

Mathieu-Witt systems の初等的・統一的記述

一橋大 商 岩崎 史郎
(Shiro Iwasaki)

今日まで多くの人によって, Mathieu-Witt systems に関する種々の興味深い研究が行われてきたが, まだ研究が十分とは言いがたい面も少なからずあり——たとえば, 小さな system W_{12} と大きな system W_{24} とはあまり統一的に扱われていないようであり, blocks の正体もどこか不明で, その記述のしかたも必ずしも簡単とはいえないであろう——これらの systems には依然として神秘的で, 研究対象としての魅力が漂っていると思われる。

本稿の目的: 従来の研究の一部を整理しながら, Mathieu-Witt systems をできるだけ自然で, 統一的かつ初等的に記述する一つの試みをする。特に, 全ての blocks を記述する簡単な一つの方法を述べる。

記号

q = 素数 $p > 7$, $q \equiv -1 \pmod{4}$.

F_q : q 個の元からなる有限体.

$\Omega = \Omega(q) = \{\infty\} \cup F_q$: F_q 上の射影直線.

$Q = \{x^2 \mid x \in F_q \setminus \{0\}\}$.

$i \in F_q$ に対し

$Q_i = Q + i$,

$U_i = \{i\} \cup Q_i = U_0 + i$.

$G = \text{PSL}(2, q) = \{x \mapsto \frac{ax+b}{cx+d} \mid a, b, c, d \in F_q, ad-bc \in Q\}$.

他に, 次のような標準的な記号も使う.

$A, B \subset \Omega$ に対し

$A \Delta B = (A \setminus B) \cup (B \setminus A)$: A, B の対称差.

$\bar{A} = \Omega \setminus A = \Omega \Delta A$.

G は Ω 上の置換群であるが, $A \subset \Omega$; $a, b, \dots \in \Omega$ に対し

$A^G = \{A^\sigma \mid \sigma \in G\}$,

$G_{(A)} = \{\sigma \in G \mid A^\sigma = A\}$,

$G_{a,b,\dots} = \{\sigma \in G \mid a^\sigma = a, b^\sigma = b, \dots\}$.

$q \equiv -1 \pmod{4}$ より, G は Ω 上 3-斉次の置換群となる (Ω の 3 個の元からなる任意の 2 つの部分集合 $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2, b_3\}$ に対し, $A^\sigma = B$ なる $\sigma \in G$ が存在する) が,

これから自然に、次のように 3-design が構成される:

任意の $A \subset \Omega$, $|A| = k \geq 3$ に対し, Ω を点集合, A^G を blocks 集合として

$$\underline{D(g, A)} = (\Omega, A^G)$$

は $3-(g+1, k, \lambda)$ design である. ここに

$$\lambda = |G : G(A)| \binom{k}{3} / \binom{g+1}{3}.$$

(一般に, t -斉次の置換群から t -design が構成できる. た
とえば, Lane [4] を参照)

問題: どんな g と A に対して, $D(g, A)$ は興味ある design
となるか? を考えよう.

$A = U_0$ のときは, 次の結果を得る.

定理 1 (i) $D(g, U_0)$ は $3-(g+1, \frac{g+1}{2}, \frac{(g+1)(g-3)}{8})$ design
であって, その blocks 集合は

$$U_0^G = \{U_i \mid i \in F_g\} \cup \{\bar{U}_i \mid i \in F_g\} \cup \{U_i \Delta U_j (= \bar{U}_i \Delta \bar{U}_j) \mid i \neq j \in F_g\} \\ \cup \{U_i \Delta \bar{U}_j (= \bar{U}_i \Delta U_j = \overline{U_i \Delta U_j}) \mid i \neq j \in F_g\}$$

である. (注. $g=7$ のとき, $D(7, U_0)$ は $3-(8, 4, 1)$ design である.) 特に, $D(g, U_0)$ が 4-design となるのは $g=11$ の
ときのみで, 実際

(ii) (Beth の定理 [1]) $D(11, U_0)$ は $5-(12, 6, 1)$ design である.

証明の概略: (i) Frobenius 群の基本性質と G の部分群の表から $G(U_0) = G_{\infty, 0}$ がわかり, これより design $D(8, U_0)$ のパラメータの値が求まる. 一方, G は Ω 上の 2 重可移群より, $G = G_\infty \cup G_\infty \tau G_\infty$ ($\tau: x \mapsto -\frac{1}{x}$) であるが, 次のことが容易に示される.

- $\sigma \in G_\infty, i \in F_2 \Rightarrow U_i^\sigma = U_{i\sigma}.$
- $U_0^\tau = \bar{U}_0.$
- $i \in Q \Rightarrow U_i^\tau = U_0 \Delta U_{i\tau}.$
- $i \in F_2 \setminus (\{0\} \cup Q) \Rightarrow U_i^\tau = \bar{U}_0 \Delta U_{i\tau}.$

これらから blocks 集合 U_0^G を書き上げることができる.

(ii) $D(11, U_0)$ の blocks 集合を $B = U_0^{PSL(2, 11)}$ とし, $\Omega(11)$ の任意の 5 点集合 T に対し, $\lambda(T) = |\{B \in B \mid T \subset B\}|$ とおく. B の元 (= blocks) 同士の共通部分の濃度を調べ, $\{(T, B) \mid T \subset \Omega(11), |T| = 5, T \subset B \in B\}$ を 2 通りにかぞえることによって, $\lambda(T) = 1 \ (\forall T)$ を得る.

定理 1 が示すように, $D(8, U_0)$ の blocks は, $U_i, \bar{U}_i$ ($i \in F_2$) の高々 2 つの Δ による結合である. 次に, 3 個以

上の結合を考える.

$$\begin{aligned} \mathbf{U}(f) : U_i, \bar{U}_i \ (i \in F_f) \text{ の } \Delta \text{ による有限個の結合の全体} \\ = \{ U_i, \bar{U}_i, U_i \Delta U_j, U_i \Delta \bar{U}_j, U_i \Delta U_j \Delta U_k, \dots \mid i, j, k, \dots (*) \in F_f \}. \end{aligned}$$

とすると, 次を得る.

命題. $A \in \mathbf{U}(f)$ とする.

- (i) $|A| \equiv 0 \pmod{2}$
- (ii) $f \equiv -1 \pmod{8} \Rightarrow |A| \equiv 0 \pmod{4}$.
- (iii) $f \equiv -1 \pmod{24} \Rightarrow 8 \leq |A|$.

上の命題を証明する際, 次の等式 — 自明な式 $|A \Delta B| = |A| + |B| - 2|A \cap B|$ の一般化 — が有効である.

- $A_1, A_2, \dots, A_n \ (n \geq 2)$ を有限集合の部分集合とすると

$$\begin{aligned} |A_1 \Delta A_2 \Delta \dots \Delta A_n| &= \sum_{1 \leq i \leq n} |A_i| - 2 \cdot \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| \\ &\quad + 2^2 \cdot \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| + \dots \\ &\quad + (-2)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

上の命題で, 特に $f = 23$ のときは

$$A \in \mathbf{U}(23) \Rightarrow |A| = 8, 12 \text{ 或 } 16$$

であるが, $|A| = 8$ なる A として, たとえば

$$U_0 \Delta U_1 \Delta U_4 = \{0, 4, 13, 14, 18, 19, 20, 22\}$$

がある。定理 1 (ii) と同様な証明で次を得る。

定理 2. $D(23, U_0 \Delta U_1 \Delta U_4)$ は $5-(24, 8, 1)$ design である。

以上の大半は既に知られているようであるが、こうしてある意味で — $D(g, A)$ に於て、適当な g と A をとることによって、あるいは対称差と群 G を通して — 統一的に、2つの Mathieu-Witt systems

$$\underline{W_{12}} = D(11, U_0)$$

$$\underline{W_{24}} = D(23, U_0 \Delta U_1 \Delta U_4)$$

を構成することができた。

これらの systems および $W_{11} = (W_{12})_\infty$, $W_{23} = (W_{24})_\infty$ — 勿論, $(W_i)_\infty$ は W_i から ∞ をとり除いてできる design, 即ち, 点 ∞ に関する W_i の内部構造 — の全ての blocks を統一的・簡潔に記述するために, 差型または代表 blocks という概念を導入する。

以下, $g = 11$ または 23 とし, $\Omega(g)$ の元の間に

$$\infty < 0 < 1 < 2 < \cdots < g-1$$

という全順序を入れておくことにする。

定義 $\Omega(f)$ の部分集合

$$A = \{a_1, a_2, \dots, a_k\} \quad (a_1 < a_2 < \dots < a_k)$$

1 に対し, 次のような $\tilde{A}$ を A の 差型 または 差輪 という:

$$\infty < a_1 \text{ なら } \tilde{A} = (a_2 - a_1, a_3 - a_2, \dots, a_k - a_{k-1}, a_1 - a_k)$$

$$= (a_3 - a_2, \dots, a_1 - a_k, a_2 - a_1) = \dots = (a_1 - a_k, a_2 - a_1, \dots, a_k - a_{k-1})$$

$$\infty = a_1 \text{ なら } \tilde{A} = (\infty, a_3 - a_2, a_4 - a_3, \dots, a_k - a_{k-1}, a_2 - a_k)$$

$$= (\infty, a_4 - a_3, \dots, a_2 - a_k, a_3 - a_2) = \dots = (\infty, a_2 - a_k, a_3 - a_2, \dots, a_k - a_{k-1})$$

また, $i = 11, 12, 23, 24$ として

$$\tilde{W}_i = \{ \tilde{B} \mid B : W_i \text{ の block } \}$$

を W_i の 差型 または 差輪 とよぶ. $d \in \tilde{W}_i$ に対し, $\tilde{B} = d$ なる W_i の任意の block B を 1 つ定めておき, それを差型 d に対応する 代表 block ということにする.

すぐ分るように, A, B を W_i の blocks とするとき,

$$\tilde{A} = \tilde{B} \quad (A, B \text{ は同一の差型をもつ})$$

$$\Leftrightarrow \exists c \in F_f; A = B + c \quad (A, B \text{ は } F_f \text{ の元による平行移動で互いにつながることができる})$$

定理 3. (i) W_i ($i = 11, 12, 23, 24$) の差型と代表 blocks は次の表のとおりである.

	Difference pattern	Representative blocks	Number
W_{12}	$(\infty, 1, 1, 1, 6, 2), (\infty, 1, 1, 2, 3, 4), (\infty, 1, 1, 3, 1, 5)$ $(\infty, 1, 2, 1, 4, 3), (\infty, 1, 2, 2, 2, 4), (\infty, 1, 3, 2, 3, 2);$ $(1, 1, 1, 1, 2, 5), (1, 1, 1, 4, 1, 3), (1, 1, 2, 1, 3, 3),$ $(1, 1, 3, 2, 2, 2), (1, 1, 4, 2, 1, 2), (1, 2, 2, 1, 2, 3).$	$\{\infty, 0, 1, 2, 3, 9\}, \{\infty, 0, 1, 2, 4, 7\}, \{\infty, 0, 1, 2, 5, 6\},$ $\{\infty, 0, 1, 3, 4, 8\}, \{\infty, 0, 1, 3, 5, 7\}, \{\infty, 0, 1, 4, 6, 9\};$ $\{0, 1, 2, 3, 4, 6\}, \{0, 1, 2, 3, 7, 8\}, \{0, 1, 2, 4, 5, 8\},$ $\{0, 1, 2, 5, 7, 9\}, \{0, 1, 2, 6, 8, 9\}, \{0, 1, 3, 5, 6, 8\}.$	12
W_{11}	$(1, 1, 1, 6, 2), (1, 1, 2, 3, 4), (1, 1, 3, 1, 5),$ $(1, 2, 1, 4, 3), (1, 2, 2, 2, 4), (1, 3, 2, 3, 2)$	$\{0, 1, 2, 3, 9\}, \{0, 1, 2, 4, 7\}, \{0, 1, 2, 5, 6\},$ $\{0, 1, 3, 4, 8\}, \{0, 1, 3, 5, 7\}, \{0, 1, 4, 6, 9\}.$	6
W_{24}	$(\infty, 1, 1, 1, 2, 9, 3, 6), (\infty, 1, 1, 4, 1, 12, 2, 2), (\infty, 1, 1, 6, 3, 1, 6, 5)$ $(\infty, 1, 1, 7, 1, 5, 5, 3), (\infty, 1, 2, 1, 7, 8, 1, 3), (\infty, 1, 2, 3, 2, 2, 3, 10),$ $(\infty, 1, 2, 4, 2, 7, 2, 5), (\infty, 1, 3, 2, 3, 3, 5, 6), (\infty, 1, 3, 6, 4, 4, 3, 2),$ $(\infty, 1, 4, 4, 2, 2, 8, 2), (\infty, 1, 4, 5, 2, 4, 3, 4);$ $(1, 1, 1, 1, 3, 3, 2, 11), (1, 1, 1, 5, 7, 1, 3, 4), (1, 1, 1, 10, 5, 2, 1, 2),$ $(1, 1, 2, 1, 4, 9, 1, 4), (1, 1, 2, 2, 2, 6, 6, 3), (1, 1, 2, 7, 4, 2, 4, 2),$ $(1, 1, 3, 1, 6, 1, 2, 8), (1, 1, 3, 2, 4, 5, 4, 3), (1, 1, 4, 4, 6, 1, 1, 5),$ $(1, 1, 7, 3, 2, 2, 5, 2), (1, 1, 8, 1, 2, 1, 5, 4), (1, 2, 2, 3, 1, 3, 8, 3),$ $(1, 2, 2, 5, 1, 4, 3, 5), (1, 2, 3, 1, 8, 2, 3, 3), (1, 2, 3, 6, 2, 4, 1, 4),$ $(1, 2, 4, 1, 3, 3, 7, 2), (1, 2, 6, 1, 7, 2, 2, 2), (1, 3, 1, 5, 3, 4, 3, 3),$ $(1, 3, 2, 1, 4, 2, 5, 5), (1, 3, 4, 4, 1, 6, 2, 2), (1, 5, 2, 1, 6, 3, 3, 2),$ $(2, 2, 4, 2, 3, 2, 3, 5).$	$\{\infty, 0, 1, 2, 3, 5, 14, 17\}, \{\infty, 0, 1, 2, 6, 7, 19, 21\}, \{\infty, 0, 1, 2, 8, 11, 12, 18\},$ $\{\infty, 0, 1, 2, 9, 10, 15, 20\}, \{\infty, 0, 1, 3, 4, 11, 19, 20\}, \{\infty, 0, 1, 3, 6, 8, 10, 13\},$ $\{\infty, 0, 1, 3, 7, 9, 16, 18\}, \{\infty, 0, 1, 4, 6, 9, 12, 17\}, \{\infty, 0, 1, 4, 10, 14, 18, 21\},$ $\{\infty, 0, 1, 5, 9, 11, 13, 21\}, \{\infty, 0, 1, 5, 10, 12, 16, 19\};$ $\{0, 1, 2, 3, 4, 7, 10, 12\}, \{0, 1, 2, 3, 8, 15, 16, 19\}, \{0, 1, 2, 3, 13, 18, 20, 21\},$ $\{0, 1, 2, 4, 5, 9, 18, 19\}, \{0, 1, 2, 4, 6, 8, 14, 20\}, \{0, 1, 2, 4, 11, 15, 17, 21\},$ $\{0, 1, 2, 5, 6, 12, 13, 15\}, \{0, 1, 2, 5, 7, 11, 16, 20\}, \{0, 1, 2, 6, 10, 16, 17, 18\},$ $\{0, 1, 2, 9, 12, 14, 16, 21\}, \{0, 1, 2, 10, 11, 13, 14, 19\}, \{0, 1, 3, 5, 8, 9, 12, 20\},$ $\{0, 1, 3, 5, 10, 11, 15, 18\}, \{0, 1, 3, 6, 7, 15, 17, 20\}, \{0, 1, 3, 6, 12, 14, 18, 19\},$ $\{0, 1, 3, 7, 8, 11, 14, 21\}, \{0, 1, 3, 9, 10, 17, 19, 21\}, \{0, 1, 4, 5, 10, 13, 17, 20\},$ $\{0, 1, 4, 6, 7, 11, 13, 18\}, \{0, 1, 4, 8, 12, 13, 19, 21\}, \{0, 1, 6, 8, 9, 15, 18, 21\},$ $\{0, 2, 4, 8, 10, 13, 15, 18\}.$	33
W_{23}	$(1, 1, 1, 2, 9, 3, 6), (1, 1, 4, 1, 12, 2, 2), (1, 1, 6, 3, 1, 6, 5),$ $(1, 1, 7, 1, 5, 5, 3), (1, 2, 1, 7, 8, 1, 3), (1, 2, 3, 2, 2, 3, 10),$ $(1, 2, 4, 2, 7, 2, 5), (1, 3, 2, 3, 3, 5, 6), (1, 3, 6, 4, 4, 3, 2),$ $(1, 4, 4, 2, 2, 8, 2), (1, 4, 5, 2, 4, 3, 4).$	$\{0, 1, 2, 3, 5, 14, 17\}, \{0, 1, 2, 6, 7, 19, 21\}, \{0, 1, 2, 8, 11, 12, 18\},$ $\{0, 1, 2, 9, 10, 15, 20\}, \{0, 1, 3, 4, 11, 19, 20\}, \{0, 1, 3, 6, 8, 10, 13\},$ $\{0, 1, 3, 7, 9, 16, 18\}, \{0, 1, 4, 6, 9, 12, 17\}, \{0, 1, 4, 10, 14, 18, 21\},$ $\{0, 1, 5, 9, 11, 13, 21\}, \{0, 1, 5, 10, 12, 16, 19\}.$	11

$$W_{12} = D(11, U_0), W_{11} = (W_{12})_{\infty}; \quad W_{24} = D(23, U_0 \Delta U_1 \Delta U_4), W_{23} = (W_{24})_{\infty}$$

All the blocks of W_{12}, W_{11} (respe, W_{24}, W_{23}) are obtained by translating the representative blocks by all elements of F_{11} (resp., F_{23}).

(ii) $W_{12}, W_{11} (W_{24}, W_{23})$ の全ての blocks は, 代表 blocks を $F_{11} (F_{23})$ の元で平行移動することによって得られる. (たとえば, W_{24} の $759 = 33 \cdot 23$ 個の全 blocks は, 33 個の代表 blocks を F_{23} の元で平行移動して得られる.)

証明は, W_{12} と W_{24} の差型を直接計算で出すだけである.
たとえば, W_{24} の場合,

$$U = U_0 \triangle U_1 \triangle U_4, \quad G = \text{PSL}(2, 23) \ni \tau: x \mapsto -\frac{1}{x}$$

とすると, 直接計算によって

$$W_{24} \text{ の blocks 集合} = U^G = \{aU + b, a(U+b)^{\tau} + c \mid a \in \mathbb{Q}; b, c \in F_{23}\},$$

$$\widetilde{W}_{24} = \{\widetilde{aU}, \widetilde{aU^{\tau}}, \widetilde{a(U+b)^{\tau}} \mid a \in \mathbb{Q}\}.$$

この $\widetilde{W}_{24}$ の元を具体的に書き表したのが定理3の表における W_{24} の差型である. 差型から代表 blocks は直ちに求まる.
また, $\widetilde{W}_{24}$ の表の中で ∞ を含む 11 個のものから ∞ をとり除けば $\widetilde{W}_{23}$ が得られる.

差型の利点と応用

① 定理3で見たように, 差型あるいは代表 blocks は, Mathieu-Witt systems $W_{24}, W_{23}, W_{12}, W_{11}$ の全ての blocks をある意味で統一的に記述する簡単な方法を与えて

いるといえる。(注. $W_{22} = (W_{23})_0$ はやや異質である.

$|\widetilde{W}_{22}| = 77 = W_{22}$ の blocks の個数 で, W_{22} の差型は無意味である. しかし, W_{22} の全ての blocks も, W_{23} の 11 個の代表 blocks を F_{23} の適当な 7 個の元で平行移動すれば得られる.)

次の 2, 3 は W_{24} について述べるが, 他の W_i でも同様になりつつ.

②. $\Omega(23)$ の 8 点集合 A が W_{24} の block かどうかの判定:

$$A : W_{24} \text{ の block } \iff \tilde{A} \in \widetilde{W}_{24}$$

たとえば, $A = \{\infty, 0, 1, 3, 12, 15, 21, 22\}$ とすると,

$$\tilde{A} = (\infty, 1, 2, 9, 3, 6, 1, 1) = (\infty, 1, 1, 1, 2, 9, 3, 6) \in \widetilde{W}_{24}$$

より, A は W_{24} の block である.

③. 与えられた 5 点を含む W_{24} の unique block の見つけ方: たとえば, $\Omega(23)$ の与えられた 5 点を $A = \{0, 5, 6, 15, 18\}$ とする. W_{24} の差型表から, その適当な部分和が

$$\tilde{A} = (5, 1, 9, 3, 5) \text{ であるような差型を探すと, ただ 1 つ}$$

$$\text{の差型 } \quad \underbrace{(1, 1, 8)}_5, \underbrace{(1, 2, 1)}_9, \underbrace{(5, 4)}_3$$

が見つかる. 従って, 求める block は

$$\begin{array}{ccccccc} & 4 & & 14 & & 17 & \\ & \swarrow \quad \searrow & & \swarrow \quad \searrow & & \swarrow \quad \searrow & \\ 0 & & 5 & & 6 & & 15 & & 18 \\ & \swarrow \quad \searrow & & \swarrow \quad \searrow & & \swarrow \quad \searrow & \\ & 5 & & 1 & & 9 & & 3 & & 5 \end{array} \quad \text{即ち, } \{0, 4, 5, 6, 14, 15, 17, 18\}.$$

なお、近藤武先生は、与えられた $s (\leq 5)$ 個の点を含む全ての blocks を直ちにを見つけるパソコンのプログラムを作って下さった。

最後に、2, 3 の注意をつけ加える。

(1) これまでの全ての議論に於て、 $U_i = \{i\} \cup Q_i$ の代りに $V_i = \{\infty\} \cup Q_i$ を用いても全く同様のことがなりたち、

$$D(8, U_0) \cong D(8, V_0); \quad D(23, U_0 \Delta U_1 \Delta U_4) \cong D(23, V_0 \Delta V_1 \Delta V_4)$$

(design として同型) である。Todd [5] に出ている W_{24} の blocks の表や Curtis [2] の MOG によるものは、上の定理 3 (ii) による blocks の表 ($D(23, U_0 \Delta U_1 \Delta U_4)$) と一致している。

また、 $D(23, U_0 \Delta U_1 \Delta U_4)$ と $D(23, V_0 \Delta V_1 \Delta V_4)$ の差型とは逆回りである：

$$\text{ある} : (d_1, d_2, \dots, d_8) \in \overline{D(23, U_0 \Delta U_1 \Delta U_4)}$$

$$\iff (d_8, \dots, d_2, d_1) \in \overline{D(23, V_0 \Delta V_1 \Delta V_4)}.$$

(2) 定理 1(i) の証明では、Frobenius 群の基本性質と $G = \text{PSL}(2, 8)$ の部分群の表を用いたが、その他の全ての議論は全く初等的である。特に、定理 1(ii), 定理 2, 3 の証明は完全に初等的である。

(3) Curtis の MOG [2] も差型も、その正体が私にはまだよく分らないが、差型に現われる数列はどのような規則で並んでいるのだろうか？ MOG や差型を決定ないしは

control している, より本質的な何かがあるのだろうか?

本稿の詳しい内容は [3] を参照されたい.

参 考 文 献

- [1] T. Beth: Some remarks on D.R. Hughes' construction of M_{12} and its associated designs, in "Finite geometries and designs", London Math. Soc. Lect. Note Ser. 49, 22-30, Camb. Univ. Press, 1981.
- [2] R.T. Curtis: A new combinatorial approach to M_{24} , Math. Proc. Camb. Phil. Soc. 79 (1976), 25-42.
- [3] S. Iwasaki: An elementary and unified approach to the Mathieu-Witt systems, to appear.
- [4] R.N. Lane: t -designs and t -ply homogeneous groups, J. Comb. Th. 10 (1971), 106-118.
- [5] J.A. Todd: A representation of the Mathieu group M_{24} as a collineation group, Ann. di Math. Pura. ed. Appl. 71 (1966), 199-238.