

# 散在型単純群の周辺

北詰 正顕 (Masaaki Kitazume)

千葉大学大学院理学研究科

## 0 はじめに

本稿では、散在型単純群の周辺について、特に、最近の筆者（を含むグループ）の研究対象となっている、符号・グラフ・デザインを中心に話を進めていきたいと思う。

本論に入る前に、群を記述する記号について、簡単にまとめておく。個々の群を表す記号については [8] を参照されたい。

$G \cong A.B$  と書いたら、 $G$  が  $A$  と同型な正規部分群を持ち、その剰余群が  $B$  と同型であることを意味する：

$$\exists K \subset G : \text{normal subgroup s.t. } K \cong A, G/K \cong B$$

いわゆる群の拡大を表すわけで、この条件で群  $G$  の構造が一意に決まるとは限らない。これが、分裂 (split) 拡大になっていることを明示するときは  $A:B$ 、非分裂 (non-split) 拡大になっていることを明示するときは  $A \cdot B$  と書くこともある。素數位数  $p$  の巡回群を、単に  $p$  と表し、位数  $p^n$  の基本可換群 (elementary abelian group) を  $p^n$  と表す。記号  $p^{a+b}$  は群の拡大  $p^a.p^b$  を表すものとする。特に  $p^{1+n}$  は extra special group と呼ばれるものである。

位数 2 の元のことを involution と呼ぶ。その中心化群の構造が、有限単純群を扱う際に重要となる。一般に位数  $n$  の共役類を、その位数とアルファベットを用いて、 $nA, nB, \dots$  などと表す。その記号を冠して、 $2A$ -involution などという書き方をする。

いくつかの用例を挙げておく。対称群と交代群の関係は  $S_n \cong A_n:2$  と書かれる。交代群の自己同型群  $\text{Aut}(A_n)$  は一般に  $S_n$  と同型であるが、 $n=6$  のときのみ例外で  $\text{Aut}(A_6) \cong A_6 \cdot 2^2$  となる。この中に  $A_6$  を指数 2 で含む群は 3 つ存在する：

$$S_6, PGL(2, 9)(\cong A_6:2), M_{10}(\cong A_6 \cdot 2)$$

モンスター単純群の involution の共役類は 2 つ ( $2A, 2B$ ) で、その中心化群は、それぞれ

$$2 \cdot BM, 2^{1+24} \cdot Co_1$$

( $BM$  はベビーモンスター、 $Co_1$  は Conway 群と呼ばれる単純群) という構造である。

# 1 散在型単純群

ここでは、歴史などを振り返りながら、散在型単純群の概略を説明したいと思う。全般的な参考文献として ATLAS [8] の他に、鈴木通夫 [21] と、M. Ronan の本の最近の翻訳 [22] を挙げておこう。

## 1.1 分類定理と、散在型単純群一覧

次の定理が、いわゆる「有限単純群の分類定理」である。1980 年頃に、証明が完了したと宣言され、その文献のすべてが 2004 年に出そろったとされる。

**定理 1.** 有限単純群は、次のいずれかに分類される。

(0) 素数位数の巡回群

(1) 5 次以上の交代群  $A_n$  ( $n \geq 5$ )

(2) Lie 型の単純群

$$A_n(q), B_n(q), C_n(q), D_n(q), E_6(q), E_7(q), E_8(q), F_4(q), G_2(q) \\ {}^2A_n(q), {}^2B_n(q), {}^2D_n(q), {}^3D_4(q), {}^2E_6(q), {}^2F_4(q), {}^2G_2(q)$$

(3) 26 個の散在型単純群

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, J_3, J_4, HS, Suz, McL, He, \\ Ru, Ly, ON, Co_1, Co_2, Co_3, F_{22}, F_{23}, F'_{24}, H, Th, BM, M.$$

上記の中には、重複して分類されるものもある。例えば、交代群の中に Lie 型の群と見なされる例

$$A_5 \cong L_2(4)(= A_1(4)), A_8 \cong L_4(2)(= A_3(2))$$

があるし、Lie 型の群の中で 2 通り (以上) の見方が可能なこと

$$U_4(2) \cong S_4(3) \cong O_5(3), U_3(3) \cong G_2(2)'$$

がある (特に、このような標数の違う群の一致は興味深い)。散在型単純群は (言葉の定義から言って) 交代群や Lie 型の群のような無限系列には含まれない。しかし、散在型でない群を、散在型へ至る系列の中に入れた方が良いという場合もある。典型的な例が

$$L_3(4) \cong M_{21}, U_6(2) \cong F_{21}$$

である。また、いわゆる Tits 群  $T$  は、

$$T \cong {}^2F_4(2)'$$

という同型を持つが、交換子群 ( $'$ ) で表している) をとらないと単純群にならないという意味で  ${}^2F_4(2)$  は極めて例外的な "Lie 型の単純群" である。(上記の  $G_2(2)$  も同様であるが、これは  ${}^2A_2(3) \cong U_3(3)$  と見れば立派な Lie 型の単純群である。) それ故、Tits 群は限りなく散在型に近い Lie 型の単純群であるとも言えて、有限単純群のデータベースとも言える Web page [1] では、こっそりと (?) Tits 群  $T$  が散在型単純群の中に混ぜられていたりする。

最後に (余談だが) このような例外的な同型対応が、交代群  $A_6$  のところに集中して現れていること

$$A_6 \cong L_2(9) \cong S_4(2)' \cong M'_{10}$$

は注目すべきことである。この群は、この性質故に (小さい群であることももちろんあるだろうが)、様々な場面で出くわすものである。 $A_6$  を見るたびに、鈴木通夫先生の「群論」[20] の一節 ( $\text{Aut } A_6 \neq S_6$  を受けて)

この例外が有限群論に及ぼす影響は非常に大きく、単純群論をととても困難なものにしている大きな理由の一つである

を思い出すものである。例外的な自己同型があるため、 $A_6$  を指数 2 で含む群として、

$$S_6, PGL(2, 9), M_{10}$$

という 3 つが存在しうるのである。

さて、26 個の散在型単純群につけられた記号は、多くの場合発見者を表す記号になっている。幾つかの流儀があるように思われるが、ここでは、もっともシンプルなものに統一した。 $M, BM$  は固有の命名を表す記号を使うことが多いようである。 $M$  を特に  $\mathbb{M}$  と表すこともある。

|                                          |                 |
|------------------------------------------|-----------------|
| $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ | Mathieu         |
| $J_1, J_2, J_3, J_4$                     | Janko           |
| $HS$                                     | Higman-Sims     |
| $Suz$                                    | Suzuki (鈴木通夫)   |
| $Mc$                                     | McLaughlin      |
| $He$                                     | Held            |
| $Ru$                                     | Rudvalis        |
| $Ly$                                     | Lyons           |
| $ON$                                     | O'Nan           |
| $Co_1, Co_2, Co_3$                       | Conway          |
| $F_{22}, F_{23}, F'_{24}$                | Fischer         |
| $H$                                      | Harada (原田耕一郎)  |
| $Th$                                     | Thompson        |
| $BM$ (Baby Monster)                      | Fischer         |
| $M$ (Monster)                            | Fischer, Griess |

これらを、より数学的な意味合いから大きく分類すると、次の4つに分類できる。

- (1) Mathieu groups :  $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$
- (2) Leech lattice groups :  $Co_1, Co_2, Co_3, HS, McL, J_2, Suz$
- (3) Monster sections :  $M, BM, F_{22}, F_{23}, F'_{24}, Th, H, He$
- (4) Other groups :  $J_1, J_3, J_4, Ru, Ly, ON$

実際 (1) の Mathieu 群を調べるなら (5つのうちどれでも)、後述の Golay code や 5-design を用いるのが良い。(2) の群は Leech lattice の自己同型群の中で調べるのがスタンダードな方法である。後ろの2つ ( $J_2, Suz$ ) は、係数体・環を変えた "Leech lattice" の自己同型群から得られる。(3) は位数最大の散在型単純群であるモンスター  $M$  の部分群 (または、その剰余群) として得られるものである。このうち多くは、素数位数の元の中心化群から得られる ( $p = 2, 3, 3, 5, 7$  に対して  $BM, F'_{24}, Th, H, He$  が出てくる)。これを用いて、調べるのが易しくなるかという、話は別であるが。最後の (4) は、Monster と無関係な群である。ひとつひとつが独立しているとも言え、わかりやすく説明するのが難しい。Web page [1] では "pariahs" などと書かれているが (元々は Griess の命名か)、そこまで言わなくても良いと思い、別の (あたりさわりのない) 見出しにした。新しい切り口を見つけて、なじみやすいものにしたいという希望もあるからである。27 個目の「散在型」の Tits 群を入れるなら、この (4) の中に入る。

## 1.2 散在型単純群の周辺 (歴史と概観)

ここでは、必要な定義等を取り混ぜながら、散在型単純群とその周辺に関するエポックメイキングな出来事を、年代順に並べておこうと思う。後半に必要な部分を詳しく書いているので、その重要度に比べて短い記述になっている部分も多い。

### 1861–1873: Mathieu 群の発見

Mathieu により、5重可移群として  $M_{12}, M_{24}$  が発見された。その1点の固定部分群  $M_{11}, M_{23}$  は4重可移、その2点の固定部分群  $M_{10}, M_{22}$  は3重可移である。ただし、 $M_{10}$  は  $A_6$  を指数2で含む群であり単純群ではない。また、 $M_{24}$  の3点の固定部分群  $M_{21}$  は  $L_3(4)$  と同型である。

### 1938: Witt systems の研究

Mathieu 群  $M_m (m = 11, 12, 22, 23, 24)$  を自己同型群に持つ Witt system という組合せ構造 (デザイン)  $W_m$  が研究された。

ここで、 $n$  点集合  $\Omega_n$  と、その  $k$  点部分集合のある族  $\mathcal{B}$  (これをブロックの集合と呼ぶ) の組  $(\Omega_n, \mathcal{B})$  が次の条件:

任意の  $t$  点部分集合  $\{x_1, \dots, x_t\} \subset \Omega_n$  に対し、それらを含むブロック ( $\mathcal{B}$  の元) の個数が、点の取り方によらず一定値  $\lambda$  である

をみたすとき、 $t$ -( $n, k, \lambda$ ) デザイン (design) であると言う。特に  $\lambda = 1$  であるとき、 $t$ -( $n, k, 1$ ) design は Steiner system  $S(t, k, n)$  と呼ばれる。Witt system  $W_m$  は、 $m = 22, 23, 24$  のとき  $5$ -( $m, m-16, 1$ ) design であり、 $m = 11, 12$  のとき  $5$ -( $m, m-6, 1$ ) design である。

#### 1949: (extended) Golay code $G_{24}$ の発見

Shanon による情報理論の創生とほぼ同時に、誤り訂正符号という情報伝達に欠かせない方式が提案され、直ちに  $G_{24}$  が発見された。この符号は、実用的という観点からも優秀であり、数学的に重要なものが現実世界でも重要であるという、象徴的な例の一つである。

符号は有限体上の部分ベクトル空間と定義されるのが一般的であるが、ここでは 2 元体上の binary code に話を限る。この場合は、デザイン等の組合せ論との関わりから、次のように記述しておくと話がしやすい。まず、 $\Omega_n$  を  $n$  点集合とし、その部分集合全体の族を  $\mathcal{P}(\Omega_n)$  と表すことにすると、 $\mathcal{P}(\Omega_n)$  は和を対称差で定義 ( $A + B = A \cup B \setminus A \cap B$ ) することにより、2 元体上のベクトル空間と見なせる。ここには、内積も  $(A, B) = |A \cap B| \pmod{2}$  により定義される。符号理論特有の概念として、weight が  $\text{wt}(A) = |A|$  で与えられる。

$\mathcal{P}(\Omega_n)$  の部分空間  $C$  を長さ  $n$  の符号 (code) と呼ぶ。 $C$  の元は codeword と呼ばれる。符号は、その次元と minimum weight ( $\min(C) = \min\{\text{wt}(X) | X(\neq \emptyset) \in C\}$ ) を用いて  $[n, \dim(C), \min(C)]$  code と書かれる。符号  $C$  は  $C \subset C^\perp$  のとき self-orthogonal,  $C = C^\perp$  のとき self-dual と呼ばれる。長さ 24 の Golay code は  $[24, 12, 8]$  code であり、このパラメータで特徴づけられる。さらに、self-dual, doubly even ( $\text{wt}(A) \in 4\mathbb{Z} \ (\forall A \in C)$ ) という性質を持つ。

Golay code  $G_{24}$  には、様々な構成法が知られている。ここで述べるものは [9] (Chapter 11, p.323) による。

最初に、次のような簡単な問題を考えよう。

$21 = n_1 + n_2 + \dots + n_6, \quad 0 \leq n_1 < n_2 < \dots < n_6$  をみたす自然数の組を全て求めよ。

答は簡単で、次の 11 組である。

$$\begin{aligned} H_1 &= \{ 1, 2, 3, 4, 5, 6 \}, & H_7 &= \{ 0, 2, 3, 4, 5, 7 \} \\ H_2 &= \{ 0, 1, 2, 3, 7, 8 \}, & H_8 &= \{ 0, 1, 2, 3, 6, 9 \} \\ H_3 &= \{ 0, 1, 2, 4, 5, 9 \}, & H_9 &= \{ 0, 1, 3, 4, 5, 8 \} \\ H_4 &= \{ 0, 1, 3, 4, 6, 7 \}, & H_{10} &= \{ 0, 1, 2, 5, 6, 7 \} \\ H_5 &= \{ 0, 1, 2, 3, 5, 10 \}, & H_{11} &= \{ 0, 1, 2, 3, 4, 11 \} \\ H_6 &= \{ 0, 1, 2, 4, 6, 8 \} \end{aligned}$$

話のポイントは、解の並べ方に意味があるところで、上記の  $H_i$  達は

$$|H_i \cap H_j| = \begin{cases} 3 & (|i - j| = 1) \\ 4 & (|i - j| > 1) \end{cases}$$

をみたしているのである。この意味で、この並べ方は（全体を逆にすることを除いて）一意である。

さて、 $\Delta = \{0, 1, \dots, 11\}, \Delta' = \{12, 13, \dots, 23\}$  とおいて、24 点集合  $\Omega_{24} = \Delta \cup \Delta'$  を考える。上記の  $H_i$  を用いて、 $\tilde{H}_i = H_i \cup \{11 + i, 12 + i\} (\subset \Omega_{24})$  と定義する。明らかに、

$$|\tilde{H}_i \cap \tilde{H}_j| = 4 (i \neq j)$$

が成り立ち、 $\mathcal{P}(\Omega_n)$  における内積の値が 0 になる（従って self-orthogonal code を生成する）ことがわかる。

**定理 2** (Simple construction of  $G_{24}$ ).  $G_{24} \cong \langle \tilde{H}_1, \dots, \tilde{H}_{11}, \Delta \rangle$ .

さて、この  $G_{24}$  から前述のデザイン (5-(24, 8, 1) design, あるいは、 $S(5, 8, 24)$ ) を構成することが出来る。その最小の weight (= 8) を持つ  $G_{24}$  の codeword をブロックとするのである。

**定理 3.**  $\mathcal{O}_{24} := \{ X \in G_{24} \mid |X| = 8 \}$  とすれば、 $(\Omega_{24}, \mathcal{O}_{24})$  は 5-(24, 8, 1) デザインをなす。

この定理の主張を実感してもらうために、ここでは最も安直な（しかし、ある意味では本質的な）議論を紹介しておく。

安直というのは、その自己同型群が  $M_{24}$  で、 $\Omega_{24}$  に 5 重可移に作用するという著しい性質を仮定してしまうからである。すると、 $M_{24}$  が 5 重可移に作用することから、5 点を含むブロックの個数は 5 点の取り方によらない。特に  $(\Omega_{24}, \mathcal{O}_{24})$  は 5-design である。次に、5 点  $x_1, \dots, x_5$  を含むブロック  $X, Y$  を取ると、簡単な計算で  $|X + Y| \leq 6$  を得る。 $G_{24}$  の性質  $\min(G_{24}) = 8$  より、 $X + Y = \emptyset$  すなわち  $X = Y$  を得る。

### 1955: Chevalley 群の理論

Lie 型の単純群のうち、古典的な線形群の統一理論が出来上がったことになる。Dieudonné [10] の初版が出版されたのもこの頃である。この後の、単純群発見の前の「嵐の前の静けさ」あるいは「夜明け前」という時期のように思える。

### 1960: 鈴木群 $Sz(q)$ の発見

誰もが予想していなかった（と想像される）鈴木群の発見である。無限系列であり、最終的には Lie 型の群の一系列 ( ${}^2B_n(q)$ ) として扱われることになる。

**1965:** 6番目の散在型単純群  $J_1$  (Janko 群) の発見

位数 2 の元 (以下, involution と書く) の中心化群からの特徴付け (分類) による単純群の発見が, Janko による成功から始まった。Mathieu 群から数えれば, 約 100 年ぶりの散在型単純群の発見である。

**1967–1973:** この数年間の間に, 様々な散在型単純群が発見・構成された。 $J_1$  に続く Janko の群  $J_2, J_3$  の発見は次のような定理として述べられる。

**定理 4** (Janko(1968)).  $G$  を単純群で, その位数 2 の元  $t$  の中心化群が  $C_G(t) \cong 2_1^{1+4}.A_5$  をみたすならば,  $G$  は  $|G| = 2^7.3^3.5^2.7$  か  $|G| = 2^7.3^5.5.17.19$  のいずれか ( $G = J_2$  or  $J_3$ ) である。

この定理は群の存在は主張していない。従って, 別の方法で構成する必要がある。ここでは  $J_2$  の構成と, その続きについて少し詳しく述べる。

$J_2$  はランク 3 の置換表現を持つ。すなわち, ある部分群  $G(= J_2) \supset H(\cong U_3(3))$  が存在して, その coset  $G/H = \{xH \mid x \in G\}$  への置換表現  $g \cdot xH = (gx)H (g \in G)$  において, 1 点の固定部分群となる  $H$  の作用が, ちょうど 3 つの orbits ( $\{H\}, \Delta_1, \Delta_2$ ) を持つ。このことは, 群の存在を仮定して指標表から読み取ることが出来る。このとき, いわゆる rank 3 graph  $\Gamma(G, H)$  が, その頂点集合を  $G/H$  とし, その辺集合を  $\{aH, bH \mid a^{-1}bH \in \Delta_1\}$  と定義できる。このグラフを  $J_2$  の存在を仮定せずに  $U_3(3)$  の情報から構成できれば, その自己同型群 (の部分群) として  $J_2$  を構成出来るだろうということになる。

**定理 5** (Hall-Wales(1968), Suzuki(1969)).  $\text{Aut}(\Gamma(J_2, U_3(3))) \cong J_2:2$

このアイディアは M.Hall によるものと思われ, その後の散在型単純群の構成の先駆けとなるものであった。そのため, Janko の群のうち,  $J_2$  だけは Hall-Janko の群と呼ばれ  $HJ$  と書かれることもある。グラフ  $\Gamma(J_2, U_3(3))$  は当初は計算機を用いて構成され, その直後に, 鈴木先生により, 計算機なしに, かつ, 散在型鈴木群を含む系列  $(U_3(3), J_2, G_2(4), \text{Suz})$  を伴って構成が与えられた [17]。

$$\begin{aligned} \text{Suz}:2 &\cong \text{Aut}(\Gamma(\text{Suz}, G_2(4))), \\ G_2(4):2 &\cong \text{Aut}(\Gamma(G_2(4), J_2)), \\ J_2:2 &\cong \text{Aut}(\Gamma(J_2, U_3(3))), \\ U_3(3):2 &\cong \text{Aut}(\Gamma(U_3(3), L_2(7))). \end{aligned}$$

これらのグラフは, それぞれの  $\Gamma(G, H)$  の 1 点の近傍 (1 点と辺で結ばれる点全体のなす部分グラフ) が, 部分群  $H$  に対するグラフになっており, 帰納的に定義されるようになっている。総称して Suzuki tower (chain) と呼ばれることもあり, その構成は Gorenstein の著書の中で "lovely construction" と評されている。とは言っても, これは部分群  $H$  の involution の関係を用いた群論的なもので, 理解しやすいものとは言えない。

グラフとデザインが関係する例として、Higman-Sims 群  $HS$  の例を紹介しておこう。この群は、 $J_2$  の構成に関する M. Hall の講義の翌朝（と言われている）までに構成に成功したと伝えられている。

まず、Mathieu 群  $M_{22}$  が作用する Witt system  $W_{22}$  ( $S(3, 6, 22)$ ,  $3$ -( $22, 6, 1$ ) design) を  $D = (\mathcal{P}, \mathcal{B})$  とおく。グラフ  $\Gamma$ （これが、結果的に rank 3 graph  $\Gamma(HS, M_{22})$  になる）を、頂点集合を  $\{\infty\} \cup \mathcal{P} \cup \mathcal{B}$  として、グラフの辺を

- (1)  $\mathcal{P}$  の 2 頂点, および,  $\infty$  と  $\mathcal{B}$  の頂点は, 辺で結ばない。
- (2)  $p \in \mathcal{P}$  と  $B \in \mathcal{B}$  は, デザインにおいて  $p \in B$  であるとき辺で結ぶ。
- (3)  $B_1, B_2 \in \mathcal{B}$  は,  $|B_1 \cap B_2| = 0$  のとき辺で結ぶ。

と定義する。数ある rank 3 graph の中でも、最も理解しやすいグラフの構成だと思われる。

**定理 6** (Higman-Sims(1968)).  $\text{Aut}(\Gamma) \cong HS$ .

なお、MacLaughlin の群  $McL$  や Fischer 群  $F_{22}, F_{23}, F'_{24}$  も rank 3 graph から構成される。特に Fischer 群は、3-transposition group と呼ばれるもので、2 元の積の位数が 1, 2, 3 であるような involution の共役類で生成される。その共役類を頂点集合として、位数 2（つまり、可換）のとき辺で結ぶことにより、対応する rank 3 graph が定義できる。これは、Baby Monster を含む  $\{3, 4\}$ -transposition group（積の位数が 1, 2, 3, 4）の研究を経由して、Monster の発見への道のりの出発点とも言えるものである。

さて、この時期の最も重要なトピックは、Leech lattice (1967), Conway 群 (1968) の発見であろう。Leech lattice は Golay code から構成される。その構成を簡単に書いておこう。詳しくは [9] をご覧いただきたい。

$$A(G_{24}) = \left\{ \frac{1}{\sqrt{2}}(x_1, \dots, x_{24}) \mid x_i \in \mathbb{Z}, (x_i \bmod 2) \in G_{24} \right\}$$

$$B(G_{24}) = \{x \in A(G_{24}) \mid \langle x, v \rangle \in \mathbb{Z}\}, \quad v = \frac{1}{2\sqrt{2}}(-3, 1, 1, \dots, 1)$$

$$\Lambda_{24} := B(G_{24}) \oplus \mathbb{Z}v$$

$A(G_{24})$  は Golay code の mod 2 による逆像で、Construction A と呼ばれる構成法の一つである。 $B(G_{24})$  は Construction B と呼ばれる index 2 の sublattice で、最後の  $\Lambda_{24}$  が Leech lattice である。ランク 24 の even unimodular lattice で、最小のノルムが 4 であるようなものとして特徴づけられる。

Conway は  $\Lambda_{24}$  の自己同型群を決定し、その中心による剰余群が散在型単純群であること

$$Co_1 = \text{Aut}(\Lambda_{24})/\{\pm 1\}$$



を示した。その詳しいいきさつが [19] や [22] に記録されている。特筆すべきは、 $\text{Aut}(\Lambda_{24})$  が非常に多くの（散在型）単純群を含んでいたことである。まず、 $\Lambda_{24}$  のノルム 4, 6 のベクトルの固定部分群として、 $Co_2, Co_3$  が得られる。さらに、

$$\cdot pqr = \{\sigma \in \text{Aut}(\Lambda_{24}) \mid \sigma(x) = x, \sigma(y) = y\}$$

（ただし、 $x, y \in \Lambda_{24}$  は  $\langle x, x \rangle = 2p$ ,  $\langle y, y \rangle = 2q$ ,  $\langle x - y, x - y \rangle = 2r$  をみたすとする）と定めると、次が成り立つのである。

**定理 7** (Conway(1968)).  $\cdot 233 \cong HS$ ,  $\cdot 223 \cong McL$ ,  $\cdot 222 \cong U_6(2)$

さらに、Suzuki tower の群達は、係数体（環）を替えた "Leech lattice" の自己同型群として現れる。 $6.Suz$  が、 $\mathbb{Z}[\sqrt[3]{1}]$  上の "complex Leech lattice",  $2.G_2(4)$  が Hurwitz order  $\mathbb{Z}[i, j, k, \frac{1}{2}(1+i+j+k)]$  上の "quaternionic Leech lattice", そして、 $2.J_2$  が、 $\mathbb{Q}(\sqrt{5})[i, j, k]$  の部分環上（もはや、名前はない）という具合である。

このように、沢山の散在型単純群が Leech lattice を通して、再発見されたのである。

1970 年代になると、発見されるのは難しい群が増えてくる。 $Ly, Ru, ON$  などの Monster に含まれない群である。 $Ru$  は rank 3 graph  $\Gamma(Ru, T)$  の自己同型群として得られるのであるが、この場合の  $H = T$  (Tits 群) もまた難しい群で（少なくとも筆者には）理解しやすい群とは言えない。

**1974:** Monster の発見 (Fischer)

最大（位数という意味でも、その数学的な深さ・広がりという意味でも）の散在型単純群 Monster が発見された。その (2A-)involution の中心化群が、 $\{3, 4\}$ -transposition group の Baby Monster  $BM$  を用いて、 $2 \cdot BM$  と表される群として存在が预言されたのである。

**1975:** 26 番目の散在型単純群  $J_4$  (Janko 群) の発見

これで 26 個の全てが出そろったことになる。一連の散在型単純群発見の最初と最後を Jnako が飾ったのである。[22] によると、Janko がもうひとつ見つけるのではないかと思われていたこともあったようである。

**1981:** 有限単純群の分類定理の完了宣言

**1982–1988:** Monster の構成

散在型単純群発見の歴史は、この Monster の構成で（ひとまず）締めくくられるものであろう。これは、まず Griess [12] により非結合的可換代数の自己同型群として構成され、数年後に、頂点作用素代数 (VOA=Vertex Operator Algebra) を用いた構成 (Frenkel-Lepowsky-Meurman [11]) が得られた。理論物理を背景に持つ VOA なる概念が現れたことは、驚くべきことであったと思う。

この可換代数や頂点作用素代数は、Leech lattice から作られる。これは、Monster の  $2B$ -involution の中心化群が  $2^{1+24}.Co_1$  という形をしていることに起因している。ここでは、これ以上触れないが、ここに至って完成した

Binary code  $\rightarrow$  Lattices  $\rightarrow$  Vertex operator algebra

という流れは、 $M_{24}, Co_1, M$  といった単純群を扱うために本質的と思われ、そこから派生する問題も数多い。筆者も 2002 年の代数学シンポジウムで、この辺りの話題をお話したが内容のそう深くない話になってしまった。今回のシンポジウムでは、島倉裕樹氏により新発見と共に語られたことになる。そちらの報告もご覧いただきたい。

## 2 有限置換群と自己直交符号

この Section の内容は、千吉良直紀氏（熊本大学）と原田昌晃氏（山形大学）との共同研究によるものである。

話の出発点は、Golay code  $G_{24}$  である。その weight 8 の codeword は Section 1 で述べたように、デザインのブロックになる非常に重要な対象である。群論的には、その自己同型群 Mathieu 群  $M_{24}$  の  $2A$  と呼ばれる involution の固定点が weight 8 の codeword になっていることがよく知られている。

一方、我々は最近になって [6] において、Janko 群を少し大きくした  $J_2:2$  を自己同型群に持つ新しい self-dual  $[100, 50, 10]$  code  $C_{10}$  を発見・構成した。その重要な性質の一つが、 $C_{10}$  が weight 14 の codeword 全体で生成されることであり、この weight 14 の codeword が outer involution の固定点の集合として得られるということであった。この固定点の集合についても、群の発見当初から知られていて ([18])、群論的に注目されていた対象ではあった。

さて、このような符合は偶然なのだろうか、というのが話の出発点であった。

### 2.1 例と主定理

一般に、有限置換群を考えたときに、その involution の固定点の生成する符号というものについて、何か言うことが出来るだろうか。これが、我々の問題意識であった。その結果得たのは、「生成する符号」ではなく、その直交補空間を考えるべし、ということだった。self-dual code ならば、両者が一致するため、すぐには気づかなかったのである。

$(G, \Omega)$  を次数  $n(= |\Omega|)$  の置換群とする。2 元体上の  $n$  次元ベクトル空間  $\mathcal{P}(\Omega_n)$  において、 $G$  の位数 2 の元  $\sigma$  の固定点  $Fix(\sigma)$  の生成する code の直交補空間を  $C(G, \Omega)$  と表す。

$$C(G, \Omega) := \langle Fix(\sigma) \mid \sigma \in I(G) \rangle^\perp$$

その次数で置換表現が一意に決まる場合は、これを  $C(G, n)$  と表すことにする。

**定理 8** ([7]).  $C$  を  $G$  の  $\Omega$  への作用で不変な、長さ  $n$  の self-orthogonal code とするとき、

$$C \subset C(G, \Omega)$$

が成り立つ。

*Proof.*  $X \in C$  と  $\sigma \in I(G)$  を任意にとると、 $\sigma^2 = 1$  であることから、 $\langle \sigma \rangle$  は  $X \cap X^\sigma$  に作用する。また  $C$  が self-orthogonal であるという仮定から  $|X \cap X^\sigma|$  は偶数である。さて  $X \cap X^\sigma \supseteq \text{Fix}(\sigma) \cap X$  であることに注意して、 $Y = (X \cap X^\sigma) \setminus (\text{Fix}(\sigma) \cap X)$  とおく。 $Y$  は  $\{a, a^\sigma\}$  ( $a \in Y$ ) という形の部分集合の disjoint union になり、 $|Y|$  が偶数であることがわかり、従って  $|\text{Fix}(\sigma) \cap X|$  も偶数である。すなわち、任意の  $\text{Fix}(\sigma)$  と  $X$  が直交するので定理を得る。  $\square$

証明は非常に易しい。しかしながら、次の例 1 に述べた  $C(J_2:2, 100)$  が過去の文献に見あたらない（グラフから作る例 2 の code が文献にあるにもかかわらず）ところを見ると、これまでに着目された対象ではないのだろうと思う。この定理の弱点は  $C(G, \Omega)$  の計算が（一般に）容易でないことで、我々も、大抵の場合 computer (Magma というソフトウェア) を用いて計算している。

**例 1.** 話の出発点となった code は、

$$G_{24} = C(M_{24}, 24), C_{10} = C(J_2:2, 100)$$

となっている。また、 $M_{24}$  の 2 点の固定部分群  $M_{22}$  は、 $G_{24}$  から作られる  $[22, 11, 6]$  code  $G_{22}$  に作用するが、これも  $G_{22} = C(M_{22}, 22) = C(M_{22}:2, 22)$  として得られる。

例 1 のような、 $C(G, \Omega)$  自身が self-dual になっている場合というのは、数少ないように思われる。実際、我々が知っているのは、単純群に限らなくても、原始的な置換群の場合は、上記の  $C_{10}, G_{24}, G_{22}$  以外には、

$$C(M_{22}:2, 330), C(2^{2m+1}:L_{2m+1}(2), 2^{2m+1})$$

に限る。前者は、self-dual  $[330, 165, 10]$  code で  $\text{Aut} \cong M_{22}:2$  をみたす ([7])。後者は、有名な Reed-Muller code と呼ばれるもので、 $R(m, 2m+1)$  とも書かれる。

**例 2.**  $G = J_2$  とすると、 $C(J_2, 100)$  は少し大きく  $[100, 63, 8]$  code になる。実は、直交補空間を取らない、固定点が生成する符号  $\langle \text{Fix}(\sigma) \mid \sigma \in I(G) \rangle$  はすでに計算されていて ([16]),  $J_2$  が作用する rank 3 graph の近傍 (36 点集合) によって生成される  $[100, 36, 16]$  code に全体集合  $\Omega$  を付け加えた self-orthogonal  $[100, 37, 16]$  code である。しかし、 $C(J_2, 100)$  は 63 次元と大きいから、もっと大きな self-dual が存在しうるわけで、実際、 $C_{10}$  が存在するのである。他にも、 $J_2$  を自己同型群に持つ  $[100, 50, 16]$  code  $C_{16}$  を構成することが出来て、さらに、さらに、 $C(J_2, 100)$  に含まれる  $J_2$  不変な self-dual code が、 $C_{10}, C_{16}$ , および、 $C_{16}$  と同値な  $C'_{16}$  に限ることも証明することが出来る。

$C(G, \Omega)$  は一般に self-orthogonal ではない。しかし,  $C(G, \Omega)$  自体が self-orthogonal である場合もいくつかあって, 過去に知られていた多くの (散在型単純群に関連する) 例を含んでいる。これを以下に例示しておこう。

**例 3** (Calderbank–Wales (1982)). Higman’s design として知られている 2-(176, 50, 14) design がある [14]。そのブロックで生成される self-orthogonal [176, 22, 50] code が Calderbank–Wales [5] で構成されたが, これは  $C(HS, 176)$  と一致する。その自己同型群は, デザイン, code 共に, Higman-Sims の群  $HS$  である。

この Higman’s design は,  $HS$  の部分群  $M_{22}$  の言葉だけで定義されていて, そこから  $HS$  が自己同型群として得られるところに面白さがある。今回の code については,  $C(HS, 176) = C(M_{22}, 176)$  が成立していて,  $M_{22}$  から定義される符号に  $HS$  が作用していることの説明を与えている。

**例 4** (Haemers–Parker–Pless–Tonchev (1993)). Conway 群  $Co_3$  は 276 次の 2 重可移表現を持つ。その 1 点の固定部分群は McLaughlin の群の拡大  $McL:2$  で 275 点上にランク 3 に作用している。[13] では, ここから,  $Co_3, McL:2$  を自己同型群とする self-orthogonal [276, 23, 100], [275, 22, 100] code が構成されている。これらは, それぞれ,  $C(Co_3, 276)$ ,  $C(McL:2, 275)$  として得られる。

## 2.2 Self-dual codes

ここでは  $C(G, \Omega)$  (自体ではなく) が self-dual code を含む場合についてのべる。次の補題は, 容易に示される。

**補題 9.**  $C (\subset \mathcal{P}(\Omega))$  が  $G$ -不変な長さ  $n$  の self-dual code ならば,  $C(G, \Omega)^\perp$  は self-orthogonal で

$$C(G, \Omega) \supset C \supset C(G, \Omega)^\perp$$

が成立する。

この補題の条件を満たす原始置換群は, どれくらいあるだろうか。次の定理は, これもまた, 実は, 限られた場合にすぎないこと, すなわち, ”有限単純群を自己同型群に持つ self-dual code” というものが, いかにか希なものか, を示す定理である。

ここでは散在型単純群 (あるいは, それを少し大きくしたもの) に限って述べたが, 実際には, 一般の単純群についてもある程度の範囲で (さらに言えば, 単純群でなくても小さい次数なら) 調べてあり, そうしてもめばしい例が増えることはない。しかし, 一般の場合にすると, 「調べた範囲」を明示することが煩雑になるので, 本稿のタイトルに免じて, そこは省略させていただく。また, 以下の 2 つの命題で  $C(G, \Omega)^\perp$  に  $(\neq \{0\})$  という注釈を付けたが, これは, 位数 2 の元が固定点を持たず  $C(G, \Omega)$  が全空間になる場合を除いたものである。

**定理 10.**  $(G, \Omega)$  を 次数 10080 以下の原始置換群とし,  $G$  は, ある散在型単純群  $S$  に対し,  $S \subset G \subset \text{Aut}(S)$  をみたすものとする。このとき,  $C(G, \Omega)^\perp (\neq \{0\})$  が self-orthogonal となるのは, 以下のいずれかに限る。

$$\begin{aligned} C(M_{22}, 22) &= C(M_{22}:2, 22)(\cong G_{22}), C(M_{24}, 24)(\cong G_{24}), \\ &C(J_2:2, 100)(\cong C_{100}), C(M_{22}:2, 330), \\ C(J_2, 100), C(M_{12}, 144), C(M_{12}, 220), C(M_{22}, 330), C(M_{22}, 672), \\ &C(M_{12}:2, 1584), C(M_{24}, 2024), C(Ru, 4060), C(J_2(2), 10080) \end{aligned}$$

この中のいくつかについては,  $G$ -不変 self-dual code の分類が可能である。例えば,  $C(J_2, 100)$  は, 例 2 で述べたとおり (3 つ) で,  $C(M_{12}, 220)$  は 3 つ,  $C(M_{22}, 330)$  は 1 つ ( $C(M_{22}:2, 330)$ ) となる。また,  $C(M_{12}, 144)$ ,  $C(M_{22}, 672)$  については非存在が示される。

次数が大きくなると, computer を用いても計算が困難になる。 $C(M_{12}:2, 1584)$ ,  $C(M_{24}, 2024)$ ,  $C(J_2(2), 10080)$  は, 未計算である。最後に述べる  $C(Ru, 4060)$  も簡単には計算できなかったのであるが, 最近 (シンポジウムの直前) になって, 千吉良氏から

**定理 11.**  $C(Ru, 4060)(= C(Ru, Ru/{}^2F_4(2)))$  は, ちょうど 3 つの  $Ru$ -不変 self-dual codes を含んでいる。

という連絡が入った。Section 1 でも触れた, 難しい rank 3 の置換表現から来るものである。この符号の存在から, 新しい研究が始められないか, 現在模索しているところである。

### 3 Strongly Regular Graphs and Designs

この Section の内容は基本的に, 中空大幸氏 (岡山大研究協力員) および, 堀口直之氏 (千葉大研究生) との共同研究であり, 一部, 葛田一慶氏 (千葉大大学院), A. E. Brouwer 氏 (Eindhoven) との結果を含む。

実は, この話も  $J_2$  の作用する self-dual  $[100, 50, 10]$  code  $C_{10}$  から始まる。この記号で使った添え字 10 は, minimum weight を意味している。Section 2 では, weight 14 の codeword について述べたが, 今回の weight 10 の codeword は, また別の意味を持っている。

それは,  $J_2$  が作用する rank 3 graph での話である。これは 100 次の置換表現であり,  $C_{10}$  を含む空間の 100 個の座標は, rank 3 graph の 100 点に対応している。このとき, weight 10 の codeword は, 極大な clique (どの 2 点も辺でないような部分グラフ) に相当していて, 10 という大きさは, 理論的な最大値になっているのである。そこから, あるデザイン (3-design) が定義される。このことに, 中空氏が気づいたのが, 出発点であった。

### 3.1 Hoffman bound

頂点集合  $V$  と辺集合  $E$  を持つグラフ  $\Gamma = (V, E)$  がパラメータ  $(v, a, c, d)$  を持つ strongly regular graph であるとは、 $x \in V$  の近傍を  $V(x) = \{y \in V \mid \{x, y\} \in E\}$  と表すとき、

- (1)  $|V| = v$ ,
- (2) 任意の  $x \in V$  に対し  $|V(x)| = a$ (定数), かつ,
- (3) 2点  $x, y \in V$  に対し,  $|V(x) \cap V(y)|$  が  $\{x, y\}$  が辺か否かによってのみ定まり  $|V(x) \cap V(y)| = c(\{x, y\} \in E), d(\{x, y\} \notin E)$

となっていることを意味する。Section 1 で述べた rank 3 graph は, strongly regular graph になる。

グラフの coclique とは, どの2点も辺でないような部分グラフのことを言う。次の定理は, strongly regular graph の coclique の大きさについて, グラフのパラメータによるバウンドが存在するというものである。これを Hoffman bound と呼ぶ ([3] の 10 ページ)。

**定理 12** (Hoffman).  $\Gamma = (V, E)$  をパラメータ  $(v, a, c, d)$  を持つ strongly regular graph で, その最小の固有値 (グラフの隣接行列の固有値のことであり, パラメータから得られる) を  $\alpha$  とする。このとき,  $C$  を  $\Gamma$  の coclique とすると, 次の不等式

$$|C| \leq (1 - a/\alpha)^{-1}v$$

が成り立つ。等号が成立するならば, 結合構造  $\mathcal{D} = \mathcal{D}(C) = (C, V \setminus C)$  は  $2-(n, -\alpha, d)$  デザインをなす。ただし,  $p \in C$  と  $B \in V \setminus C$  の incidence は,  $p$  と  $B$  がグラフ  $\Gamma$  で辺で結ばれていることと定義する。

さて,  $J_2$  の rank 3 graph は, strongly regular graph としては  $(100, 36, 14, 12)$  というパラメータを持つ。Hoffman bound を適用すれば  $C \leq 10$  となる。従って, 先に述べた, 大きさ 10 の clique が存在することから,  $\mathcal{D} = \mathcal{D}(C) = (C, V \setminus C)$  として  $2-(10, 6, 30)$  design が得られる。ところが, 中空氏によれば, これは  $3-(10, 4, 1)$  design で, Witt system  $W_{10}$  のブロックを 3 回重複させた (同じブロックが 3 つある) ものになっていたのだった。我々は, ここから  $J_2$  のグラフの再構成を行った [15]。これは, 後述の Suzuki graph の再構成のモデルとなる結果であるが, ここでは詳細は省略する。

$J_2$  は Suzuki tower の一つである。我々は, 他の群についても同様のことが起こっていないかと期待したのであるが, 直ちに得られたのは, 少しがっかりする結果だった。 $Suz, G_2(4), J_2, U_3(3)$  という系列のうち,  $G_2(4)$  は Hoffman bound をみたましているが, デザインは単に 2-design で (3-design にはならず) 面白みに欠ける。 $U_3(3)$  に至っては, Hoffman bound をみたましてさえいないのである。しかしながら, 幸いなことに, Suzuki graph は良い方の例になってくれたのである。

### 3.2 Suzuki graph

Suzuki graph は, strongly regular graph として  $(1782, 416, 100, 96)$  というパラメータを持つ。Hoffman bound を Suzuki graph に適用すると  $C \leq 66$  が得られる。我々は, 計算機 (Magma) を用いて Suzuki graph の大きさ 66 の coclique が存在することを確認し, さらに  $\mathcal{D}$  が (Theorem 12 により得られる  $2-(66, 16, 96)$  という結論以上の) 3-デザインになっていることを確認したのである。(なお, coclique の一意性は, 葛田一慶 (千葉大大学院) の修論で Magma を用いて示されている。)

**定理 13** ([4]). Suzuki graph  $\Gamma$  は大きさが 66 の coclique  $C$  を持ち,  $\mathcal{D} = (C, V \setminus C)$  は simple  $3-(66, 16, 21)$  デザインになる。その自己同型群  $\text{Aut } \mathcal{D}$  は  $U_3(4) : 4$  に同型である。

自己同型群  $\text{Aut } \mathcal{D}$  の点集合への作用を調べてみると, その作用は 1 点を固定していて, 残りの 65 点上に 2 重可移 に作用していた。これは,  $U_3(4)$  の 16 元体上の 3 次元ユニタリ空間における, isotropic point 全体への作用として得られるものである。その固定される点を  $p (\in C)$  とすると,  $p$  を含むブロック (から  $p$  を除いて) 全体の作る derived design  $\mathcal{D}_p$  は  $2-(65, 15, 21)$  デザインであり,  $p$  を含まないブロック全体の作る residual design  $\mathcal{D}^p$  は  $2-(65, 16, 75)$  デザインである。 $\mathcal{D}_p, \mathcal{D}^p$  が 2-デザインになるのは,  $p$  以外の 65 点への作用が 2 重可移であることから必然であり意外性はない。デザイン  $\mathcal{D}$  は  $\mathcal{D}_p$  の (群の可移拡大ではない) デザインの拡大の一つの例になっている。

付記しておく,  $J_2$  の場合では clique の固定部分群が  $M_{10}$  を含んでいて 10 点上に 3 重可移に作用している。それゆえの 3-design なのであった。

### 3.3 3-デザインとグラフの構成

次の目的は, デザイン  $\mathcal{D}$  を 16 元体上の 3 次元ユニタリ空間から構成することである。このユニタリ空間の内積を  $\langle (x_1, x_2, x_3), (y_1, y_2, y_3) \rangle = x_1y_1^4 + x_2y_2^4 + x_3y_3^4$  とし,

$$\mathcal{P} = \{[x] | x \in \mathbb{F}_{16}^3, \langle x, x \rangle = 0\}, \mathcal{Q} = \{x \in \mathbb{F}_{16}^3 | \langle x, x \rangle \neq 0\}$$

とおく。ただし,  $[x] = \{\gamma x | \gamma \in \mathbb{F}_{16} \setminus \{0\}\}$  である。さらに,  $\mathcal{O}$  を  $\mathcal{Q}$  の元からなる直交基底全体とする。このとき,  $x \in \mathcal{Q}$  に対し  $O_x = \{[y] \in \mathcal{P} | \langle x, y \rangle = 0\}$  とすると, 結合構造  $(\mathcal{P}, \{O_x | x \in \mathcal{Q}\})$  は, よく知られた  $2-(65, 5, 1)$  デザインであり, ユニタリ群全般に対し同様の定義が可能である。ここから, 我々が求める  $\mathcal{D}_p$  が得られる。直交基底  $\{b_1, b_2, b_3\} \in \mathcal{O}$  に対し,

$$B(b_1, b_2, b_3) = O_{b_1} \cup O_{b_2} \cup O_{b_3}$$

とおき, これら全体をブロックとするのである。

**補題 14.**  $\mathcal{B}_1 = \{B(b_1, b_2, b_3) | \{b_1, b_2, b_3\} \in \mathcal{O}\}$  とすると, 結合構造  $(\mathcal{P}, \mathcal{B}_1)$  は,  $\mathcal{D}_p$  と同型な  $2-(65, 15, 21)$  デザインをなす。

次の  $\mathcal{D}^p$  の構成は、やや難しい問題だった。ひとつの理由は、 $U_3(4)$  の  $\mathcal{D}^p$  のブロックへの作用が primitive でなく、あまり良い置換表現になっていないため、捕らえづらいのである。我々は、試行錯誤を繰り返していたのだが、最終的に、Brouwer 氏の助けを得て、以下のような記述を得ることが出来たのである。

まず、 $\mathbb{F}_{16}$  を  $\mathbb{F}_4^2$  と見て、 $\mathbb{F}_4$  上のアフィン平面と見る。すると、そこには 20 本の直線があるので、それを  $\mathcal{L}$  と表す。 $\ell(\in \mathcal{L})$  は 4 つの点 ( $\mathbb{F}_{16}$  の元) を含んでいる。さて、 $[x] \in \mathcal{P}$  に対し、 $\langle x, y \rangle = 0$  をみたす  $[y] \in \mathcal{Q}$  は一意に存在する。このとき、

$$L_\lambda(x) := \{[z] \in \mathcal{P} \mid \langle z, \lambda x + y \rangle = 0\}$$

と定義しよう。そして、ブロックの集合を、

$$\mathcal{B}_2 = \{ (\bigcup_{\lambda \in \ell} L_\lambda(x)) \setminus \{x\} \mid [x] \in \mathcal{P}, \ell \in \mathcal{L} \}$$

と定めるのである。

**補題 15.**  $(\mathcal{P}, \mathcal{B}_2)$  は、2-(65, 16, 96) design である。

これらを用いて Suzuki graph から得られるデザイン  $\mathcal{D}$  が構成される。

**定理 16.**  $X = \mathcal{P} \cup \{\infty\}$ ,  $\mathcal{B} = \{B \cup \{\infty\} \mid B \in \mathcal{B}_1\} \cup \mathcal{B}_2$  とすると、結合構造  $(X, \mathcal{B})$  は、 $\mathcal{D}$  と同型な 3-(66, 16, 21) デザインをなす。

そして、さらに、このデザインから Suzuki graph を再構成することが出来る。

**定理 17** ([4]). 3-(66, 16, 21) デザイン  $(X, \mathcal{B})$  に対し、頂点集合として  $X \cup \mathcal{B}$  を持つグラフ  $\Gamma'$  を次のように定義する。

- (1)  $X$  の任意の 2 頂点は、辺で結ばない。
- (2)  $p \in X$  と  $B \in \mathcal{B}$  は、デザインにおいて  $p \in B$  であるとき辺で結ぶ。
- (3)  $B_1, B_2 \in \mathcal{B}$  は、 $|B_1 \cap B_2| = 4$  であるとき辺で結ぶ。

このとき  $\Gamma'$  は  $\Gamma$  と同型。

定理の (1), (2) はデザインの構成法から必然である。ブロック間の辺の定義である (3) が簡潔に記述できたことは、我々にとって幸運なことであった。Section 1 で述べた Higman-Sims の群に対する rank 3 graph に匹敵するような、簡単な記述になっているのが、この定理の自慢である。また、 $U_3(4)$  という群が、特別な群であるという認識は（少なくとも私には）過去にはなかったものである。実際、 $U_3(4)$  の記述は、ATLAS ([8]) でも簡素である。この  $U_3(4)$  という群が、散在型単純群と深く関わっていると（初めて？）指摘し得たことが、もう一つの自慢なのである。



## 参考文献

- [1] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh and R. Wilson, “ATLAS of Finite Group Representations - Version 3”, published electronically at  
<http://brauer.maths.qmul.ac.uk/Atlas/v3/>.
- [2] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Department of Mathematics, University of Sydney, Available online at  
<http://magma.maths.usyd.edu.au/magma/>.
- [3] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-regular graphs*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 18, Springer-Verlag, Berlin (1989).
- [4] A. E. Brouwer, N. Horiguchi, M. Kitazume and H. Nakasora, A construction of the sporadic Suzuki graph from  $U_3(4)$ , *J. Combin. Theory Ser. A*, to appear.
- [5] A. R. Calderbank and D. B. Wales, A global code invariant under the Higman–Sims group, *J. Algebra*, **75** (1982), 233–260.
- [6] N. Chigira, M. Harada and M. Kitazume, Some Self-Dual Codes Invariant under the Hall–Janko Group, *J. Algebra*, **316** (2007), 578–590.
- [7] N. Chigira, M. Harada and M. Kitazume, Finite permutation groups and self-orthogonal codes, *J. Algebra*, **309** (2007), 610–621.
- [8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups*, Clarendon Press, Oxford, 1985.
- [9] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, 3rd ed., Springer-Verlag, New York, 1999.
- [10] J. Dieudonné, *La géométrie des groupes classiques*, 2nd ed., Springer-Verlag, Berlin, 1963.
- [11] I. B. FRENKEL, J. LEPOWSKY AND A. MEURMAN, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. **134**, Academic Press, 1988.
- [12] R.L.GRIESS, The Friendly Giant, *Invent. Math.* **69** (1982), 1–102.
- [13] W. H. Haemers, C. Parker, V. Pless and V. Tonchev, A design and a code invariant under the simple group  $Co_3$ , *J. Combin. Theory Ser. A*, **62** (1993), 225–233.

- [14] G. Higman, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* **13** (1969), 74–80.
- [15] N. Horiguchi, M. Kitazume and H. Nakasora, The Hall-Janko graph and the Witt system  $W_{10}$ , *European J. Combin.*, **29** (2008), 1–8.
- [16] J. D. Key and J. Moori, Codes, designs and graphs from the Janko groups  $J_1$  and  $J_2$ , *J. Combin. Math. Combin. Comput.* **40** (2002), 143–159.
- [17] M. Suzuki, A simple group of order, 448,345,497,600, *Theory of Finite Groups* (R. Brauer and C. Sah eds.), 113–119, Benjamin, New York-Amsterdam, 1969.
- [18] J. Tits, Le groupe de Janko d’ordre 604,800, *Theory of Finite Groups* (R. Brauer and C. Sah eds.), 91–95, Benjamin, New York-Amsterdam, 1969.
- [19] T. M. Thompson, *From error correcting codes through sphere packings to simple groups*, The Carus Mathematical Monographs 21, The Mathematical Association of America, 1983.
- [20] 鈴木通夫, 「群論(上)」, 岩波書店, 1977.
- [21] 鈴木通夫, 「有限単純群」, 紀伊國屋書店, 1987.
- [22] マーク・ロナン (宮本雅彦・宮本恭子訳), 「シンメトリーとモンスター」, 岩波書店, 2008.