omega'=\{1,2,3,4,5,6,7\}$ とする。これに原点 0 を付け加えたものは $\mathbb{F}_2$ 上の 3 次元アフィン空間 $\Omega=\mathbb{A}^3(2)$ と同一視される。

巾集合 $\mathcal{P}(\Omega')$ を標準的に $\mathbb{F}_2$ 上のベクトル空間とみなしたとき, 空集合, 直線, 直線の補集合および全体集合のなす部分空間が $[7,4,3]$ Hamming 符号 H_7 であり

$$H_8=\{w_0w_1\cdots w_7\,|\,w_1\cdots w_7\in H_7\}$$

としたものが $[8,4,4]$ 拡張 Hamming 符号である。符号語を列挙すると

00000000,	01010101,	10010110,	11000011,
00001111,	01011010,	10011001,	11001100,
00110011,	01100110,	10100101,	11110000,
00111100,	01101001,	10101010,	11111111.

となる。符号 H_7 の自己同型群は位数 168 の単純群 $GL_3(2)$ であり, H_8 の自己同型群はアフィン変換群 $AGL_3(2)$ である[14]。

さて, H_8 に附随した VOA V_{H_8} を考えよう[15]。H_8 は重偶だから V_{H_8} は重 Boson 的であり, その Griess 代数 B_{H_8} が考えられる。ベクトル空間としては

$$B_{H_8}=\bigoplus_{w\in H_8,|w|=4}\mathbb{C}|w\rangle\oplus\bigoplus_{i=0}^{7}\mathbb{C}\omega^i,\quad |w\rangle=|w_0/2\rangle\otimes\cdots\otimes|w_7/2\rangle$$

となり, 特に B_{H_8} は 22 次元である。その Griess 代数の構造は以下のようにして華麗に記述される。

まず, 各 $v\in\mathbb{F}_2^8$ に対して

$$s^v=\frac{1}{8}\omega+\frac{1}{8}\sum_{|w|=4}(-1)^{\sum_{i=0}^{7}v_iw_i}|w\rangle,$$

とおけば, s^v は中心電荷 $\frac{1}{2}$ の Virasoro ベクトルであり, $s^u=s^v$ が成立するのは $u-v\in H_8$ のときに限ることが, 宮本 [Mi2] によって観察されている。そこで,

$$e_1^i=\omega^i,\quad e_2^i=\frac{1}{8}\omega+\frac{1}{8}\sum_{|w|=4}(-1)^{w_i}|w\rangle,\quad e_3^i=\frac{1}{8}\omega+\frac{1}{8}\sum_{|w|=4}(-1)^{w_0+w_i}|w\rangle,$$

とおく。ただし, i は $\Omega=\{0,1,\ldots,7\}$ の元を動く。容易にわかるように, これら 24 個の Virasoro ベクトルは B_{H_8} を張っているので, これらのベクトルを用いて Griess 代数の構造を記述することができる。アフィン空間 $\Omega=\{0,1,\ldots,7\}=\mathbb{A}^3(2)$ を加法群 $(\mathbb{Z}/2\mathbb{Z})^3$ と見たときの加法を $\circ$ で表すことにする。単位元は 0 である。

命題 3.1 Griess 代数の乗法および双線型形式は次のように与えられる。

$$e_a^i\cdot e_a^j=\delta_{i,j}e_a^j,\qquad e_a^i\cdot e_b^j=\frac{1}{8}(e_a^i+e_b^j-e_c^{i\circ j}),\quad (a\neq b)$$

$$(e_a^i|e_a^j)=\frac{1}{2}\delta_{i,j},\qquad (e_a^i|e_b^j)=\frac{1}{16},\quad (a\neq b)$$

ここに c は $\{a,b,c\}=\{1,2,3\}$ となる番号である。

14. 群 $AGL_3(2)$ は平行移動のなす加法群による $GL_3(2)$ の分裂拡大である。
15. 前節で注意したように, テンソル積で生じる ±1 の因子は除くことができるので, 以下ではそうする。

4 V_{H_8} の自己同型群

まず Griess 代数 B_{H_8} の自己同型群を決定するため 24 個の Virasoro ベクトル (巾等元) を Griess 代数の内在的な性質で特徴付けることを考えよう。正確には

$$E_1 = \{e_1^0, \ldots, e_1^7\}, \quad E_2 = \{e_2^0, \ldots, e_2^7\}, \quad E_3 = \{e_3^0, \ldots, e_3^7\}.$$

なる三つの集合 E_1, E_2, E_3 を特徴付けるのである。

そこで, Griess 代数 B_{H_8} の巾等元 e がスペシャルであるとは[16], $(e|e) = \frac{1}{2}$ であって, e の作用 $a \mapsto R_e a = a \cdot e$ に関して B_{H_8} を固有空間分解したとき, 固有値が $0, \frac{1}{4}, 1$ に限ることと定める。

命題 4.1 Hamming 符号 VOA の Griess 代数 B_{H_8} の互いに直交する 8 個のスペシャルな巾等元の集合は E_1, E_2, E_3 に限る[17]。

これを用いると, 前節の B_{H_8} の記述から $\mathrm{Aut}(B_{H_8})$ の構造が決定できる。この部分は初等的だがなかなか面白いので詳しく記してみよう。

命題から, B_{H_8} の自己同型は 3 つの集合 E_1, E_2, E_3 を置換し, $E_1 \sqcup E_2 \sqcup E_3$ は B_{H_8} を張るので, $\mathrm{Aut}(B_{H_8})$ は対称群 S_{24} の部分群と思える。このとき, 各自己同型に対して, それが引き起こす E_1, E_2, E_3 の置換を対応させる写像 $\mathrm{Aut}(B_{H_8}) \to S_3$ の核を Aut' とすると, Aut' は $S_8 \times S_8 \times S_8$ の部分群とみなされる。一方, 添字 $1,2,3$ の置換は B_{H_8} の自己同型を与えるので, $\mathrm{Aut}(B_{H_8}) = \mathrm{Aut}' : S_3$ となる。

補題 4.2 対称群の元 $g_1, g_2, g_3 \in S_8$ および $\sigma \in S_3$ に対して, 元 $\alpha = (g_1, g_2, g_3)\sigma$ が $\mathrm{Aut}(B_{H_8})$ に属するための必要充分条件は $g_1(i) \circ g_2(j) = g_3(i \circ j)$ がすべての $i, j = 0, \ldots, 7$ に対して成立することである[18]。

[証明] 実際, $\alpha(e_a^i) \cdot \alpha(e_b^j)$ と $\alpha(e_a^i \cdot e_b^j)$ を比較してみれば良い。

補題 4.3 元 $(g_1, g_2, g_3) \in \mathrm{Aut}'$ および $\{a, b, c\} = \{1, 2, 3\}$ に対して, $g_a = g_b$ となるための必要充分条件は $g_c(0) = 0$ である。

[証明] 例えば $g_2 = g_3$ とする。このとき, $g_1(0) \circ i = g_1(0) \circ g_2(g_2^{-1}(i)) = g_3(0 \circ g_2^{-1}(i)) = g_3(g_2^{-1}(i)) = i$ が任意の i について成立するので, $g_1(0) = 0$ でなければならない。逆に $g_1(0) = 0$ とすると, 任意の i に対して $g_2(i) = 0 \circ g_2(i) = g_1(0) \circ g_2(i) = g_3(0 \circ i) = g_3(i)$ であるから, $g_2 = g_3$ を得る。

これらを用いると, 次がわかる。

16. ここだけの用語のつもりでこのように呼んだが, 講演終了後に「このような普通の言葉を特殊な意味に用いるべきでない」との指摘を受けた。不埒なる用語の流布するはかくなる所以かと反省している (厚)。
17. この命題は本質的には宮本 [Mi4] によるが, B_{H_8} の性質として述べるための変更を行った。なお, 二つの巾等元 e, f が直交するとは $e \cdot f = 0$ となることである。このとき, 不変双線型形式に関して $(e|f) = (e \cdot e|f) = (e|e \cdot f) = 0$ となる。
18. このとき, $g_1(i) \circ g_3(j) = g_2(i \circ j)$ および $g_2(i) \circ g_3(j) = g_1(i \circ j)$ も自動的に成り立つ。

命題 4.4 部分群 Aut' の任意の元は, 平行移動 t_1, t_2, t_3 であって $t_1t_2t_3 = \mathrm{id}$ なるものと[19] $g \in GL_3(2)$ を用いて $(t_1, t_2, t_3)(g, g, g)$ の形に一意的に表される。

[証明] 群 Aut' の任意の元 (g_1, g_2, g_3) に対し, $s(0) = g_1(0)$ となる平行移動 s および $t(0) = g_3(0)$ となる平行移動 t をとる。このとき (s, st, t) は Aut' に属するので, 合成 $(h_1, h_2, h_3) = (sg_1, stg_2, tg_3)$ も Aut' に属する。このとき $h_1(0) = h_3(0) = 0$ であるから, 前補題により $h_1 = h_2 = h_3$ でなければならない。これを g とおくと, g は原点 0 を固定していて, しかも $g(i \circ j) = g(i) \circ g(j)$ を満足するので, $GL_3(2)$ の元である。よって $(g_1, g_2, g_3) = (s, st, t)(g, g, g)$ と書けた。一意性は容易にわかる。

以上から, $\mathrm{Aut}(B_{H_8})$ は $2^6 : (GL_3(2) \times S_3)$ なる構造を持つことがわかる。特にその位数は 64512 である。

さて VOA V_{H_8} の自己同型群を考えたい。VOA V_{H_8} の自己同型の B_{H_8} への制限は

$$\mathrm{Aut}(V_{H_8}) \to \mathrm{Aut}(B_{H_8})$$

なる群の準同型を引き起こす。ここで VOA V_{H_8} は, その構成により, 共形ウェイト 2 の部分空間 B_{H_8} から生成されているので, この準同型は単射である。よって, $\mathrm{Aut}(B_{H_8})$ の元の $\mathrm{Aut}(V_{H_8})$ への持ち上げが構成できれば, $\mathrm{Aut}(V_{H_8}) \cong \mathrm{Aut}(B_{H_8})$ が示されるが, この持ち上げの構成は既に宮本によってなされている。

実際, 符号の自己同型 $\mathrm{Aut}(H_8) = AGL_3(2)$ は V_{H_8} の構成から直ちに $\mathrm{Aut}(V_{H_8})$ の元に持ち上がる。また, 24 個の Virasoro ベクトルそれぞれに対して, 対応する Virasoro 代数の作用に関して V_{H_8} を既約分解したとき, そこに現れる $L(\frac{1}{2}, \frac{1}{2})$ の成分を -1 倍する写像は V_{H_8} の自己同型となる[20]。これらの持ち上げとその合成によって B_{H_8} のすべての自己同型が V_{H_8} の自己同型に持ち上がり, かくして

定理 1 Hamming 符号頂点作用素代数 V_{H_8} の自己同型群は $2^6 : (GL_3(2) \times S_3)$ なる構造を持つ。

5 トリオ安定化群との同型

前節の $\mathrm{Aut}(V_{H_8})$ の記述を眺めてみれば, それと良く似た群が知られているのに気付く。それは Mathieu 群 M_{24} の極大部分群の一つであるトリオ安定化群 (trio stabilizer) である。

Mathieu 群 M_{24} は [24, 12, 8] 拡張 Golay 符号の自己同型群である。この符号は拡張 Hamming 符号 H_8 三つの直積を加工することにより具体的に構成されるが, その三つのブロックの集合を保つような M_{24} の元全体のなす部分群がトリオ安定化群である[21]。

トリオ安定化群は $2^6 : (PSL_2(7) \times S_3)$ なる表示を持っているが, $\mathrm{Aut}(V_{H_8})$ の表示とは $PSL_2(7)$ と $GL_3(2)$ の違いしかない。良く知られている通り $GL_3(2)$ と $PSL_2(7)$ はともに

19. アフィン空間 $\mathbb{A}^3(2)$ における平行移動を集合 Ω の置換と見て群演算を乗法的に表す。
20. この場合は $L(\frac{1}{2}, \frac{1}{16})$ は現れないが, もし現れた場合にはその成分を -1 倍する写像が自己同型となる。これらの自己同型はしばしば宮本の自己同型と呼ばれるが, 実際は以前から知られていたものである。ただし, その構成法を VOA の公理に基づいて定式化し厳密な証明を与えたのは宮本 [Mi1] が最初である。
21. 詳しくは文献 [Co][Ko1] を参照。

位数 168 の単純群であって, これらは同型である。よって $\mathrm{Aut}(V_{H_8})$ はトリオ安定化群と同型なのではないかと想像される。ただし, 抽象群として $GL_3(2)$ と $PSL_2(7)$ は同型であるが, 自然な置換表現は異なっており, $\mathrm{Aut}(V_{H_8})$ とトリオ安定化群の自然な 24 次の置換表現も異なる。従って, 両者が本当に同型かどうかは自明ではない[22]。

しかし, 文献 [Co] にある $PSL_2(7)$ から $GL_3(2)$ への具体的な同型写像の構成をみると, それがうまく拡張されて, トリオ安定化群から $\mathrm{Aut}(V_{H_8})$ への同型写像を与えることが, 置換表現の構造を具体的に見て確かめられる。実は, トリオ安定化群の中に, 共役類をなす 24 個の対合を見つけることができて, これにトリオ安定化群を共役で作用させると, それが前節で述べた $\mathrm{Aut}(V_{H_8})$ による 24 個の Virasoro ベクトルの置換と一致してしまうのである。かくして

定理 2 Hamming 符号頂点作用素代数 V_{H_8} の自己同型群は Mathieu 群 M_{24} のトリオ安定化群と同型である。

6 三対性

さて, V_{H_8} の自己同型群には対称群 S_3 が含まれていた。この対称性は拡張 Hamming 符号 H_8 の対称性からは全く予期できないものであるが, 宮本によるムーンシャイン加群 $V^\natural$ の再構成において技術的に重要な役割を果たしている[23]。それは Frenkel-Lepowsky-Meurman による $V^\natural$ の VOA 構造の存在証明において, A_1 型の Lie 環に働く S_3 対称性[24]が果たした役割と類似のものである。彼らがこの対称性を三対性 (triality) と呼んでいるのに倣って, V_{H_8} の S_3 対称性を V_{H_8} の三対性と呼ぼう。

ところで, 三対性という言葉は, 本来は Lie 群 $Spin(8)$ の外部自己同型群としての対称群 S_3 のことを意味している[25]。これは D_4 型の Dynkin 図形の対称性から来る単純ルートないしは基本ウェイトの置換としてもとらえられるが, 実は V_{H_8} の三対性はこの本来の D_4 型の三対性と解釈できるのである。

すなわち, D_4 型ルート格子に附随した VOA V_{D_4} を考えると, その中に, 中心電荷 $\frac{1}{2}$ の互いに可換な 8 個の Virasoro ベクトルの集合であって, 三対性で互いに移りあうもの 3 個がうまく構成できる。その一つによって V_{D_4} を分解することによって, V_{D_4} はすべての偶語からなる長さ 8 の符号に附随する VOA と同型になることがわかる。これによって V_{H_8} を V_{D_4} に埋めこむことができ, D_4 の三対性が誘導する V_{D_4} の自己同型が V_{H_8} の三対性と一致するのである。

さらに詳しく言うと, D_4 型ルート格子の標準的な対合 $\theta = -1$ を V_{D_4} へ持ち上げて, それによる固定部分空間 $V_{D_4}^+$ を考える。これは A_1^4 型ルート格子に附随した VOA $V_{A_1^4}$ と同

22. つまり, みかけの表示は同じでも異なる拡大かもしれない。
23. S_3 対称性により, 因子 $L(\frac{1}{2}, \frac{1}{16})$ を含む部分が $L(\frac{1}{2}, 0)$ と $L(\frac{1}{2}, \frac{1}{2})$ からなっているように見えて, その結果 VOA の構造の与え方がわかる ([Mi4]を参照)。ただし, これが VOA 構造の存在にとって本質的かどうかは不明であり, それを用いない構成法があればそれに越したことはない。
24. 正確には $[y_i, y_{i+1}] = 2y_{i+2}$, $(i = 1, 2, 3)$, なる基底 y_1, y_2, y_3 をとるとき, Lie 環の自己同型であって集合 $\{\pm y_1, \pm y_2, \pm y_3\}$ を保つもの全体が S_3 の拡大 $2^2 : S_3$ となる。
25. 本当はもう少し一般的かつ精密な意味付けがあるが, 本稿ではこの意味で用いる。

一視される。さらにその標準的な対合による固定部分空間を考えると，その中に V_{H_8} が入る。これらの VOA は D_4 の三対性によって不変に保たれており，次の定理を得る。

定理 3 (未佳) 頂点作用素代数の系列 $V_{H_8} \subset V_{A_1^4}^+ \subset V_{A_1^4} = V_{D_4}^+ \subset V_{D_4}$ には D_4 の三対性が自然に作用する。

7 三対性による固定部分空間

さて，V_{H_8} の Griess 代数 B_{H_8} の S_3 作用に関する固定部分空間 $B_{H_8}^{S_3}$ を考えよう。

$$e' = \frac{4}{5}(e_1^0 + e_2^0 + e_3^0)$$
$$e^i = \frac{2}{3}(e_1^i + e_2^i + e_3^i) - \frac{2}{15}(e_1^0 + e_2^0 + e_3^0), \quad (i = 1, \ldots, 7)$$

とすると，e' は中心電荷 $\frac{6}{5}$，e^i は中心電荷 $\frac{4}{5}$ の巾等元であり，固定部分空間は

$$B_{H_8}^{S_3} = \mathbb{C}e' \oplus C_{1/6}, \quad (C_{1/6} = \bigoplus_{i=1}^{7} \mathbb{C}e^i)$$

と直交分解する。$C_{1/6}$ の乗法は

$$e^i \cdot e^i = e^i, \qquad e^i \cdot e^j = \frac{1}{6}(e^i + e^j - e^{i \circ j}), \ (i \neq j)$$

で与えられ，特に $u = \frac{1}{2}(e^1 + \cdots + e^7)$ は単位元となる。この代数は，原田耕一郎氏が文献 [Hal] において考察した $GL_3(2)$ を自己同型群とする非結合的可換代数に類似している[26]。

さて，$\alpha + \beta + \gamma = \frac{3}{4}$ かつ $\alpha\beta + \beta\gamma + \gamma\alpha = 0$ を満たす複素数 α, β, γ および点 i を通過する三つの直線 $\{i, j, i \circ j\}, \{i, k, i \circ k\}, \{i, l, i \circ l\}$ を用いて，

$$e^i_{\alpha\beta\gamma} = -\frac{1}{4}e^i + \alpha(e^j + e^{i \circ j}) + \beta(e^k + e^{i \circ k}) + \gamma(e^l + e^{i \circ l})$$

と表される元を考える[27]。すると，$C_{1/6}$ の 5 種類の元 $u, e^i, u - e^i, e^i_{\alpha\beta\gamma}, u - e^i_{\alpha\beta\gamma}$ はすべて巾等元 (Virasoro ベクトル) であり，中心電荷はそれぞれ $\frac{14}{5}$, $\frac{4}{5}$, $\frac{10}{5}$, 1, $\frac{9}{5}$ である。

実は，原田の計算方法を真似することにより[28]，代数 $C_{1/6}$ の巾等元は完全に分類することができて，次の結果を得る。

定理 4 代数 $C_{1/6}$ の巾等元は上に挙げたものに限る。

これより $C_{1/6}$ の自己同型は巾等元 $e^1, \ldots, e^7$ を置換することがわかり，代数の構造から $C_{1/6}$ の自己同型群は位数 168 の単純群 $GL_3(2)$ と一致することが容易にわかる。それは $\mathrm{Aut}(V_{H_8})$ のなかで，E_1, E_2, E_3 に対角的に作用する $GL_3(2)$ の制限に他ならない。従って，$C_{1/6}$ あるいは $B_{H_8}^{S_3}$ で生成された $V_{H_8}^{S_3}$ の部分代数を考えれば，それは $GL_3(2)$ を自己同型群とする VOA となる[29]。

---

26. しかし大きな違いがある。これについては次節を参照。
27. 従ってこの形の元は無限個ある。
28. 過剰決定的な 7 元連立 2 次方程式を解くのだが，安直に Mathematica にやらせたらお手上げであった。対称性を利用した原田の変数変換を用いればちゃんと手で解ける。
29. この VOA の構造を知りたいところであるが，今のところまだ良くわかっていない。

8 $GL_3(2)$ を自己同型群に持つ非結合的可換代数の族

代数 $C_{1/6}$ の構造を複素数 $\lambda \in \mathbb{C}$ で変形して,

$$e^i \cdot e^i = e^i, \qquad e^i \cdot e^j = \lambda(e^i + e^j - e^{i\circ j}),\ (i \neq j)$$

なる乗法を持つ非結合的可換代数 C_λ を考えよう。

命題 8.1 代数 C_λ は, $\lambda = -\frac{1}{6}, 0, \frac{1}{2}, 1$ の場合を除き, 巾結合的[30]でない単純な単位的可換代数であり, スカラー倍を除いて一意的な非退化対称不変双線型形式を持つ。

さて, この代数の自己同型群を決定するために, 巾等元の集合 $E = \{e^1, \ldots, e^7\}$ を代数の内在的な性質で特徴付けることを考える。そのためには e の作用 $a \mapsto R_e a = a \cdot e$ の特性多項式の情報を利用するのが効果的である。

実際, 巾等元 e^i の作用 R_{e^i} による C_λ の固有空間分解は

$$\begin{aligned} C_\lambda &= C^i(0) \oplus C^i(2\lambda) \oplus C^i(1), \\ C^i(0) &= \langle 2\lambda e^i - e^j - e^{i\circ j}, 2\lambda e^i - e^k - e^{i\circ k}, 2\lambda e^i - e^l - e^{i\circ l} \rangle, \\ C^i(2\lambda) &= \langle e^j - e^{i\circ j}, e^k - e^{i\circ k}, e^l - e^{i\circ l} \rangle, \\ C^i(1) &= \langle e^i \rangle, \end{aligned}$$

で与えられる[31]。ここに, $\{i,j,i\circ j\}$, $\{i,k,i\circ k\}$, $\{i,l,i\circ l\}$ は点 i を通過する三つの直線である。特に, 特性多項式は $x^3(x-2\lambda)^3(x-1)$ で与えられる。その情報をすべて利用するのは技術的に困難と思われるが, 実際は λ がいくつかの例外的な値をとる場合を除いてトレースの情報で充分である。いずれにせよ, 計算により次の結果が示される。

命題 8.2 $\lambda = \frac{1}{2}$ の場合を除き, 集合 E は特性多項式が $x^3(x-2\lambda)^3(x-1)$ となるような巾等元全体の集合である[32]。

これを用いると, C_λ の自己同型群が次のように決定される[33]。

定理 5 代数 C_λ の自己同型群は $\lambda = 0, \frac{1}{2}$ の場合は対称群 S_7 であり, それ以外の場合は位数 168 の単純群 $GL_3(2)$ である。

さて, 代数 C_λ においては, $\lambda = -\frac{1}{6}$ の場合を除き, $GL_3(2)$ が自明に働く 1 次元部分空間は単位元 u の張る部分空間である。一方, 原田がかつて考察した代数においては, この 1 次元部分空間がイデアルになっており, 自己同型群は 6 次元の商代数上に落ちる。

---

30. 任意の元で生成された部分代数が結合的となるとき, 巾結合的 (power-associative) という。
31. 結合的な代数の巾等元の固有値は 0, 1 であるのに対し, 巾結合的な代数の巾等元の固有値は $0, \frac{1}{2}, 1$ である。代数 C_λ は巾結合的ですらないが, C_λ を張る巾等元の集合であって, 固有値が $0, 2\lambda, 1$ であるようなものがとれるという意味では巾結合的な代数に近いと言えるかもしれない。
32. 代数 C_λ の巾等元をすべて分類したいところであるが, 前節の計算には $\lambda = \frac{1}{6}$ の場合に限って奇跡的に成り立つ中間式があり, 一般の λ の場合はうまくいかない。
33. この節では自己同型が不変双線型形式を保つことは要請していないが, 結果的に保つことになる。

ところで, 原田が $GL_3(2)$ を自己同型群に持つ非結合的可換代数を考察した動機は, R. Griess 氏が文献 [Gr] においてモンスターを自己同型群とする 196884 次元の非結合的可換代数を構成したことにあった。この代数は, 後に Frenkel-Lepowsky-Meurman [FLM] が $V^\natural$ を定義して, その共形ウェイト 2 の部分空間のなす Griess 代数という再解釈を得たが, 共形ベクトルから来る自然な単位元があるという点で, Griess が最初に構成した代数とは異なっている。Frenkel-Lepowsky-Meurman によれば, $V^\natural$ の Griess 代数を不変双線型形式に関する単位元の直交補空間に射影したものが Griess の代数の 196883 次元の成分と同型となるのだが, ムーンシャインに関するその後の発展[34]を見れば, $V^\natural$ の Griess 代数の方が自然なものであると思われる。

我々の代数 C_λ と原田の代数の関係もこれと類似しており, 単位元を持つ代数 C_λ の方が自然なものであると考えられよう。実際, 前節で見たように $\lambda = \frac{1}{6}$ の場合には $C_{1/6}$ はある VOA の Griess 代数になっていた[35]。

この種の代数をより一般のデザインや, 有限群が基底の多重可移な置換として作用する空間に附随する場合に拡張することは興味ある問題であると思われる[36]。

参考文献

[Bo] R.E. Borcherds: Monstrous moonshine and monstrous Lie superalgebras, Invent. Math. 109 (1992) 405–444.

[Co] J.H. Conway: "Three lectures on exceptional groups" and "The Golay codes and the Mathieu groups", in J.H. Conway and N.J.A. Sloan: Sphere packings, lattices and groups, Second edition. Springer-verlag, New York, 1993. 267–330.

[DGH] C.-Y. Dong, R.L. Griess Jr and G. Höhn: Framed vertex operator algebras, codes and the moonshine module, Commun. Math. Phys. 193 (1998) 407–448.

[DMZ] C.-Y. Dong, G. Mason and Y.-C. Zhu: "Discrete series of the Virasoro algebra and the moonshine module", in W.J. Haboush and B.J. Parshall, eds.: Proc. Symp. Pure Math. 56, Algebraic Groups and Their Generalizations. American Mathematical Society, Providence, RI. Part 2, 295–316.

[FLM] I.B. Frenkel, J. Lepowsky and A. Meurman: A natural representation of the Fischer-Griess Monster with the modular function J as character. Proc. Natl. Acad. Sci. USA, 81 (1984) 3256–3260; Vertex operator algebras and the Monster. Pure and Appl. Math. 134, Academic Press, Boston, 1989.

34. 文献 [Bo][Ha2][Ha3] を参照。
35. 経験から言って $\lambda = \frac{1}{6}$ の場合は非常に特殊であると思われるが, その内在的な意味はよくわからない。これを理解することは Griess 代数を理解するための一つの課題であると思われる。
36. 自明表現の部分がイデアルとなっているものについては, 原田の研究を始めとして過去に研究がなされている。例えば文献 [Su] を参照。

[Gi] P. Ginsparg: "Applied conformal field theory", in E. Brézin and J. Zinn-Justin, eds.: Les Houches Session XLIX, 1988, Champs, cordes, et phénomènes critiques. Elsevier, 1989. 3-168.

[Gr] R.L. Griess, Jr.: The friendly giant. Invent. Math. 69 (1982) 1-102.

[Ha1] K. Harada: On a commutative nonassociative algebra associated with a doubly transitive group. J. Algebra 91 (1984) 192-206.

[Ha2] 原田耕一郎: モンスターの数学, 数学 51, 1999.

[Ha3] 原田耕一郎: モンスター 群の広がり. 岩波書店, 1999.

[KR] V.G. Kac and A.K. Raina: Bombay lectures on highest weight representations of infinite dimensional Lie algebras. World Scientific, 1987.

[Ko1] 近藤 武: Mathieu 群と Conway 群, 講義録.

[Ko2] 近藤 武: Moonshine VOA の指標の計算, 代数分科会報告集, 1998.

[Ma1] M. Matsuo: On the triality of the Hamming code vertex operator algebra, submitted to J. Algebra.

[Ma2] A. Matsuo and M. Matsuo: The automorphism group of the Hamming code vertex operator algebra, submitted to J. Algebra.

[Ma3] A. Matsuo and M. Matsuo: On a Commutative Nonassociative Algebra associated with $GL_3(2)$, in preparation.

[MN] A. Matsuo and K. Nagatomo: Axioms for a vertex algebra and the locality of quantum fields, MSJ Memoirs 4. 日本数学会, 1999.

[Mi1] M. Miyamoto: Griess algebras and conformal vectors in vertex operator algebras, J. Algebra 179 (1996) 528-548.

[Mi2] M. Miyamoto: Binary codes and vertex operator (super)algebras, J. Algebra 181 (1996) 207-222.

[Mi3] M. Miyamoto: Representation theory of code vertex operator algebra, J. Algebra 201 (1998) 115-150.

[Mi4] M. Miyamoto: Hamming code vertex operator algebra and construction of vertex operator algebras, J. Algebra, 215 (1999) 509-530.

[Su] H. Suzuki: Commutative algebras associated with a doubly transitive group. Osaka J. Math. 23 (1986) 541-561.

A Combinatorial Proof of Hook Length Property of the d-Complete Posets

Masao ISHIKAWA* and Hiroyuki Tagawa†

September 15, 1999

*Department of Mathematics, Faculty of Education, Tottori University

†Department of Mathematics, Faculty of Education, Wakayama University

1 Introduction

この記事は d-complete poset の hook-length の公式の証明が主な目的である. 特にここでは Swivel shifteds と呼ばれる既約な d-complete poset について取り上げている. hook-length の公式というのは linear extension の個数を積の形に書く公式で, d-complete poset 共通の universal な公式があるが, ここではそれを述べず Swivel shifteds の場合の公式を証明することを最終的な目的とする. linear extension の個数については, linear extension から定義される charge を重みとして, その q-version を証明する. この q-version は第 2 節で (P,ω)-partition の母関数と関連づけられる. 第 3 節では Swivel shifteds の定義と Swivel shifteds を順序集合 P とする (P,ω)-partition の母関数を求める. そして最後に第 4 節で, この母関数がある積になることを証明する.

2 (P,ω)-Partitions

(P,ω)-partitions の概念は [5] の中で R.P.Stanley によって定義され, その母関数についていくつかの一般的な結果が得られている. 有限半順序集合 P と単射 $\omega : P \to \mathbb{P}$ の組 (P,ω) を *labeled* poset という. ここで $\mathbb{P}$ は正整数全体の集合とする. すなわち, これは半順序集合 P の各元に異なる正整数を振ったものと考えられる. 簡単のために今後大体 P の base set を $P = [n] = \{1, 2, \cdots, n\}$ とし $\mathrm{Img}\,\omega = [n]$ とする. すべての $x, y \in P$ に対して $x < y$ ならば $\omega(x) < \omega(y)$ である labeling ω を *natural* という. labeling ω と dual な labeling ω^* は $\mathbb{P}$ の順序を逆にすることに定義される. 同様に P の順序を逆転した半順序集合を *order dual poset* P^* とかき P の dual という. すなわち P で $x \leq y$ ということは P^* で $x \geq y$ ということと同値である. (P,ω)-*partition* とは map $\sigma : P \to \mathbb{N}$ ですべての P の元 $x < y$ に対して次を満たすことである. ここで $\mathbb{N}$ は非負整数全体の集合である.

*Partially supported by Grant-in-Aid for Scientific Research (C) No. 09640037, the Ministry of Education, Science and Culture of Japan.

†Partially supported by Grant-in-Aid for Encouragement of Young Scientists No. 11740019, the Ministry of Education, Science and Culture of Japan

(i) $\sigma(x) \geq \sigma(y)$

(ii) $\omega(x) > \omega(y)$ ならば $\sigma(x) > \sigma(y)$

w が order-preserving のとき σ は簡単のために *P-partition* と呼ばれる. w が order-reversing のとき σ は簡単のために *strict P-partition* と呼ばれる. $|\sigma| = \sum_{x \in P} \sigma(x) = m$ であるとき σ は m の (P,ω)-partition といわれ $\sigma \vdash m$ と記述される. (P,ω)-partitions 全体の集合は $\mathcal{A}(P,\omega)$ と記述される.

同様に *reverse* (P,ω)*-partition* $\sigma : P \to \mathbb{N}$ を上の (i),(ii) の条件を下の (i'),(ii') の条件に置き換えることによって定義する.

(i') $\sigma(x) \leq \sigma(y)$,

(ii') $\sigma(x) > \sigma(y)$ whenever $\omega(x) < \omega(y)$.

これによってほぼ平行した議論をすることが可能である. $\mathcal{R}(P,\omega)$ を reverse (P,ω)-partitions 全体の集合とする. この論文の中では (P,ω)-partition の $|\sigma|$ で重みをつけられた 1 変数の母関数のみしか使わない. それは次の式で定義される.

$$F_{\mathcal{A}}(P,\omega;q) = \sum_{\sigma \in \mathcal{A}(P,\omega)} q^{|\sigma|}$$

同様にして

$$F_{\mathcal{R}}(P,\omega;q) = \sum_{\sigma \in \mathcal{R}(P,\omega)} q^{|\sigma|}.$$

この論文の中ではある有限半順序集合のクラスの母関数を計算し, それに対してシンプルな積公式が成り立つことを示す. $|P| = n$ のとき, 順序同型写像 $\tau : P \to n$ は P の linear extension といわれる. ここで n は n 個の元からなる chain である. $\mathcal{L}(P)$ を P の linear extension 全体の集合とする. また $\mathcal{L}(P,\omega) = \{\omega \circ \tau^{-1} : \tau \in \mathcal{L}(P)\}$ とおく. このとき $\mathcal{L}(P^*) = \{\pi_0 \circ \tau : \tau \in \mathcal{L}(P)\}$ と $\mathcal{L}(P^*,\omega) = \{\omega \circ \tau^{-1} \circ \pi_0 : \tau \in \mathcal{L}(P)\}$ が成り立つ. ここで π_0 は対称群 S_n の最長元である. また $\mathcal{W}(P,\omega) = \{\tau \circ \omega^{-1} : \tau \in \mathcal{L}(P)\} \subseteq S_n$ とおき, この元を linear extension の ω に関する *reading words* という.

任意の $\pi \in S_n$ に対して

$$D(\pi) = \{1 \leq i \leq n-1 : \pi(i) > \pi(i+1)\}$$

とおき π の descent set という. また

$$A(\pi) = \{1 \leq i \leq n-1 : \pi(i) < \pi(i+1)\}$$

は π の ascent set といわれる. さらに $\pi \in S_n$ に対して $\mathrm{maj}(\pi) = \sum_{i \in D(\pi)} i$ を π の *major index*, $\min(\pi) = \sum_{i \in A(\pi)} i$ を π の *minor index* という.

任意の permutation $\pi \in S_n$ と $i \in [n]$ に対して

$$c_i(\pi) = \begin{cases} 0 & \text{if } i = 1, \\ c_{i-1}(\pi) + \delta(\pi^{-1}(i-1) > \pi^{-1}(i)) & \text{if } 2 \leq i \leq n. \end{cases}$$

とおく. ここで $\delta(*)$ は $*$ が真のとき 1 で, そうでないとき 0 とする. 同様に

$$c'_i(\pi) = \begin{cases} 0 & \text{if } i = 1, \\ c'_{i-1}(\pi) + \delta(\pi^{-1}(i-1) < \pi^{-1}(i)) & \text{if } 2 \leq i \leq n. \end{cases}$$

とおく. $\mathrm{ch}(\pi)=\sum_{i=1}^{n} c_i(\pi)$ を π の charge といい, $\mathrm{coch}(\pi)=\sum_{i=1}^{n} c'_i(\pi)$ を π の cocharge という. このとき $\mathrm{ch}(\pi)=\sum_{i\in D(\pi^{-1})}(n-i)=\min(\pi^{-1}\circ\pi_0)$ かつ $\mathrm{coch}(\pi)=\sum_{i\in A(\pi^{-1})}(n-i)=\mathrm{maj}(\pi^{-1}\circ\pi_0)$ が成り立つことを見るのは易しい. ここで π_0 は S_n の最長元とする. ゆえに $\mathrm{ch}(\pi)+\mathrm{coch}(\pi)=\binom{n}{2}$ が成り立つ.

任意の linear extension $\tau\in\mathcal{L}(P)$ に対して, $D(\tau,\omega)=\{i\in[n-1]:\omega(\tau^{-1}(i))>\omega(\tau^{-1}(i+1))\}$ を τ の ω に関する descent set という. また

$$\mathcal{A}(P,\omega,\tau)=\left\{\sigma\in\mathcal{A}(P,\omega):\quad \begin{array}{l}\sigma(\tau^{-1}(1))\le\cdots\le\sigma(\tau^{-1}(n)) \text{ and}\\ i\in D(\tau,\omega)\Rightarrow\sigma(\tau^{-1}(i))<\sigma(\tau^{-1}(i+1))\end{array}\right\}$$

とおく. (P,ω)-partition の基本定理より

$$\mathcal{A}(P,\omega)=\bigcup_{\tau\in\mathcal{L}(P)}\mathcal{A}(P,\omega,\tau).$$

である. この系として

$$F_{\mathcal{A}}(P,\omega;q)=\frac{\sum_{\pi\in\mathcal{L}(P,\omega)}q^{\mathrm{maj}(\pi)}}{(q;q)_n}=\frac{\sum_{\pi\in\mathcal{W}(P,\omega)}q^{\mathrm{coch}(\pi\circ\pi_0)}}{(q;q)_n}.$$

が成り立つ. また

$$F_{\mathcal{A}}(P,\omega^*;q)=\frac{\sum_{\pi\in\mathcal{L}(P,\omega)}q^{\min(\pi)}}{(q;q)_n}=\frac{\sum_{\pi\in\mathcal{W}(P,\omega)}q^{\mathrm{ch}(\pi\circ\pi_0)}}{(q;q)_n}.$$

が成り立つことをみるのも容易である. Stanley は [5] の中で

$$q^n F_{\mathcal{A}}(P,w^*;q)=(-1)^n F_{\mathcal{A}}\left(P,w;\frac{1}{q}\right).$$

を示した. 同様にして reverse (P,ω)-partitions の母関数に関しては

$$F_{\mathcal{R}}(P,\omega;q)=\frac{\sum_{\pi\in\mathcal{L}(P,\omega)}q^{\min(\pi\circ\pi_0)}}{(q;q)_n}=\frac{\sum_{\pi\in\mathcal{W}(P,\omega)}q^{\mathrm{ch}(\pi)}}{(q;q)_n},$$

であり, また

$$F_{\mathcal{R}}(P,\omega^*;q)=\frac{\sum_{\pi\in\mathcal{L}(P,\omega)}q^{\mathrm{maj}(\pi\circ\pi_0)}}{(q;q)_n}=\frac{\sum_{\pi\in\mathcal{W}(P,\omega)}q^{\mathrm{coch}(\pi)}}{(q;q)_n},$$

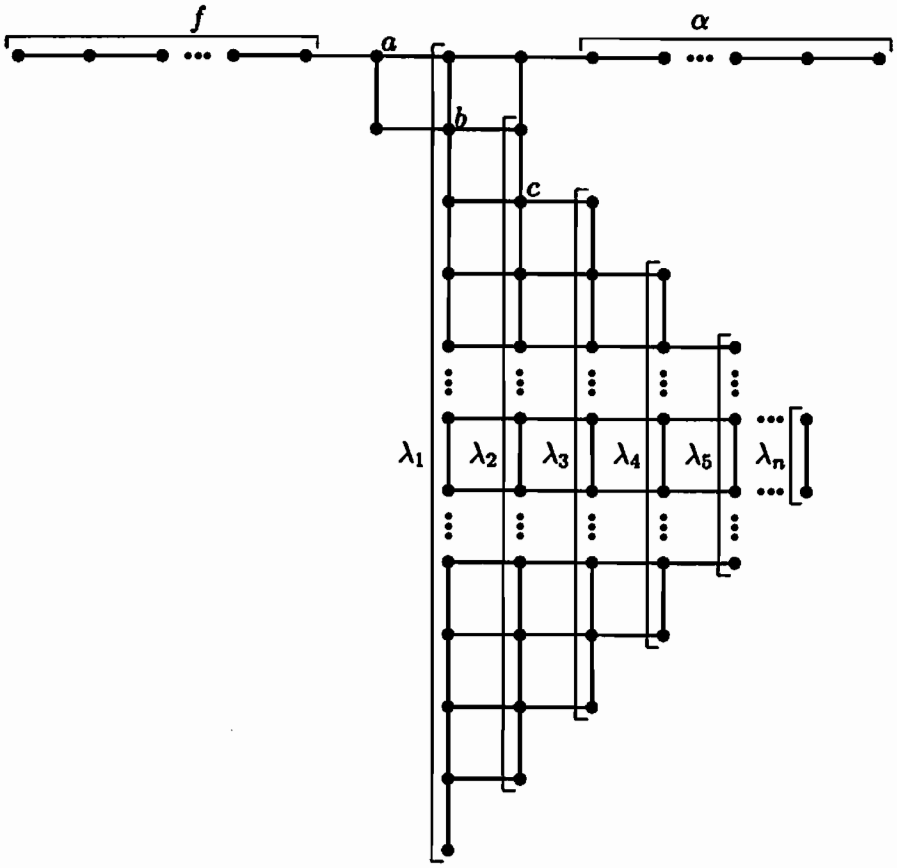
である. これ以降 (P,ω)-partitions のみを扱うことにする. そして混乱の恐れのない限り $F_{\mathcal{A}}(P,\omega;q)$ のかわりに $F(P,\omega;q)$ と書く. このことより charge や cocharge の母関数を求めるには適当な label ω を固定して (P,ω)-partitions の母関数を求めれば良いことがわかる.

3 Swivel Shifteds の場合

紙数の関係でここでは d-complete poset の定義を省略することにする. かわりに Swivel Shifteds と呼ばれる次のようなハッセ図形で定義される d-complete poset P に対して, raw-strict な label ω を定義し, その母関数 $F(P,\omega;q)$ を計算する.

raw-strict な labeling とは，上から下に弱い意味で単調増加，左から右に強い意味で単調増加になるような (P,ω)-partition を考えることである．

Swivel Shifteds $(f \geq \lambda_1 > \lambda_2 > \cdots > \lambda_n \geq 1, r \geq 5)$



このとき上図の主対角線上の 3 点での (P,ω)-partition の値を a, b, c とおき，lattice path method を使うと，このような (P,ω)-partition の母関数は次のような和で表される．ここでは紙数の関係で lattice path method についての詳しい説明は省略する．

$$\frac{q^{\binom{\alpha+3}{2}+\binom{2}{2}}}{(q;q)_{\alpha+2}(q;q)_1^2}\sum_{0\leq a<b<c}\begin{bmatrix}a\\f\end{bmatrix}q^{a+b+c}\begin{vmatrix}q^{(\alpha+2)a} & q^{(\alpha+2)b} & q^{(\alpha+2)c}\\ q^a & q^b & q^c\\ 1 & 1 & 1\end{vmatrix}\begin{vmatrix}q^a & q^b\\ 1 & 1\end{vmatrix}$$

$$\times\mathrm{pf}\begin{bmatrix}\frac{q^{\lambda_i+\lambda_j}}{(q;q)_{\lambda_i}(q;q)_{\lambda_j}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & \frac{1}{(q;q)_{\lambda_i-2}} & \frac{q^{(\lambda_i-2)b+(|\lambda|-\lambda_i-2)c}}{(q;q)_{\lambda_i-2}}\\ -\frac{1}{(q;q)_{\lambda_j-2}} & 0 & 0\\ -\frac{q^{(\lambda_j-2)b+(|\lambda|-\lambda_j-2)c}}{(q;q)_{\lambda_j-2}} & 0 & 0\end{bmatrix}$$

この和を直接, 計算すると次のような Pfaffian になることがわかる.

$$\frac{q^{\binom{\alpha+3}{2}+|\lambda|+(|\lambda|+\alpha+3)f}(q;q)_{|\lambda|+\alpha+2}}{(q;q)_\alpha(q;q)_1(q;q)_{|\lambda|+\alpha+f+3}}\frac{1}{(|\lambda|)_q(|\lambda|+1)_q(|\lambda|+\alpha+1)_q}$$
$$\times\mathrm{pf}\begin{bmatrix}\frac{q^{\lambda_i+\lambda_j}}{(q;q)_{\lambda_i}(q;q)_{\lambda_j}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & \frac{1}{(q;q)_{\lambda_i-2}} & A_i\\ -\frac{1}{(q;q)_{\lambda_j-2}} & 0 & 0\\ -A_j & 0 & 0\end{bmatrix}$$

ここで

$$A_i=\frac{1}{(q;q)_{\lambda_i-2}}\frac{1}{(|\lambda|-\lambda_i+\alpha+1)_q}\begin{vmatrix}\frac{q^{|\lambda|-\lambda_i-1}}{(|\lambda|-\lambda_i-1)_q} & \frac{(2|\lambda|+\alpha+1)_q}{(|\lambda|+\alpha+2)_q}\\ \frac{q^{|\lambda|-\lambda_i}}{(|\lambda|-\lambda_i)_q} & \frac{(2|\lambda|+\alpha)_q}{(|\lambda|+\alpha)_q}\end{vmatrix}$$

である. ここで書く主な結果は上の Pfaffian が次のような積で書けることである.

$$\frac{q^{\binom{\alpha+3}{2}+|\lambda|+(|\lambda|+\alpha+3)f-1}(q;q)_{|\lambda|+\alpha}}{(q;q)_\alpha(q;q)_{|\lambda|+\alpha+f+3}}\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\prod_{i=1}^{n}\frac{(|\lambda|+\lambda_i+\alpha+1)_q}{(|\lambda|-\lambda_i+\alpha+1)_q}$$

次の節でこの証明を述べる. 他の d-complete poset についても同様の方法が適用され現在 15 個の既約な d-complete poset のうち 8 個についてこのような積公式を証明した.

4 Pfaffian の評価

Lemma 4.1 n を偶数 $\lambda=(\lambda_1,\cdots,\lambda_n)$ を整数の列とするとき

$$\mathrm{pf}\left(\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\right)_{1\le i,j\le n}=\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}$$

Proof. Stembridge による有名な式であるが証明は次の式に帰着する.

$$\mathrm{pf}\left(\frac{x_j-x_i}{1-x_ix_j}\right)_{1\le i,j\le n}=\prod_{1\le i<j\le n}\frac{x_j-x_i}{1-x_ix_j}$$

ここでは, この式の証明は省略する.

Lemma 4.2 n を奇数 $\lambda=(\lambda_1,\cdots,\lambda_n)$ を整数の列とするとき

$$\mathrm{pf}\begin{pmatrix}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & (\lambda_i)_q\\ -(\lambda_j)_q & 0\end{pmatrix}=(|\lambda|)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\tag{1}$$

$$\mathrm{pf}\begin{pmatrix}q^{\lambda_i+\lambda_j}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & (\lambda_i)_q\\ -(\lambda_j)_q & 0\end{pmatrix}=(|\lambda|)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\tag{2}$$

Proof. 左辺を 第 $(n+1)$ 列について展開して上の補題を使うと

$$\sum_{k=1}^{n}(-1)^{k+1}(\lambda_k)_q\prod_{\substack{1\le i<j\le n\\ i,j\ne k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}=(|\lambda|)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}$$

を示せばよい．この両辺に $\prod_{1\le i<j\le n}(\lambda_i+\lambda_j)_q$ をかけると

$$\sum_{k=1}^{n}(-1)^{k+1}(\lambda_k)_q \prod_{\substack{1\le i<j\le n\\ i,j\neq k}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=1\\ i\neq k}}^{n}(\lambda_i+\lambda_k)_q=(|\lambda|)_q\prod_{1\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i}) \tag{3}$$

を示せば十分である．同様にしてもう1つの式を示すには

$$\sum_{k=1}^{n}(-1)^{k+1}q^{|\lambda|-\lambda_k}(\lambda_k)_q \prod_{\substack{1\le i<j\le n\\ i,j\neq k}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=1\\ i\neq k}}^{n}(\lambda_i+\lambda_k)_q=(|\lambda|)_q\prod_{1\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i}) \tag{4}$$

を示せば十分である．この後 n は奇数とは限らず，この2つの式が常に成り立つことを帰納法で示す．この式を q^{λ_1} の多項式と見れば q^{λ_1} について n 次式である．よって $(n+1)$ 個の異なる点で両辺が一致することを見れば良い．$l=2,\cdots,n$ に対して $q^{\lambda_1}=q^{\lambda_l}$ すなわち $\lambda_1=\lambda_l$ とすると右辺は明らかに 0 である．左辺は

$$(\lambda_1)_q\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})\prod_{i=2}^{n}(\lambda_i+\lambda_1)_q$$
$$+(-1)^{l+1}(\lambda_l)_q\prod_{\substack{1\le i<j\le n\\ i,j\neq l}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=1\\ i\neq l}}^{n}(\lambda_i+\lambda_l)_q$$

これを変形して

$$=(\lambda_l)_q\prod_{\substack{2\le i<j\le n\\ i,j\neq l}}(q^{\lambda_j}-q^{\lambda_i})\prod_{i=2}^{l-1}(q^{\lambda_l}-q^{\lambda_i})\prod_{i=l+1}^{n}(q^{\lambda_i}-q^{\lambda_l})(2\lambda_l)_q\prod_{\substack{i=2\\ i\neq l}}^{n}(\lambda_i+\lambda_l)_q$$
$$+(-1)^{l+1}(\lambda_l)_q\prod_{\substack{2\le i<j\le n\\ i,j\neq l}}(q^{\lambda_j}-q^{\lambda_i})\prod_{i=2}^{l-1}(q^{\lambda_i}-q^{\lambda_l})\prod_{i=l+1}^{n}(q^{\lambda_i}-q^{\lambda_l})(2\lambda_l)_q\prod_{\substack{i=2\\ i\neq l}}^{n}(\lambda_i+\lambda_l)_q$$

よって，これは 0 に等しい．まったく同様にして下の式も $q^{\lambda_1}=q^{\lambda_l}$ のとき，両辺とも 0 になることが示される．次に (3) の式の左辺の q^{λ_1} についての最高次の係数は

$$(-1)^n q^{\sum_{i=2}^{n}\lambda_i}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

であり，これは右辺の q^{λ_1} の最高次の係数と等しい．この式の左辺の q^{λ_1} についての定数項は

$$q^{\sum_{i=2}^{n}\lambda_i}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

となり，これは右辺の q^{λ_1} の定数項に等しい．最後に (3) の式の左辺の q^{λ_1} についての定数項は

$$\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})+\sum_{k=2}^{n}(-1)^{k+1}q^{|\lambda|-\lambda_1-\lambda_k}(\lambda_k)_q\prod_{\substack{2\le i<j\le n\\ i,j\neq k}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=2\\ i\neq k}}^{n}(\lambda_i+\lambda_k)_q$$

帰納法の仮定によりこれは

$$\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})-(|\lambda|-\lambda_1)_q\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

になり結局 $q^{|\lambda|-\lambda_1}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$ に等しいことがわかり，右辺の定数項と一致する．同様にして，(4) の式の左辺の q^{λ_1} の最高次の係数は

$$(-1)^n q^{2(|\lambda|-\lambda_1)}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$
$$+(-1)^n q^{|\lambda|-\lambda_1}\sum_{k=2}^{n}(-1)^k(\lambda_k)_q\prod_{\substack{2\le i<j\le n\\ i,j\neq k}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=2\\ i\neq k}}^{n}(\lambda_i+\lambda_k)_q$$

やはり帰納法の仮定により，これは

$$(-1)^n q^{2(|\lambda|-\lambda_1)}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})+(-1)^n q^{|\lambda|-\lambda_1}(|\lambda|-\lambda_1)_q\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

に等しく，これは $(-1)^n q^{|\lambda|-\lambda_1}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$ であり右辺の最高次の係数と一致する．

Lemma 4.3 n を奇数 $\lambda=(\lambda_1,\cdots,\lambda_n)$ を整数の列とするとき

$$\mathrm{pf}\begin{pmatrix} q^{\lambda_i+\lambda_j}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & (\lambda_i)_q(\lambda_i-1)_q \\ -(\lambda_j)_q(\lambda_j-1)_q & 0\end{pmatrix}=(|\lambda|)_q(|\lambda|-1)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} \tag{5}$$

Proof. 左辺の Pfaffian を第 n 列について展開し，最初の補題を用いると

$$\sum_{k=1}^{n}(-1)^{k+1}(\lambda_k)_q(\lambda_k-1)_q q^{|\lambda|-\lambda_k}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}=(|\lambda|)_q(|\lambda|-1)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} \tag{6}$$

を示せば良いことになる．両辺に $\prod_{1\le i<j\le n}(\lambda_i+\lambda_j)_q$ をかけることによって

$$\sum_{k=1}^{n}(-1)^{k+1}(\lambda_k)_q(\lambda_k-1)_q q^{|\lambda|-\lambda_k}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=1\\ i\neq k}}^{n}(\lambda_i+\lambda_k)_q$$
$$=(|\lambda|)_q(|\lambda|-1)_q\prod_{1\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

を示せば良いことになる．今後 n は奇数と仮定せずに任意の n に対してこの式が成り立つことを見る．この式の両辺を q^{λ_1} の多項式と見ると $(n+1)$ 次式である．よって $(n+2)$ 個の異なる点で，両辺が一致することを見れば良い．$l=2,\cdots,n$ に対して $q^{\lambda_1}=q^{\lambda_l}$ すなわち $\lambda_1=\lambda_l$ とすると右辺は明らかに 0 である．

一方, 左辺に $\lambda_1 = \lambda_l$ を代入すると,

$$(\lambda_1)_q(\lambda_1-1)_q q^{|\lambda|-\lambda_1}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})\prod_{i=2}^{n}(\lambda_i+\lambda_1)_q$$
$$+(-1)^{l+1}(\lambda_l)_q(\lambda_l-1)_q q^{|\lambda|-\lambda_l}\prod_{\substack{1\le i<j\le n\\ i,j\neq l}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=1\\ i\neq l}}^{n}(\lambda_i+\lambda_l)_q$$

となり, これは

$$(\lambda_l)_q(\lambda_l-1)_q q^{|\lambda|-\lambda_l}\prod_{\substack{2\le i<j\le n\\ i,j\neq l}}(q^{\lambda_j}-q^{\lambda_i})\prod_{i=2}^{l-1}(q^{\lambda_l}-q^{\lambda_i})\prod_{i=l+1}^{n}(q^{\lambda_i}-q^{\lambda_l})\prod_{i=2}^{n}(\lambda_i+\lambda_l)_q$$
$$+(-1)^{l+1}(\lambda_l)_q(\lambda_l-1)_q q^{|\lambda|-\lambda_l}\prod_{\substack{2\le i<j\le n\\ i,j\neq l}}(q^{\lambda_j}-q^{\lambda_i})\prod_{i=2}^{l-1}(q^{\lambda_i}-q^{\lambda_l})\prod_{i=l+1}^{n}(q^{\lambda_i}-q^{\lambda_l})\prod_{i=2}^{n}(\lambda_i+\lambda_l)_q$$

よって, これは 0 に等しい.

次に左辺の q^{λ_1} についての定数項は $k=1$ のところのみに現れて

$$q^{|\lambda|-\lambda_1}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

であり, これは右辺の定数項と一致する. また, 左辺の q^{λ_1} についての最高次の係数は $k=1$ のところのみに現れて

$$(-1)^{n+1}q^{-1+2(|\lambda|-\lambda_1)}\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

であり, これは右辺の最高次の係数と一致する. 最後に, もう 1 点で両辺が等しいことを言えばよいわけであるから $q^{\lambda_1}=1$ すなわち $\lambda_1=0$ を代入することにする. このとき, 左辺は

$$(-1)^n\prod_{i=2}^{n}(\lambda_i)_q\sum_{k=2}^{n}(-1)^{k+1}(\lambda_k)_q(\lambda_k-1)_q q^{\sum_{i\neq k}^{n}\lambda_i}\prod_{\substack{2\le i<j\le n\\ i,j\neq k}}(q^{\lambda_j}-q^{\lambda_i})\prod_{\substack{i=2\\ i\neq k}}^{n}(\lambda_i+\lambda_k)_q$$

となる. 帰納法により, これは

$$(-1)^{n+1}\prod_{i=2}^{n}(\lambda_i)_q\Big(\sum_{i=2}^{n}\lambda_i\Big)_q\Big(\sum_{i=2}^{n}\lambda_i-1\Big)_q\prod_{2\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})$$

に等しいので, これは右辺に $\lambda_1=0$ を代入したものと同じであることがわかる.

Theorem 4.4 n を偶数 $\lambda=(\lambda_1,\cdots,\lambda_n)$ を整数の列とするとき

$$p=\mathrm{pf}\begin{pmatrix} q^{\lambda_i+\lambda_j}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & (\lambda_i)_q(\lambda_i-1)_q & B_i \\ -(\lambda_j)_q(\lambda_j-1)_q & 0 & 0 \\ -B_j & 0 & 0 \end{pmatrix}$$

とおく．ただし

$$B_i=\frac{(\lambda_i)_q(\lambda_i-1)_q}{(|\lambda|-\lambda_i+\alpha+1)_q}\begin{vmatrix} \frac{q^{|\lambda|-\lambda_i-1}}{(|\lambda|-\lambda_i-1)_q} & \frac{(2|\lambda|+\alpha+1)_q}{(|\lambda|+\alpha+2)_q} \\ \frac{q^{|\lambda|-\lambda_i}}{(|\lambda|-\lambda_i)_q} & \frac{(2|\lambda|+\alpha)_q}{(|\lambda|+\alpha)_q} \end{vmatrix}$$

である．このとき

$$p=\frac{q^{-1}(1)_q(|\lambda|)_q(|\lambda|-1)_q}{(|\lambda|+\alpha+2)_q}\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\prod_{i=1}^{n}\frac{(|\lambda|+\lambda_i+\alpha+1)_q}{(|\lambda|-\lambda_i+\alpha+1)_q} \qquad (7)$$

が成り立つ．

Proof. 上の Pfaffian を第 n 列について展開して前の補題を用いると示すべき式は次のようになる．

$$\sum_{k=1}^{n}(-1)^{k+1}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\frac{(\lambda_k)_q(\lambda_k-1)_q}{(|\lambda|-\lambda_k+\alpha+1)_q}\begin{vmatrix} q^{|\lambda|-\lambda_k-1}(|\lambda|-\lambda_k)_q & \frac{(2|\lambda|+\alpha+1)_q}{(|\lambda|+\alpha+2)_q} \\ q^{|\lambda|-\lambda_k}(|\lambda|-\lambda_k-1)_q & \frac{(2|\lambda|+\alpha)_q}{(|\lambda|+\alpha)_q} \end{vmatrix}$$
$$=\frac{q^{-1}(1)_q(|\lambda|)_q(|\lambda|-1)_q}{(|\lambda|+\alpha+2)_q}\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\prod_{i=1}^{n}\frac{(|\lambda|+\lambda_i+\alpha+1)_q}{(|\lambda|-\lambda_i+\alpha+1)_q}$$

この両辺に $(|\lambda|+\alpha)_q(|\lambda|+\alpha+2)_q\prod_{i=1}^{n}(|\lambda|-\lambda_i+\alpha+1)_q$ をかけると次の式を示せば十分である．

$$\sum_{k=1}^{n}(-1)^{k+1}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}(\lambda_k)_q(\lambda_k-1)_q\prod_{\substack{i=1\\ i\neq k}}^{n}(|\lambda|-\lambda_i+\alpha+1)_q$$
$$\times\begin{vmatrix} q^{|\lambda|-\lambda_k-1}(|\lambda|-\lambda_k)_q & (2|\lambda|+\alpha+1)_q(|\lambda|+\alpha)_q \\ q^{|\lambda|-\lambda_k}(|\lambda|-\lambda_k-1)_q & (2|\lambda|+\alpha)_q(|\lambda|+\alpha+2)_q \end{vmatrix}$$
$$=q^{-1}(1)_q(|\lambda|)_q(|\lambda|-1)_q(|\lambda|+\alpha)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\prod_{i=1}^{n}(|\lambda|+\lambda_i+\alpha+1)_q$$

この式を q^α についての多項式と見ると両辺とも q^α についての $(n+1)$ 次式である．よって $(n+2)$ 個の異なる点で両辺が同じ値を取ることを示せば十分である．まず $\alpha=\lambda_l-|\lambda|-1$ $(l=1,\cdots,n)$ を代入する．このとき左辺は

$$(-1)^{l+1}\prod_{\substack{1\le i<j\le n\\ i,j\neq l}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}(\lambda_l)_q(\lambda_l-1)_q\prod_{\substack{i=1\\ i\neq l}}^{n}(\lambda_l-\lambda_i)_q$$
$$\times\begin{vmatrix} q^{|\lambda|-\lambda_l-1}(|\lambda|-\lambda_l)_q & (2|\lambda|+\alpha+1)_q(|\lambda|+\alpha)_q \\ q^{|\lambda|-\lambda_l}(|\lambda|-\lambda_l-1)_q & (2|\lambda|+\alpha)_q(|\lambda|+\alpha+2)_q \end{vmatrix}$$

この行列式を実際に直接計算すると，これは

$$(-1)^{l+1}q^{-1}\prod_{\substack{1\le i<j\le n\\ i,j\neq l}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}(\lambda_l)_q(\lambda_l-1)_q\prod_{\substack{i=1\\ i\neq l}}^{n}(\lambda_l-\lambda_i)_q$$
$$\times(1)_q(|\lambda|)_q(|\lambda|-1)_q\frac{(2\lambda_l)_q}{(\lambda_l)_q}q^{|\lambda|-\lambda_l-1}$$

に等しい. よって結果として左辺は

$$q^{-1}\frac{\prod_{1\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})}{\prod_{\substack{1\le i<j\le n\\ i,j\neq l}}(\lambda_i+\lambda_j)_q}(1)_q(|\lambda|)_q(|\lambda|-1)_q(2\lambda_l)_q(\lambda_l-1)_q$$

になる. 一方, 右辺は

$$\begin{aligned}&q^{-1}(1)_q(|\lambda|)_q(|\lambda|-1)_q(\lambda_l-1)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\prod_{i=1}^{n}(\lambda_i+\lambda_l)_q\\ =&q^{-1}(1)_q(|\lambda|)_q(|\lambda|-1)_q(\lambda_l-1)_q(2\lambda_l)_q\frac{\prod_{1\le i<j\le n}(q^{\lambda_j}-q^{\lambda_i})}{\prod_{\substack{1\le i<j\le n\\ i,j\neq l}}(\lambda_i+\lambda_j)_q}\end{aligned}$$

ゆえに両辺は一致する. つぎに $\alpha=-|\lambda|$ を代入すると左辺は

$$\begin{aligned}&\sum_{k=1}^{n}(-1)^{k+1}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}(\lambda_k)_q(\lambda_k-1)_q\prod_{\substack{i=1\\ i\neq k}}^{n}(1-\lambda_i)_q q^{|\lambda|-\lambda_k-1}(|\lambda|-\lambda_k)_q(|\lambda|)_q(2)_q\\ &=(-1)^{n-1}q^{n-2}(2)_q(|\lambda|)_q\prod_{i=1}^{n}(\lambda_i-1)_q\sum_{k=1}^{n}(-1)^{k+1}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}(\lambda_k)_q(|\lambda|-\lambda_k)_q\\ &=(-1)^{n-1}q^{n-2}(2)_q(|\lambda|)_q\prod_{i=1}^{n}(\lambda_i-1)_q\mathrm{pf}\begin{pmatrix}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q} & (\lambda_i)_q(|\lambda|-\lambda_i)_q\\ -(\lambda_j)_q(|\lambda|-\lambda_j)_q & 0\end{pmatrix}\end{aligned}$$

この Pfaffian が 0 になることは前の補題と同様にして示せる. これは右辺に $\alpha=-|\lambda|$ を代入した値と一致する.

最後に両辺の q^{α} に関する定数項を比較する. まず左辺は

$$\begin{aligned}&\sum_{k=1}^{n}(-1)^{k+1}\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}(\lambda_k)_q(\lambda_k-1)_q\begin{vmatrix}q^{|\lambda|-\lambda_k-1}(|\lambda|-\lambda_k)_q & 1\\ q^{|\lambda|-\lambda_k}(|\lambda|-\lambda_k-1)_q & 1\end{vmatrix}\\ &=\sum_{k=1}^{n}(-1)^{k+1}q^{|\lambda|-\lambda_k-1}(1)_q(\lambda_k)_q(\lambda_k-1)_q\prod_{\substack{1\le i<j\le n\\ i,j\neq k}}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\\ &=q^{-1}(1)_q(|\lambda|)_q(|\lambda|-1)_q\prod_{1\le i<j\le n}\frac{q^{\lambda_j}-q^{\lambda_i}}{(\lambda_i+\lambda_j)_q}\end{aligned}$$

ここで最後の式は前の補題を使った. これは右辺の q^{α} に関する定数項に一致する.

これによって Swivel Shifteds の場合の証明が終わった. 最後に他の場合も良く似た方法で証明できることを注意しておく.

Masao Ishikawa, Department of Mathematics, Faculty of Education,
Tottori University, Tottori 680 8551, Japan
E-mail address: ishikawa@fed.tottori-u.ac.jp

Hiroyuki TAGAWA, Department of Mathematics, Faculty of Education,
Wakayama University, Wakayama 640 8510, Japan
E-mail address: tagawa@math.edu.wakayama-u.ac.jp

References

[1] M.Ishikawa and M.Wakayama *Minor summation formula of Pfaffians*, Linear and Multilinear Alg. **39** (1995), 285-305

[2] I.G.Macdonald *Symmetric Functions and Hall Polynomials, 2nd Edition* Oxford University Press, 1995.

[3] R. A. Proctor, *Minuscule elements of Weyl groups, the numbers game, and d-complete posets Lattices and of d-Complete Posets*, J. Alg. **213** (1999), 272-303.

[4] R. A. Proctor, *Dynkin Diagram Classification of λ-Minuscule Bruhat Lattices and of d-Complete Posets*, Journal of Algebraic Combinatorics **9** (1999), 61-94.

[5] R. P. Stanley, *Ordered structures and partitions*, Mem. of Amer. Math. Soc., **119** (1972).

[6] R. P. Stanley, *Enumerative Combinatorics Vol.I*, Wadsworth & Brooks /Cole Mathematics Series, 1986.

[7] J.Stembridge *Nonintersecting paths, pfaffians and plane partitions*, Adv. Math. **83** (1990), 96–131

[8] J.Stembridge *Enriched P-partitions, Trans. Ameri. Math. Soc.*, **349** (1997), 763–788

On Siegel modular forms of half integral weights of $\Gamma_0(4)$ of degree two

Tomoyoshi Ibukiyama
伊吹山知義（大阪大学理学研究科）

次数2のジーゲル保型形式で、離散群 $\Gamma_0(4)$ に属する重さ半整数のものを具体的に全部記述する。結論は十分単純であり、weighted polynomial ring にある関数をかけたものになっている。また、これらの保型形式の一部（プラススペースと呼ばれる）は次数2の Jacobi form と対応があるが、これについて、林田秀一氏（阪大博士課程）が具体的な計算を実行しており、これについても少し述べる。

筆者の研究は、対馬龍司氏が代数幾何学的手法により、このような保型形式の次元を計算したことに端を発しているし、これは計算の途上で大変助けになっている。しかし結果的に言えば、彼の次元公式は用いない別証が得られている。（ここでは証明は述べないのであるが。）なお、B. Runge [12] は $Sp(2,\mathbb{Z})$ と $\Gamma^*(2,4)$ の間にあるいくつかの群について、保型形式の構造を論じている。これから言えば、一見 Runge の記号で H_2 という untary reflection group から、その部分群の不変部分として $\Gamma_0(4)$ の半整数ウェイトの保型形式を求めることが可能であるように見えるかもしれない。しかし、H_2 は本質的に2重被覆群であり、その中で $\Gamma_0(4)$ や $\Gamma^*(2,4)$ のセクションが正確に論じられているわけではなく（つまり半整数ウェイトの保型因子を正確に与えて議論しているわけではなく）、直接は適用はできない。実際、我々の半整数ウェイトの保型形式は、彼の取り扱った保型形式の中には含まれていない。また、たとえ整数ウェイトに話を限っても、奇数ウェイトはいわゆる theta constants of the second kind では記述されてもいないので、この部分に限っても純粋に unitary reflection group の話というわけではない。以上のように、あれやこれやで、Runge の論文から具体的な記述が直ちにやさしくできるというわけではない。ここではこのような理論から離れて、直接結果を与える。（関連は本文中でも少しふれる。）

なお、以前に立教大学で話した折に、落合啓之氏より生成元の簡易化についてコメントを受けた。以下はこの点で私の当初の記述より若干簡単になっている部分がある。この点彼に感謝したい。

1　保型形式環と半整数ウェイトの保型形式

$Sp(2,\mathbb{Z})$ を行列サイズ4の普通のジーゲルモジュラー群《整数係数のシンプレクティック群》とする。自然数 N　について、合同部分群

$$\Gamma_0(N)=\{g=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in Sp(2,\mathbb{Z});\ C\equiv 0 \bmod N\}$$

をとる。これの共役をとるほうが見やすいこともあるので

$$\rho_2=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix},$$

として $\Gamma=\rho_2^{-1}\Gamma_0(4)\rho_2$ とおく。. すると

$$\Gamma=\{g=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in Sp(2,\mathbb{Z});\ B\equiv C\equiv 0 \bmod 2\}$$

である。

$$g=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\in \Gamma_0(4),\ \text{または}\ \Gamma,$$

について $\psi(g)=(\frac{-1}{\det(D)})$ (ルジャンドル記号) とおくと、これは $\Gamma_0(4)$ または Γ の指標である。整数 k と $Sp(n,\mathbb{R})$ の離散群 Γ' で $\mathrm{vol}(\Gamma'\backslash Sp(n,\mathbb{R}))<\infty$ なるもの、Γ' の指標 χ、および2次ジーゲル上半空間 $\mathfrak{H}_2=\{Z=X+iY={}^tZ\in M_2(\mathbb{C});X,Y,\mathrm{real},Y>0\}$ の関数 F について

$$(F|_{k,\chi}\gamma)(\tau)=\chi(\gamma)^{-1}\det(C\tau+D)^{-k}F(\tau)$$

と書く。$\mathfrak{H}_2$ 上の正則関数 F がすべての $\gamma\in\Gamma'$ について

$$F|_{k,\chi}\gamma=F$$

を満たすとき、F を Γ' のウェイト k、指標 χ の（正則）保型形式という。各カスプ（佐武コンパクト化の境界）で消えれば、カスプ形式という。正則保型形式の空間を $A_k(\Gamma',\chi)$、カスプ形式の空間を $S_k(\Gamma',\chi)$ と書く。χ が自明ならば χ を略す。簡単のために

$$A(\Gamma',\chi)=\oplus_{k=0}^{\infty}A_k(\Gamma',\chi^k)$$

と書こう。
次は知られている。

Proposition 1.1 (Tsushima [15])

$$\sum_{k=0}^{\infty} \dim A_k(\Gamma_0(4), \psi^k)t^k = \frac{1+t+t^3+t^4}{(1-t^2)^3(1-t^6)}.$$

われわれは、ここでは具体的に空間を記述したい。まず $\oplus_{k=0}^{\infty} A_k(\Gamma_0(4), \psi^k)$ を求めたいが、$\Gamma_0(4)$ のかわりに Γ を考える。その理由は、$\Gamma \subset \Gamma_0(2)$ であり、$A(\Gamma_0(2))$ は [4] ですでにわかっているからである。次のようにおく。

$$\begin{aligned}
X &= ((\theta_{0000})^4 + (\theta_{0001})^4 + (\theta_{0010})^4 + (\theta_{0011})^4)/4 \\
f_2 &= (\theta_{0000})^4 \\
g_2 &= (\theta_{0000})^4 + (\theta_{0100})^4 + (\theta_{1000})^4 + (\theta_{1100})^4 \\
Y &= (\theta_{0000}\theta_{0001}\theta_{0010}\theta_{0011})^2 \\
Z &= ((\theta_{0100})^4 - (\theta_{0110})^4)^2/16384, \\
K &= (\theta_{0100}\theta_{0110}\theta_{1000}\theta_{1001}\theta_{1100}\theta_{1111})^2/4096, \\
f_1 &= (\theta_{0000})^2, \\
f_3 &= (\theta_{0001}\theta_{0010}\theta_{0011})^2, \\
\theta &= \theta_{0000}\theta_{0001}\theta_{0010}\theta_{0011}\theta_{0100}\theta_{0110}\theta_{1000}\theta_{1001}\theta_{1100}\theta_{1111}, \\
f_6 &= (\theta_{0001}^4 - \theta_{0010}^4)(\theta_{0001}^4 - \theta_{0011}^4)(\theta_{0010}^4 - \theta_{0011}^4), \\
f_{11} &= f_6\theta, \\
f_{21/2} &= f_{11}/\theta_{0000}.
\end{aligned}$$

ここで θ_m は characteristic m (mod2) のテータ定数である。定義は Igusa [9] 参照。

Proposition 1.2 関数 X, f_2, g_2, Z, Y, K, f_{11} はそれぞれ Γ のウェイト *2, 2, 2, 4, 4, 6, 11* の保型形式である。f_1 と f_3 は Γ の指標 ψ のウェイト *1* ないしは *3* の保型形式である。とくに X, Y, Z, K は $\Gamma_0(2)$ の保型形式である。

次のような関係がなりたつ。

$$f_1^2 = f_2, \qquad f_1 f_3 = Y, \qquad Z = (g_2 + 2X - 3f_2)^2/36864$$

$f_{21/2}$ はもちろん正則である。

Theorem 1.3 保型形式環 $A(\Gamma, \psi)$ は

$$A(\Gamma, \psi) = \mathbb{C}[f_1, f_3, g_2, X]$$

で与えられる。ここで f_1, f_3, g_2, X は代数的に独立である。また、$B = \mathbb{C}[X, f_2, g_2, K]$ とおくと

$$A(\Gamma) = B \oplus YB \oplus f_{11}(B \oplus YB)$$

である。

ここで $\oplus$ は加群としての直和を表す。ちなみに

$$\begin{aligned} f_3^2 &= -4096K + \frac{1}{9}f_2(4g_2X - 6f_2g_2 + 24f_2X + g_2^2 - 32X^2) + Y(4X - 2f_2) \\ &= -4096K + f_2(4096Z - f_2^2 + 4f_2X - 4X^2) + Y(4X - 2f_2), \\ f_1^2 &= f_2, \\ Y &= f_1f_3 \end{aligned}$$

などがなりたつ。f_{11}^2 の公式は略す。

注意：$A(\Gamma,\psi)$ についてのこの結果は、詳細を詰めていない部分があるが、Shephard-Todd の表の No. 2 の unitary reflection group で、$m=2, q=1, n=4$ のときの不変式環に相当すると思う。なお不変式の次数は、2，4，4，6であり、もとの多項式環は、Runge のいう 4 つの theta constants of second kind であろう。しかし、unitary reflection group H_2 の部分群をそのまま考えればよいわけではなく、作用を変更する必要がある。
なお、上の環 $A(\Gamma,\psi)$ において、奇数ウェイトでは指標つきであるが、偶数ウェイトでは定義により、$\psi^k=1$ になっているから指標がついていない。この部分を以下に補う。

Theorem 1.4 Γ の指標つきの偶数ウェイトの保型形式のなすベクトル空間は

$$\oplus_{k=0}^{\infty}A_{2k}(\Gamma,\psi) = f_{11}(f_1B \oplus f_3B)$$

で与えられる。

もちろん以上の結果を $\Gamma_0(4)$ の結果に書きなおすのはやさしい。実際

$$A_k(\Gamma_0(4),\psi) = \{F(2\tau); F \in A_k(\Gamma,\psi)\}, \qquad A_k(\Gamma_0(4)) = \{F(2\tau); F \in A_k(\Gamma)\}$$

であり、$\theta_m(2\tau)^2$ は望むなら、いわゆる「倍角」の公式でふつうのテータ定数で書くこともできる。
半整数ウェイトの保型形式の定義は、保型因子として、$(\theta_{0000}(2M\tau)/\theta_{0000}(2\tau))^k$ $(M \in \Gamma_0(4))$ をもちいる。この保型因子に対応する保型形式を、ウェイト $k/2$ という。指標つきの意味は整数ウェイトのときと同じに定義される。ちなみに $M \in \Gamma_0(4)$ について $(\theta_{0000}(2M\tau)/\theta_{0000}(2\tau))^2 = \psi(M)$ に注意しておく。
これらの空間を $A_{k+1/2}(\Gamma_0(4))$, $A_{k+1/2}(\Gamma_0(4),\psi)$ などと書くことにする。半整数ウェイトだけならば、k を動かしても、環ではなく、単にベクトル空間である。対馬により

$$\sum_{k=0}^{\infty}\dim A_{k+1/2}(\Gamma_0(4))t^k = \frac{1+t+t^3+t^4}{(1-t^2)^3(1-t^6)}.$$

が知られているが、ベクトル空間そのものについては知られていなかった。これは次で与えられる。

Theorem 1.5

$$\oplus_{k=0}^{\infty} A_{k+1/2}(\Gamma_0(4)) = \theta_{0000}(2\tau)(\oplus_{k=0}^{\infty} A_k(\Gamma_0(4), \psi^k)).$$

半整数に限らず、$\theta_{0000}(2M\tau)/\theta_{0000}(2\tau)$ のベキを保型因子にもつ環 $A^{(1/2)}(\Gamma_0(4))$ をまとめて考えると、いっそう単純であり

$$A^{(1/2)}(\Gamma_0(4)) = \mathbb{C}[\theta_{0000}(2\tau), g_2(2\tau), X(2\tau), f_3(2\tau)]$$

となる。
なお、$A_{k+1/2}(\Gamma)$ の半整数ウェイトのカスプ形式は $\oplus M_{2k}(\Gamma)$ 加群として次で生成される。(独立ではない。依存関係は省略するが正確に書ける。)

$$\begin{array}{rr} K & (g_2-4X)(g_2+8X-6f_2)(g_2+2X-3f_2) \\ f_3(3f_2-2X-g_2) & (g_2-4X)((-3f_3+f_1(g_2+8X-6f_2). \end{array}$$

指標つきの半整数ウェイト保型形式は以下で与えられる。

Theorem 1.6

$$\oplus_{k=0}^{\infty} A_{k+1/2}(\Gamma,\psi) \;=\; f_{21/2}(\oplus_{k=0}^{\infty} M_k(\Gamma,\psi^k)).$$

証明はすべて省略する。準備中の論文 [8] を参照されたい。

2 Jacobi forms and plus space

しばらく一般の次数のジーゲル上半空間で考える。k が偶数の時、半整数ウェイト $k-1/2$ の $\Gamma_0(4)$ の n 次の保型形式の plus space と呼ばれる部分空間 $A^+_{k-1/2}(\Gamma_0(4))$ があって、インデックス 1、ウェイト k の $Sp(2,\mathbb{Z})$ に属するヤコービ形式の空間 $J_{k,1}(Sp(n,\mathbb{Z}))$ と線形同型になることが知られている。(1 変数で Kohnen [11] が最初に示し、後に Ibukiyama [7] で plus space の定義の拡張が行われ、多変数へ一般化された。) ここでは plus space は、フーリエ係数の現れ方で特徴づけられる。すなわち、$f(\tau) \in A_{k-1/2}(\Gamma_0(4))$ は

$$f(\tau) = \sum_T a(T) e^{2\pi i \mathrm{tr}(T\tau)}$$

(ただし T は半整数対称行列、つまり対角成分が整数でその他が $2^{-1}\mathbb{Z}$ に属する対称行列) とフーリエ展開できる。実際には T が半正定値でなければ $a(T)=0$ である。さて、plus space の条件はフーリエ係数への代数的な条件である。すなわち、ある縦ベクトル μ について、$T+\mu\,{}^t\mu$ が

半整数対称行列の4倍に等しいとき以外は $a(T)=0$ となるような保型形式は線形部分空間をなすが、これを plus space と呼ぶ。さて、[7] では k が偶数と仮定されていたが、この結果をそのまま模倣することにより k が奇数のときに、指標付き半整数ウェイトの plus space が林田秀一により定義され、やはりウェイト $k-1/2$ の保型形式とウェイト k、インデックス1のヤコービ形式との同型が示された。以上の説明よりわかるように、plus space とはいわば new form のようなものであり、この空間を求める方が望ましい。
さて、対馬氏は、次数 $n=2$ については、Jacobi form の次元公式も得ている。以下の通りである。(対馬 [16])

$$\sum_{k=0}^{\infty} \dim J_{k,1}(Sp(2,\mathbb{Z}))t^k = \frac{t^4+t^6+t^{10}+t^{12}+t^{21}+t^{27}+t^{29}+t^{35}}{(1-t^4)(1-t^6)(1-t^{10})(1-t^{12})}.$$

一方で、$f(\tau) \in A_k(Sp(2,\mathbb{Z}))$ ならば、$f(4\tau)$ のフーリエ係数はあきらかに T が4の倍数のときのみ現れるから、$R=\{f(4\tau); f \in A_k(Sp(2,\mathbb{Z}) \text{ for some } k\}$ とすれば、plus space は環 R 上の加群になる。対馬の次元公式はこれが自由加群であることを示唆しているが、実際にこれを証明するには具体的に書いてみる必要がある。林田はかなり面倒な計算機実験により、この R 加群としての生成元8個を具体的に確定し、R 上独立なことを示した([1] および最近の新結果。) よって、plus space も確定したことになるが、結論の具体的な保型形式はきわめて複雑であり、今のところ残念ながらここで簡単に記述できるような形にはなっていない。

参考文献

[1] 林田秀一、次数2、重さ半整数 Siegel modular form の部分空間 plus space における重さ 23/2 までの決定, 大阪大学修士論文、１９９９年２月。

[2] T. Ibukiyama, On symplectic Euler factors of genus two, J. Fac. Sci. Univ. Tokyo Sect. IA, Vol.30(1984),587-614.

[3] T. Ibukiyama, On relations of dimensions of automorphic forms of $Sp(2,\mathbb{R})$ and its compact twist Sp(2) (I), Advanced Studies in Pure Mathematics 7 (1985), 7-29.

[4] T. Ibukiyama, On Siegel modular varieties of level 3, International J. Math. Vol.2 No.1(1991),17-35.

[5] T. Ibukiyama, On some alternating sum of dimensions of Siegel cusp forms of general degree and cusp configurations J. Fac. Sci. Univ. Tokyo Sect. IA 40 (1993),245-283.

[6] T. Ibukiyama and F. Onodera, On the graded ring of modular forms of the Siegel paramodular group of level 2, Abh. Math. Sem. Univ. Hamburg 67(1997), 297–305.

[7] T. Ibukiyama, On Jacobi forms and Siegel modular forms of half integral weights, Commentarii Math. St. Pauli, Vol. 41, No. 2 (1992), 109–124.

[8] T. Ibukiyama and S. Hayashida, Siegel modular forms of half integral weights of $\Gamma_0(4)$ and the plus space, in preparation.

[9] J. Igusa, On Siegel modular forms of genus two (II), Amer. J. Math. 86(1964),392-412.

[10] J. Igusa, On the graded ring of theta constants, Amer. J. Math. 86(1964),219-246.

[11] Modular forms of half-integral weight on $\Gamma_0(4)$, Math. Ann. 248(1980),249-266.

[12] B. Runge, On Siegel modular forms, J. reine angew. Math. 436 (1993), 57–85.

[13] I. Satake, L'opérateur Φ, Séminaire H. Cartan 1957/58 Exposé 14(1958),1-18.

[14] R. Tsushima, Dimension formula for the Spaces of Siegel cusp forms and a certain exponential sum, preprint.

[15] R. Tsushima, A letter to the author, November, 1997.

[16] R. Tsushima, On the dimension formula for the spaces of Jacobi forms of degree two, 数理研講究録 No. 1103 (1999), 96–110.

Department of Mathematics,
Graduate School of Science,
Osaka University,
Machikaneyama 1-16,
Toyonaka, Osaka, 560-0043 Japan.
ibukiyam@math.wani.osaka-u.ac.jp