J. Math. Soc. Japan
Vol. 40, No. 3, 1988

An elementary and unified approach to the Mathieu-Witt systems

Dedicated to Professor Nagayoshi Iwahori on his 60th birthday

By Shiro IWASAKI

(Received Dec. 17, 1986)

1. Introduction.

Up to now, a great variety of interesting and suggestive studies on the Mathieu-Witt systems $\boldsymbol{W}_{24}$ and $\boldsymbol{W}_{12}$ have been made by many people. In particular, Cameron [2, Chapters 2, 3] and Conway [4, Section 3] (resp., Beth [1]) studied $\boldsymbol{W}_{24}$ (resp., $\boldsymbol{W}_{12}$) using symmetric differences effectively, and Curtis [5] (resp., [6]) studied them introducing the somewhat magical concepts of the MOG=Miracle Octad Generator (resp., the Kitten). Although these studies have revealed many fascinating facts about the systems, it seems that the essence of them is not yet satisfactorily elucidated — for example, it seems that the treatment of both systems is not sufficiently unified and that the way of describing blocks is not so simple.

The aim of this article is to present a description of both systems from scratch in as orderly, unified and elementary a manner as possible, using mainly symmetric differences and linear fractional groups PSL(2, q). The next section collects some notation (including $\boldsymbol{D}(q, A)$) and facts on symmetric differences, which are used throughout the article. In Sections 3 and 4, in a unified way (via $\boldsymbol{D}(q, A)$) we construct the two systems and an infinite class of 3-$(q+1, (q+1)/2, (q+1)(q-3)/8)$ designs, where q is a prime power with $q\equiv -1$ (mod 4) and $q>7$. In Section 5, which is the main body of this article, we present a simple and unified way of describing all the blocks of the two systems (and $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{11}$). Namely, (instead of the MOG and Kitten) we introduce a concept of difference patterns or representative blocks, which enables us to enumerate all the blocks uniformly and immediately, and to find quickly the unique block containing five (four) given points.

All the discussions (except the proof of Proposition 3.1) in this article are completely elementary, and a considerable part of them already may be known

This research was partially supported by Grant-in-Aid for Scientific Research (Nos. 61540088 and 61540146), Ministry of Education, Science and Culture.

implicitly or explicitly, but we give a full description for readableness and self-containedness.

Our motive, idea and method are greatly influenced by the above literature, and I would like to express my deep indebtedness to the authors. I am also very grateful to Professor Takeshi Kondo for his interest to this work and helpful comments. Finally, I would like to thank the referee for his careful reading and improving redundancies of the original manuscript.

2. Notation and preliminaries.

We use the following notation.

$\dot{\cup}$: disjoint set union.

For a finite set S and any subsets A, B of S,

$A\setminus B=\{a \mid a\in A \text{ and } a\notin B\}$,

$\bar{A}=S\setminus A$: complement of A in S,

$A\triangle B=(A\setminus B)\cup(B\setminus A)=(A\cup B)\setminus(A\cap B)$: symmetric difference of A and B.

For a permutation group H on S and for a subset $A=\{a, b, \cdots\}$ of S,

A^{σ}: image of A under $\sigma\in H$,

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

$H_{(A)}=H_{\{a,b,\cdots\}}=\{\sigma\in H \mid A^{\sigma}=A\}$,

$H_{A}=H_{a,b,\cdots}=\{\sigma\in H \mid a^{\sigma}=a,\ b^{\sigma}=b,\ \cdots\}$.

For $d\in S\setminus A$, $H_{d,(A)}=H_{(A),d}$ denotes $(H_{d})_{(A)}=(H_{(A)})_{d}=H_{d}\cap H_{(A)}$.

For a subgroup K of H and $\sigma\in H$, and for a collection $\mathfrak{B}$ of subsets of S,

$K^{\sigma}=\sigma^{-1}K\sigma$,

$\mathfrak{B}^{\sigma}=\{B^{\sigma} \mid B\in\mathfrak{B}\}$.

Throughout this article we fix the following notation.

q: prime power with $q\equiv-1 \pmod 4$ and $q>7$.

F_{q}: finite field with q elements.

$\Omega=\{\infty\}\cup F_{q}$: projective line over F_{q}.

$Q=\{x^{2} \mid x\in F_{q}\setminus\{0\}\}$: set of non-zero square elements of F_{q}.

$U_{0}=\{0\}\cup Q$.

$V_{0}=\{\infty\}\cup Q$.

$N=F_{q}\setminus U_{0}$: set of non-square elements of F_{q}.

Set $aX+b=\{ax+b \mid x\in X\}$ for $X\subset\Omega$ and $a, b\in F_{q}$.

For $i\in F_{q}$,

$Q_{i}=Q+i \quad (Q_{0}=Q)$,

$U_{i}=\{i\}\cup Q_{i}=U_{0}+i$,

$V_{i}=\{\infty\}\cup Q_{i}=V_{0}+i$,

$\bar{U}_{i}=\Omega\setminus U_{i}$, $\bar{V}_{i}=\Omega\setminus V_{i}$.

$U_{\infty}=V_{\infty}=\Omega$.

For $a, b, c, d\in F_q$,

$\sigma_{a,b,c,d}: x\mapsto(ax+b)/(cx+d)$,

$\sigma_{a,b}=\sigma_{a,b,0,1}: x\mapsto ax+b$,

$\sigma_b=\sigma_{1,b,0,1}: x\mapsto x+b$,

$\tau=\sigma_{0,-1,1,0}: x\mapsto -1/x$,

$\tau'=\sigma_{0,1,1,0}: x\mapsto 1/x$.

$\mathrm{PGL}(2, q)=\{\sigma_{a,b,c,d}\mid a, b, c, d\in F_q;\ ad-bc\neq 0\}$.

$G=\mathrm{PSL}(2, q)=\{\sigma_{a,b,c,d}\mid a, b, c, d\in F_q;\ ad-bc\in Q\}$.

Note that G acts 2-transitively on Ω and that

$G_\infty=\{\sigma_{a,b}\mid a\in Q,\ b\in F_q\}$,

$G_{\infty,0}=\{\sigma_{a,0}\mid a\in Q\}$,

and $|G|=(q+1)q(q-1)/2$.

We begin by recalling elementary well-known definitions and facts. Let S be a set of v points and let $\mathfrak{B}$ be a collection of k-subsets (called *blocks*) of S. The pair $(S, \mathfrak{B})$ is called a *t-(v, k, λ) design* (with $v>k>t>0$ and $\lambda>0$) if any t-subset of S is contained in exactly λ blocks of $\mathfrak{B}$. Two designs $(S, \mathfrak{B})$ and $(S', \mathfrak{B}')$ having the same parameters t, v, k, λ are said to be *isomorphic* if there is a bijection σ from S onto S' such that $\mathfrak{B}^\sigma=\mathfrak{B}'$. A t-(v, k, λ) design $(S, \mathfrak{B})$ is also an s-(v, k, λ_s) design for any $s\leqq t$, where $\lambda_s=\lambda\binom{v-s}{t-s}\Big/\binom{k-s}{t-s}$, and in particular $|\mathfrak{B}|=\lambda_0=\lambda\binom{v}{t}\Big/\binom{k}{t}$. A t-design with $\lambda=1$ is called a *Steiner system* and the most celebrated ones are 5-(12, 6, 1), 4-(11, 5, 1), 5-(24, 8, 1), 4-(23, 7, 1) and 3-(22, 6, 1) designs, which are called *Mathieu designs* or *Witt systems*. Their existence and uniqueness (up to isomorphism) have been proved by many people since Witt [**12**, **13**], and they are sometimes denoted by $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$, $\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$ and $\boldsymbol{W}_{22}$, respectively. The number of their blocks are $12\cdot 11$, $6\cdot 11$, $33\cdot 23$, $11\cdot 23$ and $11\cdot 7$, respectively.

A permutation group H on a finite set S is said to be *t-homogeneous* if for any two (unordered) t-subsets of S, say T and T', there exists $\sigma\in H$ such that $T^\sigma=T'$. In general, any t-homogeneous permutation group yields a t-design:

PROPOSITION 2.1 (see, e.g. Lane [**9**, Theorem 2.1]). *Let H be a t-homogeneous permutation group on a finite set S with $|S|=v$. Then for any $A\subset S$ with $|A|=k\geqq t$, the pair (S, A^H) is a t-(v, k, λ) design, where*

$$\lambda=|H:H_{(A)}|\binom{k}{t}\Big/\binom{v}{t}.$$

SKETCH of PROOF. Setting $\lambda(T)=|\{B\mid T\subset B\in A^H\}|$ for any t-subset T of S, the t-homogeneity of H implies at once that $\lambda(T)$ has a constant value λ, which is easily calculated by counting in two ways the number of ordered pairs (T, B) satisfying $T\subset S$, $|T|=t$ and $T\subset B\in A^H$. □

From assumption $q\equiv-1(\mathrm{mod}\,4)$ (this is equivalent to the assumption that $(q-1)/2$ is odd), the following are easily checked:

(i) $i\in Q$ if and only if $-i\in N$ (in particular, $-1\in N$).

(ii) G acts 3-homogeneously on Ω.

(iii) G_∞ acts 2-homogeneously on F_q.

NOTATION. From Proposition 2.1 and (ii), it follows that for any $k\,(\geqq 3)$-subset $A\subset\Omega$, the pair (Ω, A^G) is a 3-$(q+1, k, \lambda)$ design, where

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

We denote this design by $\boldsymbol{D}(q, A)$.

Consider a problem: *What q and A yield an interesting design $\boldsymbol{D}(q, A)$?* We shall deal with the case $A=V_0$ (or U_0) in Section 3 and with the case $q=23$ and $A=V_0\triangle V_1\triangle V_4$ (or $U_0\triangle U_1\triangle U_4$) in Section 4. The special case $\boldsymbol{D}(11, A)$ in the former (resp., $\boldsymbol{D}(23, A)$ in the latter) is a 5-(12, 6, 1) (resp., 5-(24, 8, 1)) design. In the remainder of this section we prepare for treating them.

As is easily seen, the set 2^S of all subsets of any (finite) set S forms a commutative ring with respect to addition defined by $A\triangle B$ and multiplication by $A\cap B$ for $A, B\in 2^S$. Also, with respect to this addition and trivial scalar multiplication, 2^S forms a vector space over the field F_2 with a basis S. The empty set $\emptyset$ is the zero element of 2^S, and $A\triangle A=\emptyset$, $\bar{A}$ $(=S\setminus A)=S\triangle A$ for any $A\in 2^S$. It is immediately checked that for $A, B\in 2^S$, we have

$$\overline{A\triangle B}=\bar{A}\triangle B=A\triangle\bar{B}\quad\text{and}\quad\bar{A}\triangle\bar{B}=A\triangle B.$$

Further, if a group H acts on S, then for any $\sigma\in H$,

$$(A\triangle B)^\sigma=A^\sigma\triangle B^\sigma\quad\text{and}\quad\bar{A}^\sigma=\overline{A^\sigma}.$$

Obviously

$$|A\triangle B|=|A|+|B|-2|A\cap B|,$$

since $A\triangle B=(A\setminus(A\cap B))\dot{\cup}(B\setminus(A\cap B))$. This equality is easily generalized by induction:

PROPOSITION 2.2. *Let $A_1, A_2, \cdots, A_n$ $(n\geqq 2)$ be subsets of a finite set. Then*

$$\begin{aligned}|A_1\triangle A_2\triangle\cdots\triangle A_n|=&\sum_{1\leq i\leq n}|A_i|-2\sum_{1\leq i_1<i_2\leq n}|A_{i_1}\cap A_{i_2}|\\&+2^2\sum_{1\leq i_1<i_2<i_3\leq n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}|\\&-2^3\sum_{1\leq i_1<i_2<i_3<i_4\leq n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}\cap A_{i_4}|\\&+\cdots+(-2)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|.\end{aligned}$$

COROLLARY 2.3. *Let $A_1, A_2, \cdots, A_n$ $(n\geqq 2)$ be subsets of a finite set. Then*
(i) $|A_1\triangle A_2\triangle\cdots\triangle A_n| \equiv |A_1|+|A_2|+\cdots+|A_n| \pmod 2$;
(ii) *If* $|A_i|\equiv 0 \pmod 4$ *and* $|A_i\cap A_j|\equiv 0 \pmod 2$ *for all* i, j, *then*

$$|A_1\triangle A_2\triangle\cdots\triangle A_n| \equiv 0 \pmod 4;$$

(iii) *If* $|A_i|=a$ *for all* i *and* $|A_i\cap A_j|=d$ *for all distinct* i, j, *then*

$$|A_1\triangle A_2\triangle\cdots\triangle A_n| \equiv n(a-(n-1)d) \pmod 4.$$

As mentioned before, the set 2^{Ω} forms a vector space of dimension $|\Omega|=q+1$ over F_2.

NOTATION. We denote by $\mathfrak{V}(q)$ (resp., $\mathfrak{U}(q)$) the subspaces of 2^{Ω} generated by all the V_i (resp., U_i):

$$\mathfrak{V}(q)=\langle V_i \mid i\in\Omega\rangle, \qquad \mathfrak{U}(q)=\langle U_i \mid i\in\Omega\rangle.$$

Note that for any $A\in\mathfrak{V}(q)$ (resp., $\mathfrak{U}(q)$) we have $\bar{A}\,(=\Omega\setminus A)=V_\infty\triangle A=U_\infty\triangle A\in\mathfrak{V}(q)$ (resp., $\mathfrak{U}(q)$), particularly $\bar{V}_i\in\mathfrak{V}(q)$ and $\bar{U}_i\in\mathfrak{U}(q)$ for all $i\in F_q$.

PROPOSITION 2.4. *Let $\sigma\in G_\infty$ and $i, j\in F_q$. Then we have*

$$Q_i^\sigma=Q_{i^\sigma}, \quad V_i^\sigma=V_{i^\sigma} \quad \textit{and} \quad U_i^\sigma=U_{i^\sigma};$$
$$(V_i\triangle V_j)^\sigma=V_{i^\sigma}\triangle V_{j^\sigma} \quad \textit{and} \quad (U_i\triangle U_j)^\sigma=U_{i^\sigma}\triangle U_{j^\sigma}.$$

PROOF. Each $\sigma\in G_\infty$ is written as $\sigma=\sigma_{a,b}$ $(a\in Q,\ b\in F_q)$ and so $Q_i^\sigma=aQ_i+b=a(Q+i)+b=aQ+(ai+b)=Q+i^\sigma=Q_{i^\sigma}$, obtaining the first equality. This yields at once the remaining equalities. □

LEMMA 2.5. *For any $i\in Q$, we have*
(i) $\{0\}\cup Q_i^\tau\subset Q\cup Q_{i^\tau}$;
(ii) $(\{0\}\cup Q_i^\tau)\cap Q\cap Q_{i^\tau}=\emptyset$;
(iii) $Q\setminus Q_{i^\tau}\subset Q_i^\tau$;
(iv) $Q_{i^\tau}\setminus Q\subset\{0\}\cup Q_i^\tau$;
(v) $\{0\}\cup Q_i^\tau=Q\triangle Q_{i^\tau}$.

PROOF. (i), (ii) Clearly $0=1/i+i^\tau\in Q_{i^\tau}$. Let $x\in Q$ and $y=(x+i)^\tau$ be any element of Q_i^τ. Then, since $y=-1/(x+i)=(-1/(x+i)+1/i)+(-1/i)=x/i(x+i)+i^\tau$, we have

$$y\notin Q \text{ if and only if } x+i\in Q \text{ if and only if } y\in Q_{i^\tau}.$$

This yields (i) and (ii).

(iii), (iv) Let $x(\neq 0)\in(Q\setminus Q_{i^\tau})\cup(Q_{i^\tau}\setminus Q)$. Since $(ix+1)/i=x-i^\tau$, it follows that, if $x\in Q\setminus Q_{i^\tau}$ (resp., $\in Q_{i^\tau}\setminus Q$), then $x-i^\tau\notin Q$ (resp., $\in Q$), $ix+1\notin Q$ (resp., $\in Q$), and so $-1/x-i=-(ix+1)/x\in Q$. This implies that $x=-1/((-1/x-i)+i)$

$\in Q_i^\tau$.

(v) (i) and (ii) imply that $\{0\}\cup Q_i^\tau\subset Q\cup Q_{i^\tau}\setminus(Q\cap Q_{i^\tau})=Q\triangle Q_{i^\tau}$. (iii) and (iv) imply that $\{0\}\cup Q_i^\tau\supset(Q\setminus Q_{i^\tau})\cup(Q_{i^\tau}\setminus Q)=Q\triangle Q_{i^\tau}$. □

PROPOSITION 2.6. (i) $V_0^\tau=\bar{V}_0$, $U_0^\tau=\bar{U}_0$.

(ii) $V_i^\tau=V_0\triangle V_{i^\tau}$ *and* $U_i^\tau=U_0\triangle U_{i^\tau}$ *for any* $i\in Q$.

(iii) $V_i^\tau=\bar{V}_0\triangle V_{i^\tau}$ *and* $U_i^\tau=\bar{U}_0\triangle U_{i^\tau}$ *for any* $i\in N$.

PROOF. (i) Since $Q^\tau=N$, it follows immediately that $V_0^\tau=(\{\infty\}\cup Q)^\tau=\{0\}\cup N=\bar{V}_0$. Similarly $U_0^\tau=\bar{U}_0$.

(ii) Let $i\in Q$. By Lemma 2.5 (v),

$$V_i^\tau=(\{\infty\}\cup Q_i)^\tau=\{0\}\cup Q_i^\tau=Q\triangle Q_{i^\tau}=V_0\triangle V_{i^\tau}.$$

Also,

$$\begin{aligned}U_i^\tau&=(\{i\}\cup Q_i)^\tau=\{i^\tau\}\cup Q_i^\tau=\{i^\tau\}\cup(Q\triangle Q_{i^\tau})\setminus\{0\}\\&=(\{0\}\cup Q)\triangle(\{i^\tau\}\cup Q_{i^\tau})\qquad\text{(Note that } i^\tau\notin Q \text{ and } 0\in Q_{i^\tau}.)\\&=U_0\triangle U_{i^\tau}.\end{aligned}$$

(iii) Let $i\in N$. Then $i^\tau\in Q$ and by (ii) we have $(V_{i^\tau})^\tau=V_0\triangle V_{(i^\tau)^\tau}=V_0\triangle V_i$. Therefore, $\bar{V}_0\triangle V_i^\tau=(V_0\triangle V_i)^\tau=V_{i^\tau}$, and so $V_i^\tau=\bar{V}_0\triangle V_{i^\tau}$. Similarly we have $U_i^\tau=\bar{U}_0\triangle U_{i^\tau}$. □

COROLLARY 2.7. (i) *G acts on $\mathfrak{V}(q)$ and $\mathfrak{U}(q)$.*

(ii) *For any distinct i, $j\in F_q$, we have*

$$|Q_i\triangle Q_j|=|V_i\triangle V_j|=|\bar{V}_i\triangle V_j|=|U_i\triangle U_j|=|\bar{U}_i\triangle U_j|=(q+1)/2,$$

$$\begin{aligned}|V_i\cap V_j|&=|\bar{V}_i\cap V_j|=|\bar{V}_i\cap\bar{V}_j|=|U_i\cap U_j|=|\bar{U}_i\cap U_j|\\&=|\bar{U}_i\cap\bar{U}_j|=(q+1)/4,\end{aligned}$$

$$|Q_i\cap Q_j|=(q-3)/4.$$

PROOF. (i) follows immediately from Propositions 2.4 and 2.6, since $G=\langle G_\infty,\tau\rangle$.

(ii) $|V_0\triangle V_{-1}|=|V_1^\tau|=|V_1|=(q+1)/2$ by Proposition 2.6. Since G_∞ acts 2-homogeneously on F_q, there exists $\sigma\in G_\infty$ with $\{0,-1\}^\sigma=\{i,j\}$. Hence

$$|V_i\triangle V_j|=|(V_0\triangle V_{-1})^\sigma|=|V_0\triangle V_{-1}|=(q+1)/2,$$

and so $|V_i\cap V_j|=(|V_i|+|V_j|-|V_i\triangle V_j|)/2=(q+1)/4$. Similarly we have the other equalities. □

By Corollaries 2.3 and 2.7, we have

PROPOSITION 2.8. (i) $|A|\equiv 0\pmod 2$ *for any* $A\in\mathfrak{V}(q)$.

(ii) *If* $q\equiv -1\pmod 8$, *then*

(1) $|A|\equiv 0 \pmod 4$ *for any* $A\in\mathfrak{V}(q)$;

(2) $|A\cap B|\equiv 0 \pmod 2$ *for any distinct* $A, B\in\mathfrak{V}(q)$.

(*The same is true of* $\mathfrak{U}(q)$.)

REMARK 2.1. Although G acts on $\mathfrak{V}(q)$ and $\mathfrak{U}(q)$ by Corollary 2.7, it is immediately seen that if $q\equiv -1 \pmod 8$ then $U_0\notin\mathfrak{V}(q)$, $V_0\notin\mathfrak{U}(q)$ (so $\mathfrak{V}(q)\neq\mathfrak{U}(q)$) and PGL(2, q) acts on neither $\mathfrak{V}(q)$ nor $\mathfrak{U}(q)$. In fact, if $U_0\in\mathfrak{V}(q)$ then $\{\infty, 0\}=U_0\triangle V_0\in\mathfrak{V}(q)$, which contradicts Proposition 2.8 (ii, 1). Hence $U_0\notin\mathfrak{V}(q)$ and so PGL(2, q) does not act on $\mathfrak{V}(q)$, for PGL(2, q)$\ni\tau'$ and $V_0^{\tau'}=U_0$.

On the other hand, in the case $q=11$ we have

$$U_0 = V_0\triangle V_2\triangle V_6\triangle V_7\triangle V_8\triangle V_{10} \in \mathfrak{V}(11),$$

$$V_0 = U_\infty\triangle U_2\triangle U_6\triangle U_7\triangle U_8\triangle U_{10} \in \mathfrak{U}(11).$$

Therefore $\{\infty, 0\}=U_0\triangle V_0\in\mathfrak{V}(11)$ (so there exists $A\in\mathfrak{V}(11)$ with $|A|=2$) and $U_i=U_0^{\sigma_i}\in\mathfrak{V}(11)$, $V_i=V_0^{\sigma_i}\in\mathfrak{U}(11)$ for all $i\in F_{11}$ and so $\mathfrak{V}(11)=\mathfrak{U}(11)$. Also, since $V_0^{\tau'}=U_0$ and $V_i^{\tau'}=V_0^{\sigma_i\tau'}=V_0^{\tau'\sigma_{1,0,i,1}}=U_0^{\sigma_{1,0,i,1}}\in\mathfrak{V}(11)$ for any $i\in F_{11}$, it follows that PGL(2, 11) acts on $\mathfrak{V}(11)$.

PROPOSITION 2.9. *If* $q\equiv -1 \pmod{24}$, *then*

$$|A|\geqq 8 \quad \textit{for any } A\ (\neq\emptyset)\in\mathfrak{V}(q) \textit{ or } \mathfrak{U}(q).$$

PROOF. Assume that there exists $A\in\mathfrak{V}(q)$ or $\mathfrak{U}(q)$ with $|A|=4$ and set $A=\{a, b, c, d\}$. Since G is 3-homogeneous on Ω, it follows that $|G:G_{\{a,b,c\}}| =\binom{q+1}{3}$ and so $G_{\{a,b,c\}}$ is a cyclic group of order 3. As a generator of $G_{\{a,b,c\}}$, we may take $\sigma=(a, b, c)\cdots$. Since $q-2\equiv 0 \pmod 3$ and 3 is not a divisor of $|G_d|=q(q-1)/2$, we have $G_{\{a,b,c\}}\cap G_d=1$. Hence σ moves d and so $A\cap A^\sigma =\{a, b, c\}$, which contradicts Proposition 2.8 (ii, 2), since $A^\sigma\in\mathfrak{V}(q)$ or $\mathfrak{U}(q)$ by Corollary 2.7 (i). □

By Propositions 2.8 (ii, 1) and 2.9, we have

COROLLARY 2.10. *Suppose* $q\equiv -1 \pmod{24}$. *Then*

(i) *For any* $A(\neq\emptyset, \Omega)\in\mathfrak{V}(q)$ *or* $\mathfrak{U}(q)$, *we have*

$$|A| = 8, 12, 16, \cdots, \textit{ or } (q+1)-8;$$

(ii) *For any distinct* $A, B\in\mathfrak{V}(q)$ *or* $\mathfrak{U}(q)$ *with* $|A|=|B|=r$ *and* $r\neq 0$, $r\neq q+1$, *we have*

$$|A\cap B| = r-4, r-6, r-8, \cdots, \textit{ or } r-(q+1-8)/2.$$

3. An infinite class of 3-designs and W_{12}.

In this section we deal with the designs $\boldsymbol{D}(q, V_0)$ and $\boldsymbol{D}(q, U_0)$.

PROPOSITION 3.1. (i) *For any* $i \in F_q$, *we have*

$$G_{(V_i)} = G_{(\bar{V}_i)} = G_{\infty, i} = G_{(U_i)} = G_{(\bar{U}_i)}.$$

(ii) *For any distinct* $i, j \in F_q$, *we have*

$$G_{(V_i \triangle V_j)} = G_{(\overline{V_i \triangle V_j})} = G_{i,j} = G_{(U_i \triangle U_j)} = G_{(\overline{U_i \triangle U_j})}.$$

PROOF. The first and last equalities in (i) and (ii) are obvious.

(i) First we show that $G_{\infty,(V_0)} = G_{\infty,(Q)} = G_{\infty,0}$. It is immediate that $G_{\infty,(V_0)} = G_{\infty,(Q)} \supset G_{\infty,0} = \{\sigma_{a,0} \mid a \in Q\}$. Let $\sigma \in G_{\infty,(V_0)}$. Then σ is expressible as $\sigma = \sigma_{a,b}$ for some $a \in Q$, $b \in F_q$, and $b = 0^\sigma \notin Q^\sigma = Q$. If $b \in N$, then $-b/a \in Q$ and so $0 = (-b/a)^\sigma \in Q$, a contradiction. Thus we have $b=0$, $\sigma = \sigma_{a,0}$ and so $G_{\infty,(V_0)} \subset G_{\infty,0}$.

Secondly we show that $G_{(V_0)} = G_{\infty,(V_0)}$. Suppose this false and set $H = G_{(V_0)}$. Then, since $H \not\subset G_\infty$ and $H_\infty = G_{\infty,0}$ acts regularly on $Q = V_0 \setminus \{\infty\}$, it follows that the permutation group (H, V_0) is a sharply 2-transitive Frobenius group. The Frobenius kernel N of H is elementary abelian (see, e.g. Tsuzuku [**11**, Theorem 2.11.7]), and so we may set $|N| = |V_0| = (q+1)/2 = 2^e$ with some integer e. On the other hand, from the well-known list of the subgroups of $G = \mathrm{PSL}(2, q)$ (see, e.g. Huppert [8, II.8.27]) e must be 1 or 2. This is contrary to our assumption $q > 7$. Thus we have shown $G_{(V_0)} = G_{\infty,(V_0)} = G_{\infty,0}$. Therefore $G_{(V_i)} = G_{(V_0)}^{\sigma_i} = G_{\infty,0}^{\sigma_i} = G_{\infty,i}$ for any $i \in F_q$. Also, since the involution of $\mathrm{PGL}(2, q)$

$$\tau_i = \sigma_i^{-1} \tau' \sigma_i : \ x \mapsto 1/(x-i) + i$$

normalizes G, and interchanges ∞ and i, V_i and U_i, it follows that

$$G_{(U_i)} = G_{(V_i)}^{\tau_i} = G_{\infty,i}^{\tau_i} = G_{\infty,i}.$$

(ii) From Proposition 2.6 and (i), it follows that $G_{(V_0 \triangle V_1)}^{\tau} = G_{(V_0^\tau \triangle V_1^\tau)} = G_{(\bar{V}_0 \triangle V_0 \triangle V_{-1})} = G_{(\Omega \triangle V_{-1})} = G_{(\bar{V}_{-1})} = G_{\infty,-1}$ and so that $G_{(V_0 \triangle V_1)} = G_{\infty,-1}^{\tau} = G_{0,1}$. If we set

$$\sigma = \begin{cases} \sigma_{j-i,i} & \text{if } j-i \in Q \\ \sigma_{i-j,j} & \text{if } j-i \in N \quad (\text{i.e., } i-j \in Q), \end{cases}$$

then $\sigma \in G_\infty$, $\{0, 1\}^\sigma = \{i, j\}$ and we have $G_{(V_i \triangle V_j)} = G_{(V_0 \triangle V_1)}^\sigma = G_{0,1}^\sigma = G_{i,j}$. Similarly we have $G_{(U_i \triangle U_j)} = G_{i,j}$. □

REMARK 3.1. In the case $q=7$, we have $G_{\infty,(V_0)} = G_{\infty,0} \cong A_3$, whereas $G_{(V_0)} \ni \sigma_{1,2,1,-1}, \sigma_{2,1,1,-2}$ and $G_{(V_0)} \cong A_4$ (A_n denotes the alternating group of degree n). Hence $G_{(V_0)} \neq G_{\infty,0}$, and $\boldsymbol{D}(7, V_0)$ is a 3-(8, 4, 1) design by Proposition 2.1.

The following theorem is a generalization of Beth [**1**, Corollary 4.4].

THEOREM 3.2. *The design* $\boldsymbol{D}(q, V_0)$ *is a* 3-$(q+1, (q+1)/2, (q+1)(q-3)/8)$ *design. The set of blocks is*

$$V_0^G=\mathfrak{B}_1\dot{\cup}\overline{\mathfrak{B}}_1\dot{\cup}\mathfrak{B}_2\dot{\cup}\overline{\mathfrak{B}}_2,$$

where

$$\mathfrak{B}_1=\{V_i \mid i\in F_q\},$$
$$\overline{\mathfrak{B}}_1=\{\overline{V}_i \mid i\in F_q\},$$
$$\mathfrak{B}_2=\{V_i\triangle V_j\ (=\overline{V}_i\triangle\overline{V}_j) \mid i,\ j\ (\neq)\in F_q\},$$
$$\overline{\mathfrak{B}}_2=\{V_i\triangle\overline{V}_j\ (=\overline{V}_i\triangle V_j=\overline{V_i\triangle V_j}) \mid i,\ j\ (\neq)\in F_q\}.$$

Also, $|\mathfrak{B}_1|=|\overline{\mathfrak{B}}_1|=q$, $|\mathfrak{B}_2|=|\overline{\mathfrak{B}}_2|=\binom{q}{2}$ *and* $|V_0^G|=q(q+1)$.

The same is true of $\boldsymbol{D}(q, U_0)$.

PROOF. By definition, $\boldsymbol{D}(q, V_0)$ is a 3-$(q+1, (q+1)/2, \lambda)$ design, where

$$\lambda=\frac{|G|}{|G_{(V_0)}|}\cdot\binom{(q+1)/2}{3}\bigg/\binom{q+1}{3}.$$

Since $|G_{(V_0)}|=|G_{\infty,0}|=(q-1)/2$ by Proposition 3.1, we have $\lambda=(q+1)(q-3)/8$.

Next, note that $G=G_\infty\dot{\cup}G_\infty\tau G_\infty$, since G is 2-transitive on Ω. By Proposition 2.4 we have $V_0^{G_\infty}=\mathfrak{B}_1$ and $\overline{V}_0^{G_\infty}=\overline{\mathfrak{B}}_1$. Also, by Proposition 2.6

$$\begin{aligned}V_0^{G_\infty\tau}&=\{V_i^\tau \mid i\in F_q\}\\&=\{V_0^\tau\}\cup\{V_i^\tau \mid i\in Q\}\cup\{V_i^\tau \mid i\in N\}\\&=\{\overline{V}_0\}\cup\{V_0\triangle V_{i^\tau} \mid i\in Q\}\cup\{\overline{V}_0\triangle V_{i^\tau} \mid i\in N\}\\&=\{\overline{V}_0\}\cup\{V_0\triangle V_k \mid k\in N\}\cup\{\overline{V}_0\triangle V_k \mid k\in Q\}.\end{aligned}$$

Since G_∞ acts 2-homogeneously on F_q, it follows from Proposition 2.4 that $(V_0\triangle V_k)^{G_\infty}=\mathfrak{B}_2$ for $k\neq 0$ and $V_0^{G_\infty\tau G_\infty}=\overline{\mathfrak{B}}_1\cup\mathfrak{B}_2\cup\overline{\mathfrak{B}}_2$. Consequently

$$V_0^G=\mathfrak{B}_1\cup\overline{\mathfrak{B}}_1\cup\mathfrak{B}_2\cup\overline{\mathfrak{B}}_2. \qquad (*)$$

Obviously $|\mathfrak{B}_1|\leqq q$, $|\overline{\mathfrak{B}}_1|\leqq q$, $|\mathfrak{B}_2|\leqq\binom{q}{2}$ and $|\overline{\mathfrak{B}}_2|\leqq\binom{q}{2}$ and so $|V_0^G|\leqq q+q+\binom{q}{2}+\binom{q}{2}=q(q+1)$. On the other hand, by Proposition 3.1

$$|V_0^G|=|G:G_{(V_0)}|=|G:G_{\infty,0}|=q(q+1),$$

which implies that $|\mathfrak{B}_1|=|\overline{\mathfrak{B}}_1|=q$, $|\mathfrak{B}_2|=|\overline{\mathfrak{B}}_2|=\binom{q}{2}$ and that $(*)$ is a disjoint set union. As in the above, the same may be proved of $\boldsymbol{D}(q, U_0)$. □

REMARK 3.2. Since τ' normalizes G and interchanges V_0 and U_0, it follows that $(V_0^G)^{\tau'}=(V_0^{\tau'})^G=U_0^G$. Thus designs $\boldsymbol{D}(q, V_0)$ and $\boldsymbol{D}(q, U_0)$ are isomorphic.

REMARK 3.3. As is well-known, (F_q, Q^{G_∞}) is a 2-$(q, (q-1)/2, (q-3)/4)$ design. (This is an Hadamard 2-design which is called the Paley design.) In fact, since G_∞ acts 2-homogeneously on F_q and $G_{\infty,(Q)}=G_{\infty,0}$ (as seen in the proof of Proposition 3.1 (i)), it follows from Proposition 2.1 that (F_q, Q^{G_∞}) is a design having the above parameters. Also, by Proposition 2.4 $Q^{G_\infty}=\{Q_i=V_i\setminus\{\infty\} \mid i\in F_q\}$. It is easily seen that $(\Omega, \mathfrak{B}_1\cup\overline{\mathfrak{B}}_1)$ is an extension of (F_q, Q^{G_∞}), i.e., a 3-design such that ($\Omega\setminus\{\infty\}=F_q$ and) $\{B\setminus\{\infty\} \mid \infty\in B\in\mathfrak{B}_1\cup\overline{\mathfrak{B}}_1\}=Q^{G_\infty}$. By Theorem 3.2, it may be said that $\boldsymbol{D}(q, V_0)$ is a further block-extension of $(\Omega, \mathfrak{B}_1\cup\overline{\mathfrak{B}}_1)$. After I proved Theorem 3.2 and later Corollary 3.4, I realized that extremely related facts in a more general form had been proved in Hughes-Piper [7, pp. 137-9].

COROLLARY 3.3. *Let B, C be any distinct blocks of V_0^G (or U_0^G). Then we have*

(i) $|B\triangle C|=4, 8, 12, 16, \cdots, q+1$ *or* $(q+1)/2$;

(ii) $|B\cap C|=0, 2, 4, 6, \cdots, (q+1)/2-2$ *or* $(q+1)/4$;

(iii) *If* $q\not\equiv -1 \pmod 8$, *then*

$$B\triangle C\in V_0^G \text{ (or } U_0^G) \text{ if and only if } |B\triangle C|=(q+1)/2 \text{ if and only if } |B\cap C|=(q+1)/4.$$

PROOF. We refer to V_0^G.

(i) For $i, j, k, l\in F_q$, set

$$A_1 = V_i \text{ or } \overline{V}_i,\quad A_2 = V_j \text{ or } \overline{V}_j,$$
$$A_3 = V_k \text{ or } \overline{V}_k,\quad A_4 = V_l \text{ or } \overline{V}_l.$$

By (*) in the proof of Theorem 3.2, we may write

$$B\triangle C = A_1\triangle\cdots\triangle A_n \quad (n=2, 3 \text{ or } 4).$$

Since $|A_i|=(q+1)/2$ and $|A_i\cap A_j|=(q+1)/4$ $(i\neq j)$ by Corollary 2.7, it follows from Corollary 2.3 (iii) that

$$|B\triangle C| \equiv n(3-n)(q+1)/4 \pmod 4.$$

Hence $|B\triangle C|\equiv 0 \pmod 4$ in the cases $n=3$ and 4. In the case $n=2$, by Corollary 2.7

$$|B\triangle C| = |A_1\triangle A_2| = \begin{cases} (q+1)/2 & \text{if } i\neq j \\ q+1 & \text{if } i=j. \end{cases}$$

(ii) follows immediately from (i).

(iii) Assumption $q\not\equiv -1 \pmod 8$ implies $(q+1)/2\not\equiv 0 \pmod 4$. Therefore the proof of (i) shows that if $|B\triangle C|=(q+1)/2$ then we may write $B=V_i$ or $\bar{V}_i$, $C=V_j$ or $\bar{V}_j$ $(i\neq j)$ and so $B\triangle C\in V_0^G$. □

COROLLARY 3.4. *If $\boldsymbol{D}(q, V_0)$ or $\boldsymbol{D}(q, U_0)$ is a 4-design, then $q=11$.*

PROOF. If $\boldsymbol{D}(q, V_0)$ or $\boldsymbol{D}(q, U_0)$ is a 4-$(q+1, (q+1)/2, \lambda)$ design, then the number of blocks containing given three points is $(q+1)(q-3)/8=\lambda\cdot\binom{q+1-3}{4-3}\Big/\binom{(q+1)/2-3}{4-3}$ and so $\lambda=(q+1)(q-3)(q-5)/16(q-2)$. Since λ must be an integer, it follows that $q-2$ devides $3\cdot 1\cdot 3$ and so $q=11$. □

In reality, we have more strikingly

THEOREM 3.5 (see, e.g. Beth [**1**, Theorem 4.6]). *$\boldsymbol{D}(11, V_0)$ and $\boldsymbol{D}(11, U_0)$ are 5-(12, 6, 1) designs.*

PROOF. The proof is done as in that of Proposition 2.1, and it gives an alternative proof for a part of [**1**, Theorem 4.6]. Set $\mathfrak{B}=V_0^{PSL(2,11)}$, and for a 5-subset T of $\Omega=\{\infty\}\cup F_{11}$ set

$$\lambda(T)=|\{B\in\mathfrak{B} \mid T\subset B\}|.$$

Then $\lambda(T)\leqq 1$ for all T, since otherwise there would exist two distinct blocks $B, C\in\mathfrak{B}$ containing T and so $|B\cap C|\geqq 5$, whereas $|B\cap C|=0, 2, 3$ or 4 by Corollary 3.3, a contradiction. Counting in two ways the number of ordered pairs (T, B) satisfying $T\subset\Omega$, $|T|=5$ and $T\subset B\in\mathfrak{B}$, we have

$$\sum_T \lambda(T)=|\mathfrak{B}|\cdot\binom{6}{5},$$

where the sum in the left-hand side is over all 5-subsets T of Ω. Therefore, noting that the right-hand side is equal to $11\cdot 12\cdot\binom{6}{5}=\binom{12}{5}$ and that $|\Omega|=12$, $\lambda(T)\leqq 1$, we obtain $\lambda(T)=1$ for any 5-subset T of Ω. Thus $\boldsymbol{D}(11, V_0)=(\Omega, \mathfrak{B})$ is a 5-(12, 6, 1) design. □

4. Construction of W_{24}.

NOTATION. For any integer r with $0\leqq r\leqq q+1$, we set

$$\mathfrak{B}_r(q)=\{A\in\mathfrak{B}(q) \mid |A|=r\},$$
$$\mathfrak{U}_r(q)=\{A\in\mathfrak{U}(q) \mid |A|=r\}.$$

Clearly $\mathfrak{B}_0(q)=\mathfrak{U}_0(q)=\{\emptyset\}$ and $\mathfrak{B}_{q+1}(q)=\mathfrak{U}_{q+1}(q)=\{\Omega\}$. From Corollary 2.7 it follows that G acts on $\mathfrak{V}_r(q)$ and $\mathfrak{U}_r(q)$ for any r and that $\mathfrak{V}_{(q+1)/2}(q)\ni V_i$, $\bar{V}_i$, $V_i\triangle V_j$, $\bar{V}_i\triangle V_j$ for any i, j $(\neq)\in F_q$. Corollary 2.10 (i) is restated: If $q\equiv -1$ (mod 24) and $\mathfrak{V}_r(q)$ or $\mathfrak{U}_r(q)\neq\emptyset$ for $1\leqq r\leqq q$, then $r=8, 12, 16, \cdots,$ or $(q+1)-8$.

By Theorem 3.2, every block of $\boldsymbol{D}(q, V_0)$ or $\boldsymbol{D}(q, U_0)$ is an element of $\mathfrak{V}_{(q+1)/2}(q)$ or $\mathfrak{U}_{(q+1)/2}(q)$ and is a combination by symmetric differences of at most two V_i, $\bar{V}_i$ or U_i, $\bar{U}_i$. We next want to consider such a combination of three V_i, $\bar{V}_i$ or U_i, $\bar{U}_i$, which has a minimal cardinality, and in this section we deal with the case $q=23$. As one of elements of $\mathfrak{V}_8(23)$ and $\mathfrak{U}_8(23)$, for example, we take

$$V = V_0\triangle V_1\triangle V_4 = \{\infty, 1, 13, 14, 18, 19, 20, 22\}$$

and

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

respectively. Since the involution $\rho: x\mapsto 4/x$ normalizes $G=\mathrm{PSL}(2, 23)$ and interchanges V and U, it follows that $(V^G)^\rho=(V^\rho)^G=U^G$. Thus designs $\boldsymbol{D}(23, V)$ and $\boldsymbol{D}(23, U)$ are isomorphic. In the following we refer only to $\boldsymbol{D}(23, U)$. In the same way as $\boldsymbol{D}(11, U_0)$ (Theorem 3.5), we obtain

THEOREM 4.1. *Keeping the above notation and* $G=\mathrm{PSL}(2, 23)$, *we have*
(i) $|B\cap C| = 0, 2$ *or* 4 *for any distinct* $B, C\in\mathfrak{U}_8(23)$;
(ii) $|\mathfrak{U}_8(23)| = 759$ $(=33\cdot 23)$, $|G_{(U)}| = 8$ (*so* $G_{(U)}$ *is a Sylow* 2-*subgroup of* G) *and* $U^G=\mathfrak{U}_8(23)$;
(iii) $\boldsymbol{D}(23, U)$ *is a* 5-(24, 8, 1) *design.*

PROOF. (i) follows from Corollary 2.10 (ii).
(ii), (iii) Set $\mathfrak{B}=\mathfrak{U}_8(23)$, and for a 5-subset T of $\Omega=\{\infty\}\cup F_{23}$ set $\lambda(T) = |\{B\in\mathfrak{B} \mid T\subset B\}|$. Then, by (i) we have

$$\lambda(T)\leqq 1 \qquad \text{for all } T. \tag{1}$$

Counting argument yields

$$\sum_T \lambda(T) = |\mathfrak{B}|\cdot\binom{8}{5}, \tag{2}$$

where the sum in the left-hand side is over all 5-subsets T of Ω. Therefore, by (1) we have $\binom{24}{5}\geqq|\mathfrak{B}|\cdot\binom{8}{5}$, namely

$$|\mathfrak{B}|\leqq\binom{24}{5}\Big/\binom{8}{5} = 759. \tag{3}$$

On the other hand, G acts on $\mathfrak{B}$ and so $U^G\subset\mathfrak{B}$,

$$|\mathfrak{B}|\geqq|U^G| = |G|/|G_{(U)}|. \tag{4}$$

Let $G_{\langle U\rangle}^{U}$ be the restriction of $G_{\langle U\rangle}$ on U. Then

$$G_{\langle U\rangle} = G_{\langle U\rangle}/G_U \cong G_{\langle U\rangle}^{U} \quad (\subset S^U\text{: the symmetric group on } U),$$

and so $|G_{\langle U\rangle}|$ is a divisor of 8!. For $a\in U$, $|G_{\langle U\rangle, a}|=|G_{\langle U\rangle}\cap G_a|$ is a common divisor of 8! and $|G_a|=23\cdot 11$, and hence $G_{\langle U\rangle, a}=1$. Therefore

$$|G_{\langle U\rangle}| = |G_{\langle U\rangle} : G_{\langle U\rangle, a}| = |a^{G_{\langle U\rangle}}| \leqq |U| = 8.$$

From this and (4) we have

$$|\mathfrak{B}| \geqq |G|/8 = 759.$$

Comparison with (3) then yields $|\mathfrak{B}|=759$.

Also, since

$$759\cdot 8 = |G| = |U^G|\cdot|G_{\langle U\rangle}|\,; \qquad |U^G| \leqq |\mathfrak{B}| = 759, \quad |G_{\langle U\rangle}| \leqq 8,$$

it follows that

$$|U^G| = |\mathfrak{B}| \text{ (so } U^G=\mathfrak{B}) \quad\text{and}\quad |G_{\langle U\rangle}| = 8.$$

Finally, noting that the right-hand side of (2) is equal to $759\cdot\binom{8}{5}=\binom{24}{5}$, we conclude

$$\lambda(T) = 1 \quad\text{for any 5-subset } T \text{ of } \Omega.$$

Thus $\boldsymbol{D}(23, U)$ is a 5-(24, 8, 1) design. □

REMARK 4.1. Witt systems $\boldsymbol{W}_{24}$ constructed by Carmichael [**3**, p. 432], Todd [**10**], Conway [**4**] and Curtis [**5**] coincide with $\boldsymbol{D}(23, U_0\triangle U_1\triangle U_4)$. In particular, the one by Carmichael is $\boldsymbol{D}(23, \infty^S)$, where $S=\langle\sigma_{1,1,-1,1}, \sigma_{3,1,1,-3}\rangle$, a Sylow 2-subgroup of PSL(2, 23) and

$$\infty^S = \{\infty, 0, 1, 3, 12, 15, 21, 22\} = \overline{U_8\triangle U_{10}\triangle U_{21}} = (U_0\triangle U_1\triangle U_4)^{\tau\sigma_{2,10}}.$$

Also, Witt systems $\boldsymbol{W}_{12}$ constructed by Carmichael [**3**, p. 431] and Beth [**1**] are $\boldsymbol{D}(11, V_0)$, while $\boldsymbol{W}_{12}$ treated in Curtis [**6**] is mainly $\boldsymbol{D}(11, U_0)$.

5. Difference patterns and representative blocks.

As seen in Theorems 3.5 and 4.1, if we take appropriate q and $A\in\mathfrak{U}(q)$ or $\mathfrak{B}(q)$, then $\boldsymbol{D}(q, A)$ becomes the Mathieu-Witt designs $\boldsymbol{W}_{12}$ or $\boldsymbol{W}_{24}$. Thus, in a sense, both designs are unified via symmetric differences of U_i, $\overline{U}_i$ or V_i, $\overline{V}_i$ ($i\in F_q$) and $G=\mathrm{PSL}(2, q)$. In order to grasp better (the blocks of) both designs, we introduce concepts of difference patterns and representative blocks.

Throughout this section we assume that q is a *prime* (until Remark 5.1 we do not assume that $q\equiv -1\,(\mathrm{mod}\,4)$ and $q>7$).

DEFINITION. Among the elements of $\Omega=\{\infty\}\cup F_q$, we define a linear order relation as follows:

$$\infty < 0 < 1 < 2 < \cdots < q-1.$$

Note that this order is changeable by translation (namely, $a<b$ does not necessarily imply $a+c<b+c$ for $c\in F_q$), whereas the order as cycle in F_q is unchanged by translation: If $a_1, a_2, \cdots, a_k$ and c are elements of F_q and $a_1<a_2<\cdots<a_k$, then for some i

$$a_i+c < a_{i+1}+c < \cdots < a_k+c < a_1+c < \cdots < a_{i-1}+c.$$

DEFINITION. Let Ω have an order relation defined above.

(i) For a subset of Ω,

$$A = \{a_1, a_2, a_3, \cdots, a_k\} \quad (a_1<a_2<a_3<\cdots<a_k),$$

we define $\tilde{A}$ — which we call the *difference pattern* or the (*difference*) *cycle* of A — as follows: If $\infty\notin A$,

$$\begin{aligned}\tilde{A} &= (a_2-a_1, a_3-a_2, \cdots, a_k-a_{k-1}, a_1-a_k)\\ &= (a_3-a_2, a_4-a_3, \cdots, a_1-a_k, a_2-a_1)\\ &= \cdots\\ &= (a_1-a_k, a_2-a_1, \cdots, a_{k-1}-a_{k-2}, a_k-a_{k-1}).\end{aligned}$$

If $a_1=\infty$,

$$\begin{aligned}\tilde{A} &= (\infty, a_3-a_2, a_4-a_3, \cdots, a_k-a_{k-1}, a_2-a_k)\\ &= (\infty, a_4-a_3, a_5-a_4, \cdots, a_2-a_k, a_3-a_2)\\ &= \cdots\\ &= (\infty, a_2-a_k, a_3-a_2, \cdots, a_{k-1}-a_{k-2}, a_k-a_{k-1}).\end{aligned}$$

(Clearly $\sum_{x\in\tilde{A}}x=0$ in the former case and $\sum_{x\in\tilde{A}\setminus\{\infty\}}x=0$ in the latter case.) For two expressions of $\tilde{A}$, $(d_1, d_2, \cdots, d_k)=(e_1, e_2, \cdots, e_k)$, we say that the former is *less* than the latter if $d_1=e_1$, $d_2=e_2$, $\cdots$, $d_{i-1}=e_{i-1}$, $d_i<e_i$ for some i. Among the above k (or $k-1$) expressions of $\tilde{A}$, we usually take the least one.

Let $\Omega'\subset\Omega$, $\mathfrak{B}\subset 2^{\Omega'}$ and let $\boldsymbol{D}=(\Omega', \mathfrak{B})$ be a design.

(ii) Set

$$\tilde{\boldsymbol{D}} = \tilde{\mathfrak{B}} = \{\tilde{B} \mid B\in\mathfrak{B}\},$$

which we call the *difference pattern* of $\boldsymbol{D}$ or $\mathfrak{B}$.

(iii) For a difference pattern $d\in\tilde{\mathfrak{B}}$, we set

$$\mathfrak{B}(d) = \{B\in\mathfrak{B} \mid \tilde{B}=d\},$$

whose element is called a block belonging to d. Also, if $(d_1, d_2, \cdots, d_k)$ is the least expression of d, we set

$$B(d)=\begin{cases}\{0, d_1, d_1+d_2, \cdots, d_1+d_2+\cdots+d_{k-1}\} & \text{if } d_1\neq\infty \\ \{\infty, 0, d_2, d_2+d_3, \cdots, d_2+d_3+\cdots+d_{k-1}\} & \text{if } d_1=\infty.\end{cases}$$

Clearly, if $B(d)\in\mathfrak{B}$ then $B(d)\in\mathfrak{B}(d)$, and in this case we call $B(d)$ the *representative block* corresponding to (or belonging to) d.

From definition we have easily

PROPOSITION 5.1. *Let $\Omega'\subset\Omega$, $\mathfrak{B}\subset 2^{\Omega'}$ and let $(\Omega', \mathfrak{B})$ be a design. Then the following hold.*

(i) *For $A, B\in\mathfrak{B}$,*

$$\tilde{A}=\tilde{B} \quad \textit{if and only if} \quad A=B+c \quad \textit{for some } c\in F_q.$$

(ii) $\mathfrak{B}=\dot{\bigcup}_{d\in\tilde{\mathfrak{B}}}\mathfrak{B}(d)$.

(iii) *Suppose that the translation group on F_q*

$$T=\{\sigma_c \mid c\in F_q\}$$

acts on $\mathfrak{B}$, that is, $B+c\in\mathfrak{B}$ for all $B\in\mathfrak{B}$ and all $c\in F_q$. Then, for a difference pattern $d\in\tilde{\mathfrak{B}}$ and for any $B\in\mathfrak{B}(d)$, we have

$$B(d)\in\mathfrak{B}(d) \quad \textit{and} \quad \mathfrak{B}(d)=\{B+c \mid c\in F_q\}.$$

REMARK 5.1. By Proposition 5.1 we see that if the difference pattern $\tilde{\boldsymbol{D}}=\tilde{\mathfrak{B}}$ of a design $\boldsymbol{D}=(\Omega', \mathfrak{B})$ admitting the translation group T on $\mathfrak{B}$ is known, then all the blocks of $\boldsymbol{D}$ can be completely enumerated:

$$\mathfrak{B}=\{B(d)+c \mid d\in\tilde{\mathfrak{B}},\ c\in F_q\}.$$

In particular, for $A\subset\Omega$ with $|A|\geqq 3$, if the difference pattern $\widetilde{\boldsymbol{D}(q, A)}$ is known, then the set of all blocks of $\boldsymbol{D}(q, A)$ is

$$A^G=\{B(d)+c \mid d\in\widetilde{\boldsymbol{D}(q, A)},\ c\in F_q\}.$$

This means that all the blocks of $\boldsymbol{D}(q, A)$ are obtained by translating the representative blocks by all elements of F_q.

In the following, we refer only to designs defined by elements of $\mathfrak{U}(q)$.

PROPOSITION 5.2. *Let $q>7$ be a prime with $q\equiv-1 \pmod 4$. Then*

$$\widetilde{\boldsymbol{D}(q, U_0)}=\{\tilde{U}_0\}\dot{\cup}\{\tilde{\bar{U}}_0\}\dot{\cup}\{\widetilde{U_0\triangle U_i} \mid i\in Q\}\dot{\cup}\{\widetilde{\bar{U}_0\triangle U_i} \mid i\in Q\},$$
$$|\widetilde{\boldsymbol{D}(q, U_0)}|=q+1.$$

All the blocks of $\boldsymbol{D}(q, U_0)$ are obtained by translating U_0, $\bar{U}_0$, $U_0 \triangle U_i$, $\bar{U}_0 \triangle U_i$ $(i \in Q)$ by all $c \in F_q$.

PROOF. As seen in the proof of Theorem 3.2,

$$U_0^{G_\infty} = \{U_i = U_0 + i \mid i \in F_q\},$$
$$\bar{U}_0^{G_\infty} = \{\bar{U}_i = \bar{U}_0 + i \mid i \in F_q\},$$
$$U_0^{G_\infty \tau} = \{\bar{U}_0\} \cup \{U_0 \triangle U_k \mid k \in N\} \cup \{\bar{U}_0 \triangle U_k = \overline{U_0 \triangle U_k} \mid k \in Q\}.$$

By Proposition 2.4 we have for $\sigma_{a,i} \in G_\infty$ $(a \in Q,\ i \in F_q)$

$$(U_0 \triangle U_k)^{\sigma_{a,i}} = a(U_0 \triangle U_k) + i = (U_0 \triangle U_{ak}) + i = (U_0 \triangle U_{-ak}) + (ak + i),$$
$$(\overline{U_0 \triangle U_k})^{\sigma_{a,i}} = (\overline{U_0 \triangle U_{ak}}) + i.$$

Hence the blocks set of $\boldsymbol{D}(q, U_0)$ is

$$\mathfrak{B} = U_0^G = U_0^{G_\infty} \cup U_0^{G_\infty \tau G_\infty} = \{U_0 + i \mid i \in F_q\} \cup \{\bar{U}_0 + i \mid i \in F_q\}$$
$$\cup \{(U_0 \triangle U_j) + i \mid j \in Q,\ i \in F_q\} \cup \{(\overline{U_0 \triangle U_j}) + i \mid j \in Q,\ i \in F_q\}.$$

Consequently we obtain

$$\tilde{\mathfrak{B}} = \{\tilde{U}_0\} \cup \{\tilde{\bar{U}}_0\} \cup \{\widetilde{U_0 \triangle U_j} \mid j \in Q\} \cup \{\widetilde{\overline{U_0 \triangle U_j}} \mid j \in Q\}.$$

In particular,

$$|\tilde{\mathfrak{B}}| \leqq 1 + 1 + (q-1)/2 + (q-1)/2 = q + 1.$$

By Proposition 5.1 (iii), for $d \in \tilde{\mathfrak{B}}$ and $B \in \mathfrak{B}(d)$ we have

$$\mathfrak{B}(d) = \{B + i \mid i \in F_q\}.$$

If $B+i = B+j$ for some distinct $i, j \in F_q$, then $\sigma_{i-j} \in G_{(B)}$. This can not happen, since σ_{i-j} is of order a prime q and $|G_{(B)}| = |G_{\infty 0}| = (q-1)/2$ by Proposition 3.1. Thus $B+i \neq B+j$ for any distinct $i, j \in F_q$ and $|\mathfrak{B}(d)| = q$. Therefore by Proposition 5.1 (ii)

$$|\mathfrak{B}| = |\dot{\bigcup_{d \in \tilde{\mathfrak{B}}}} \mathfrak{B}(d)| = |\tilde{\mathfrak{B}}| \cdot |\mathfrak{B}(d)| = |\tilde{\mathfrak{B}}| q.$$

Noting that $|\mathfrak{B}| = (q+1)q$ (Theorem 3.2) and $|\tilde{\mathfrak{B}}| \leqq q+1$, we conclude $|\tilde{\mathfrak{B}}| = q+1$. The last assertion of the proposition follows Remark 5.1. □

Here we recall that, in general, for a given t-(v, k, λ) design $\boldsymbol{D} = (S, \mathfrak{B})$, the derived design $\boldsymbol{D}_a$ with respect to a point $a \in S$ is the $(t-1)$-$(v-1, k-1, \lambda)$ design $(S_a, \mathfrak{B}_a)$, where $S_a = S \setminus \{a\}$ and $\mathfrak{B}_a = \{B \setminus \{a\} \mid a \in B \in \mathfrak{B}\}$. By definition

$$\tilde{\boldsymbol{D}}_a = \tilde{\mathfrak{B}}_a = \{\widetilde{B \setminus \{a\}} \mid a \in B \in \mathfrak{B}\}.$$

NOTATION. For the remainder of this section we fix

$$\boldsymbol{W}_{12}=\boldsymbol{D}(11, U_0), \quad \boldsymbol{W}_{11}=(\boldsymbol{W}_{12})_\infty ;$$
$$\boldsymbol{W}_{24}=\boldsymbol{D}(23, U_0 \triangle U_1 \triangle U_4), \quad \boldsymbol{W}_{23}=(\boldsymbol{W}_{24})_\infty \text{ and } \boldsymbol{W}_{22}=(\boldsymbol{W}_{23})_0 .$$

The following theorem is a main result of this article.

THEOREM 5.3. *The difference patterns and the representative blocks of the Mathieu-Witt systems, and a way of obtaining all the blocks are summarized in Table 2 at the end of this article.*

PROOF. In the following, we shall determine the difference patterns, from which the corresponding representative and all the blocks are immediately obtained by Proposition 5.1 (iii) and Remark 5.1.

I. The case $\boldsymbol{W}_{12}$: By Proposition 5.2 we need only compute the difference patterns of the following blocks.

$$\begin{aligned}
U_0 &= \{0, 1, 3, 4, 5, 9\}, & \bar{U}_0 &= \{\infty, 2, 6, 7, 8, 10\} ;\\
U_0 \triangle U_1 &= \{0, 2, 3, 6, 9, 10\}, & \overline{U_0 \triangle U_1} &= \{\infty, 1, 4, 5, 7, 8\} ;\\
U_0 \triangle U_3 &= \{0, 5, 6, 7, 8, 9\}, & \overline{U_0 \triangle U_3} &= \{\infty, 1, 2, 3, 4, 10\} ;\\
U_0 \triangle U_4 &= \{0, 1, 2, 3, 7, 8\}, & \overline{U_0 \triangle U_4} &= \{\infty, 4, 5, 6, 9, 10\} ;\\
U_0 \triangle U_5 &= \{0, 1, 4, 6, 8, 10\}, & \overline{U_0 \triangle U_5} &= \{\infty, 2, 3, 5, 7, 9\} ;\\
U_0 \triangle U_9 &= \{0, 2, 4, 5, 7, 10\}, & \overline{U_0 \triangle U_9} &= \{\infty, 1, 3, 6, 8, 9\} .
\end{aligned}$$

Accordingly we have at once $\tilde{U}_0$, $\tilde{\bar{U}}_0$, $\widetilde{U_0 \triangle U_i}$, $\widetilde{\overline{U_0 \triangle U_i}}$ $(i \in Q)$, which turn out Table 2.

II. The case $\boldsymbol{W}_{24}$: Set $G=\mathrm{PSL}(2, 23)$ and $\mathfrak{B}=U^G$ where

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

First we note that

$$\mathfrak{B}=\{aU+b,\ a(U+b)^\tau+c \mid a \in Q ;\ b, c \in F_{23}\}$$

and so that

$$\tilde{\mathfrak{B}}=\{\widetilde{aU},\ \widetilde{a(U+b)^\tau} \mid a \in Q,\ b \in F_{23}\} .$$

In fact, since every element of $U^{G_\infty \tau}$ is written as

$$(aU+b)^\tau=(a(U+b/a))^\tau=1/a \cdot (U+b/a)^\tau=a' \cdot (U+b')^\tau$$

where $a, a' \in Q$ and $b, b' \in F_{23}$, we have

$$\begin{aligned}
\mathfrak{B} &= U^{G_\infty} \cup U^{G_\infty \tau G_\infty}\\
&= \{aU+b \mid a \in Q,\ b \in F_{23}\} \cup \{ca'(U+b')^\tau+d \mid a', c \in Q ;\ b', d \in F_{23}\}\\
&= \{aU+b,\ a(U+b)^\tau+c \mid a \in Q ;\ b, c \in F_{23}\} .
\end{aligned}$$

In the following we compute $\widetilde{aU}$ and $\widetilde{a(U+b)^{\tau}}$ $(a\in Q,\ b\in F_{23})$ for $\mathfrak{B}$. Since

$$Q=\{1,2,3,4,6,8,9,12,13,16,18\} \quad \text{and}$$

$$\tau=(\infty,0)(1,22)(2,11)(3,15)(4,17)(5,9)(6,19)(7,13)(8,20)(10,16)(12,21)(14,18),$$

we have immediately Table 1.

Table 1.

a	aU $\widetilde{aU}$	aU^{τ} $\widetilde{aU^{\tau}}$	$a(U+6)^{\tau}$ $\widetilde{a(U+6)^{\tau}}$
1	{0, 4, 13, 14, 18, 19, 20, 22} (1, 1, 2, 1, 4, 9, 1, 4)	{∞, 1, 6, 7, 8, 14, 17, 18} (∞, 1, 1, 6, 3, 1, 6, 5)	{6, 8, 9, 11, 15, 16, 19, 22} (1, 2, 4, 1, 3, 3, 7, 2)
2	{0, 3, 5, 8, 13, 15, 17, 21} (2, 2, 4, 2, 3, 2, 3, 5)	{∞, 2, 5, 11, 12, 13, 14, 16} (∞, 1, 1, 1, 2, 9, 3, 6)	{7, 9, 12, 15, 16, 18, 21, 22} (1, 2, 3, 1, 8, 2, 3, 3)
3	{0, 8, 11, 12, 14, 16, 19, 20} (1, 2, 2, 3, 1, 3, 8, 3)	{∞, 1, 3, 5, 8, 18, 19, 21} (∞, 1, 2, 3, 2, 2, 3, 10)	{1, 2, 4, 10, 11, 18, 20, 22} (1, 2, 6, 1, 7, 2, 2, 2)
4	{0, 3, 6, 7, 10, 11, 16, 19} (1, 3, 1, 5, 3, 4, 3, 3)	{∞, 1, 3, 4, 5, 9, 10, 22} (∞, 1, 1, 4, 1, 12, 2, 2)	{1, 7, 9, 13, 14, 18, 19, 21} (1, 4, 1, 2, 3, 6, 2, 4)
6	{0, 1, 5, 9, 15, 16, 17, 22} (1, 1, 5, 1, 1, 4, 4, 6)	{∞, 2, 6, 10, 13, 15, 16, 19} (∞, 1, 3, 6, 4, 4, 3, 2)	{2, 4, 8, 13, 17, 20, 21, 22} (1, 1, 3, 2, 4, 5, 4, 3)
8	{0, 6, 9, 12, 14, 15, 20, 22} (1, 5, 2, 1, 6, 3, 3, 2)	{∞, 2, 6, 8, 10, 18, 20, 21} (∞, 1, 4, 4, 2, 2, 8, 2)	{2, 3, 5, 13, 14, 15, 18, 19} (1, 1, 3, 1, 6, 1, 2, 8)
9	{0, 1, 2, 10, 11, 13, 14, 19} (1, 1, 8, 1, 2, 1, 5, 4)	{∞, 1, 3, 8, 9, 11, 15, 17} (∞, 1, 2, 4, 2, 7, 2, 5)	{3, 6, 7, 8, 10, 12, 14, 20} (1, 1, 2, 2, 2, 6, 6, 3)
12	{0, 2, 7, 9, 10, 11, 18, 21} (1, 1, 7, 3, 2, 2, 5, 2)	{∞, 3, 4, 7, 9, 12, 15, 20} (∞, 1, 3, 2, 3, 3, 5, 6)	{3, 4, 8, 11, 16, 17, 19, 21} (1, 2, 2, 5, 1, 4, 3, 5)
13	{0, 4, 6, 7, 8, 10, 17, 21} (1, 1, 2, 7, 4, 2, 4, 2)	{∞, 4, 9, 12, 13, 14, 21, 22} (∞, 1, 1, 7, 1, 5, 5, 3)	{1, 2, 5, 9, 10, 11, 12, 17} (1, 1, 1, 5, 7, 1, 3, 4)
16	{0, 1, 5, 7, 12, 17, 18, 21} (1, 3, 2, 1, 4, 2, 5, 5)	{∞, 4, 12, 13, 16, 17, 19, 20} (∞, 1, 2, 1, 7, 8, 1, 3)	{3, 4, 5, 6, 7, 10, 13, 15} (1, 1, 1, 1, 3, 3, 2, 11)
18	{0, 2, 3, 4, 5, 15, 20, 22} (1, 1, 1, 10, 5, 2, 1, 2)	{∞, 2, 6, 7, 11, 16, 18, 22} (∞, 1, 4, 5, 2, 4, 3, 4)	{1, 5, 6, 12, 14, 16, 17, 20} (1, 3, 4, 4, 1, 6, 2, 2)

Using Table 1, we have readily the following equalities: For any $a\in Q$,

$$\begin{array}{ll}
a(U+1)^{\tau}+7a=6a\cdot U^{\tau}, & a(U+2)^{\tau}+22a=12a\cdot U,\\
a(U+3)^{\tau}+a=2a\cdot U^{\tau}, & a(U+4)^{\tau}+4a=3a\cdot U^{\tau},\\
a(U+5)^{\tau}+21a=12a\cdot U^{\tau}, & a(U+7)^{\tau}+18a=9a(U+6)^{\tau},\\
a(U+8)^{\tau}+22a=3a\cdot U, & a(U+9)^{\tau}+a=8a\cdot U^{\tau},\\
a(U+10)^{\tau}+20a=6a\cdot U^{\tau}, & a(U+11)^{\tau}+19a=2a(U+6)^{\tau},\\
a(U+12)^{\tau}+6a=12a(U+6)^{\tau}, & a(U+13)^{\tau}+21a=8a(U+6)^{\tau},\\
a(U+14)^{\tau}+16a=12a\cdot U, & a(U+15)^{\tau}+13a=(U+6)^{\tau},\\
a(U+16)^{\tau}+11a=4a(U+6)^{\tau}, & a(U+17)^{\tau}+2a=8a\cdot U,\\
a(U+18)^{\tau}+3a=13a\cdot U, & a(U+19)^{\tau}+20a=8a\cdot U^{\tau},\\
a(U+20)^{\tau}+4a=9a(U+6)^{\tau}, & a(U+21)^{\tau}+19a=13a\cdot U,\\
a(U+22)^{\tau}+8a=8a\cdot U. &
\end{array}$$

Consequently we obtain

$$\tilde{\mathfrak{B}}=\{\widetilde{aU},\ \widetilde{aU^{\tau}},\ \widetilde{a(U+6)^{\tau}}\mid a\in Q\},$$

which turns out Table 2. (Incidentally, we have

$$\begin{aligned}
&\{\widetilde{a(U+6)^{\tau}}\mid a\in Q\}=\{\widetilde{a(U+7)^{\tau}}\mid a\in Q\}=\{\widetilde{a(U+11)^{\tau}}\mid a\in Q\}\\
&=\{\widetilde{a(U+12)^{\tau}}\mid a\in Q\}=\{\widetilde{a(U+13)^{\tau}}\mid a\in Q\}=\{\widetilde{a(U+15)^{\tau}}\mid a\in Q\}\\
&=\{\widetilde{a(U+16)^{\tau}}\mid a\in Q\}=\{\widetilde{a(U+20)^{\tau}}\mid a\in Q\}
\end{aligned}$$

and we see that {6, 7, 11, 12, 13, 15, 16, 20} is a block.)

III. The cases $\boldsymbol{W}_{11}$ and $\boldsymbol{W}_{23}$: Eliminating ∞ from the difference pattern (containing ∞) of $\boldsymbol{W}_{12}$ (resp., $\boldsymbol{W}_{24}$), we have at once that of $\boldsymbol{W}_{11}$ (resp., $\boldsymbol{W}_{23}$). which are given in Table 2.

Thus the proof of Theorem 5.3 is complete. □

REMARK 5.2. In the same way as above, we can compute the difference patterns of $\boldsymbol{D}(11, V_0)$ and $\boldsymbol{D}(23, V_0\triangle V_1\triangle V_4)$. As a result, they are obtained by inverting those of $\boldsymbol{D}(11, U_0)$ and $\boldsymbol{D}(23, U_0\triangle U_1\triangle U_4)$:

$(d_1, d_2, \cdots, d_6)\in\widetilde{\boldsymbol{D}(11, V_0)}$ if and only if $(d_6, \cdots, d_2, d_1)\in\widetilde{\boldsymbol{D}(11, U_0)}$;

$(d_1, d_2, \cdots, d_8)\in\widetilde{\boldsymbol{D}(23, V_0\triangle V_1\triangle V_4)}$ if and only if

$$(d_8, \cdots, d_2, d_1)\in\widetilde{\boldsymbol{D}(23, U_0\triangle U_1\triangle U_4)}.$$

REMARK 5.3. Set $G(q)=\mathrm{PSL}(2, q)$, and in the case $q=23$ set $U=U_0\triangle U_1\triangle U_4$, $U'=U^{\tau}\setminus\{\infty\}$, $V=V_0\triangle V_1\triangle V_4$ and $V'=V\setminus\{\infty\}=Q_0\triangle Q_1\triangle Q_4$. Then it is easily checked that $\boldsymbol{D}(23, V)=(\{\infty\}\cup F_{23}, V^{G(23)})\cong\boldsymbol{W}_{24}$ (see Section 4) and $(\boldsymbol{D}(23, V))_{\infty}=(F_{23}, V'^{G(23)_{\infty}})\cong\boldsymbol{W}_{23}=(F_{23}, U'^{G(23)_{\infty}})$ (note that $\widetilde{U'^{G(23)_{\infty}}}=\tilde{\boldsymbol{W}}_{23}$, etc., and see Remark 5.1), whereas $\boldsymbol{D}(11, V_0)=(\{\infty\}\cup F_{11}, V_0^{G(11)})\cong\boldsymbol{W}_{12}$ (see Remark 3.2) and

$(F_{11}, Q_0^{G(11)_\infty}) \not\cong \boldsymbol{W}_{11}$. In particular, note that the design (isomorphic to) $\boldsymbol{W}_{23}$ can be constructed only by F_{23}, $Q_0 \triangle Q_1 \triangle Q_4$ and the (affine) group $G(23)_\infty = \{\sigma_{a,b} \mid a \in Q,\ b \in F_{23}\}$.

Incidentally, we refer to the blocks of $\boldsymbol{W}_{22} = (\boldsymbol{W}_{23})_0$. For each $d = (d_1, d_2, \cdots, d_7)$ (the least expression) $\in \tilde{\boldsymbol{W}}_{23}$, set

$$d_1' = d_1,\ d_2' = d_1 + d_2,\ \cdots,\ d_6' = d_1 + d_2 + \cdots + d_6, \quad \text{and}$$

$$B(d) = \{0, d_1', d_2', \cdots, d_6'\} \ \text{(the representative block of } \boldsymbol{W}_{23} \text{ corresponding to } d).$$

By Remark 5.1 (or Theorem 5.3)

$$\text{the set of blocks of } \boldsymbol{W}_{23} = \{B(d) + i \mid d \in \tilde{\boldsymbol{W}}_{23},\ i \in F_{23}\}.$$

For each $d \in \tilde{\boldsymbol{W}}_{23}$, it is obvious that $0 \in B(d) + i$, $i \in F_{23}$ if and only if $i \in \{0, -d_1', -d_2', \cdots, -d_6'\}$. Therefore, translating $B(d)$ by all elements of F_{23} (resp., by only seven elements $0, -d_1', -d_2', \cdots, -d_6'$) we obtain the blocks of $\boldsymbol{W}_{23}$ (resp., $\boldsymbol{W}_{22}$) belonging to d. Thus all the blocks of $\boldsymbol{W}_{22}$ are immediately obtained from the difference pattern or representative blocks of $\boldsymbol{W}_{23}$:

PROPOSITION 5.4. *The set of blocks of* $\boldsymbol{W}_{22} = \{B(d) \setminus \{0\}, (B(d) - d_1') \setminus \{0\}, (B(d) - d_2') \setminus \{0\}, \cdots, (B(d) - d_6') \setminus \{0\} \mid d = (d_1, d_2, \cdots, d_7) \in \tilde{\boldsymbol{W}}_{23}\}$.

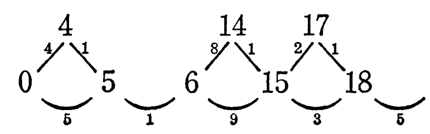
REMARK 5.4. When describing the blocks of $\boldsymbol{W}_{22}$, though the difference pattern of $\boldsymbol{W}_{23}$ is useful as seen above, that of $\boldsymbol{W}_{22}$ itself is useless or meaningless, for $|\tilde{\boldsymbol{W}}_{22}| = 11 \cdot 7 =$ the number of all blocks of $\boldsymbol{W}_{22}$.

The difference patterns or representative blocks have some advantages. One of them is to give a unified and simple way of describing the blocks of all the Mathieu-Witt systems (though somewhat heterogeneous for $\boldsymbol{W}_{22}$), as seen in Table 2.

As another advantage, we take examples from $\boldsymbol{W}_{24}$. (Of course, as for 1 and 2 below, the same may be said of $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$ and $\boldsymbol{W}_{23}$.)

1. *A criterion whether a given* 8*-element set is a block or not*: For a given 8-subset A of $\Omega = \{\infty\} \cup F_{23}$, A is a block of $\boldsymbol{W}_{24}$ if and only if $\tilde{A} \in \tilde{\boldsymbol{W}}_{24}$ (i.e., $\tilde{A}$ is a cycle in Table 2). For instance, $\{\infty, 0, 1, 3, 12, 15, 21, 22\}$ is a block of $\boldsymbol{W}_{24}$. (However, it is not a block of $\boldsymbol{D}(23, V_0 \triangle V_1 \triangle V_4)$.)

2. *Finding the block which contains five given points*: As an example, let $A = \{0, 5, 6, 15, 18\}$ be five given points. From the table of $\tilde{\boldsymbol{W}}_{24}$, looking for a cycle whose appropriate subsum is $\tilde{A} = (5, 1, 9, 3, 5)$, we find the unique cycle $(\underset{5}{1}, 1, \underbrace{8, 1}_{9}, \underbrace{2, 1}_{3}, 5, 4)$. Hence, the desired block is



i.e., $\{0, 4, 5, 6, 14, 15, 17, 18\}$.

Table 2.

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

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

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

The above way is independent of the given five points, whereas the way using the MOG [5, pp. 28-29] is slightly dependent.

3. *A criterion whether a given* 12-*element set is an element of* $\mathfrak{U}_{12}(23)$ *or not*: Let A be a given 12-subset of $\Omega=\{\infty\}\cup F_{23}$. Taking any five points of A, let B be the unique block containing them. Then, it is easily seen that $A\in\mathfrak{U}_{12}(23)$ if and only if $A\triangle B\in\mathfrak{U}_8(23)$ (i.e., $\widetilde{A\triangle B}\in\tilde{\boldsymbol{W}}_{24}$). For instance

$$\{\infty, 0, 1, 3, 6, 8, 11, 12, 14, 17, 20, 22\} \in \mathfrak{U}_{12}(23)$$

and $V_0\notin\mathfrak{U}_{12}(23)$.

REMARK 5.5. Thus the difference pattern of $\boldsymbol{W}_{24}$ has some advantages, but in general it may be less useful than the MOG due to Curtis. For example, when discussing the involutions or the maximal subgroups of the Mathieu group M_{24}, the MOG is very useful, whereas our difference pattern may be useless. But then what is the essence of the MOG or the difference pattern?

References

[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., Lecture Note, **49**, Cambridge Univ. Press, London, 1981, pp. 22-30.
[2] P.J. Cameron, Parallelisms of complete designs, London Math. Soc., Lecture Note, **23**, Cambridge Univ. Press, London, 1976.
[3] R.D. Carmichael, Introduction to the theory of groups of finite order, Ginn, Boston, 1937. (Reprint, Dover, New York, 1956.)
[4] J.H. Conway, Three lectures on exceptional groups, in "Finite simple groups" (G. Higman and M.B. Powell, eds.), Academic Press, London-New York, 1971, pp. 215-247.
[5] R.T. Curtis, A new combinatorial approach to M_{24}, Math. Proc. Cambridge Philos. Soc., **79** (1976), 25-42.
[6] R.T. Curtis, The Steiner system $S(5,6,12)$, the Mathieu group M_{12} and the "Kitten", in "Computational group theory" (M.D. Atkinson ed.), Academic Press, London-New York, 1984, pp. 353-358.
[7] D.R. Hughes and F.C. Piper, Design theory, Cambridge Univ. Press, London, 1985.
[8] B. Huppert, Endliche Gruppen I, Springer, 1967.
[9] R.N. Lane, t-designs and t-ply homogeneous groups, J. Combin. Theory, **10** (1971), 106-118.
[10] J.A. Todd, A representation of the Mathieu group M_{24} as a collineation group, Ann. Mat. Pura. Appl., **71** (1966), 199-238.
[11] T. Tsuzuku, Finite groups and finite geometries, Cambridge Univ. Press, London, 1982.
[12] E. Witt, Die 5-fach transitiven Gruppen von Mathieu, Abh. Math. Sem. Univ. Hamburg, **12** (1938), 256-264.
[13] E. Witt, Über Steinersche Systeme, ibid., 265-275.

Shiro IWASAKI
Department of Mathematics
Hitotsubashi University
Kunitachi, Tokyo 186
Japan