数理解析研究所講究録
1109 巻 1999 年 141-151

Construction of flag-transitive designs with line size 4

Jumela Sarmiento
Graduate School of Mathematics
Kyushu University
Fukuoka, JAPAN

1 Introduction

$\mathcal{D}=(\mathcal{P},\mathcal{B})$ is called a 2-$(v,k,1)$ *design* if $\mathcal{P}$ is a set of v *points* and $\mathcal{B}$ is a collection of subsets of $\mathcal{P}$ (called *blocks*), each of size k, such that every pair of distinct points is contained in exactly one block. A *flag* of $\mathcal{D}$ is an incident point-block pair (x,B), that is, $x\in\mathcal{P}$, $B\in\mathcal{B}$ with $x\in B$.

For a 2-$(v,k,1)$ design $\mathcal{D}$, let ϕ be a permutation on $\mathcal{P}$. If $\mathcal{B}^{\phi}=\{B^{\phi}|B\in\mathcal{B}\}=\mathcal{B}$ then ϕ is called an *automorphism* of $\mathcal{D}$. The group of all automorphisms of $\mathcal{D}$, denoted by $Aut(\mathcal{D})$, is called the *(full) automorphism group* of $\mathcal{D}$.

$\mathcal{D}$ is called a *flag-transitive design* if its automorphism group acts transitively on flags.

There has been a great deal of activity in the study of the pairs $(\mathcal{D},G)$, where $\mathcal{D}$ is a 2-$(v,k,1)$ design and G is a group of automorphisms acting transitively on the flags of $\mathcal{D}$. A classification of the pairs $(\mathcal{D},G)$ was announced in [1] and among the known ones, the case when G is isomorphic to a subgroup of $A\Gamma L(1,v)$ has not been handled completely.

Here, we consider flag-transitive 2-designs whose blocks are of size 4 and whose automorphism group is a subgroup of $A\Gamma L(1,v)$. Specifically, we wish to construct flag-transitive 2-$(2^{2n},4,1)$ designs such that

$$AG^{3}L(1,2^{2n})<Aut(\mathcal{D})<A\Gamma L(1,2^{2n})$$

where $AG^{3}L(1,2^{2n})=\{z\longmapsto a^{3}z+b\mid a,b\in GF(2^{2n}),a\neq 0\}$. We hope to contribute to the complete classification of flag-transitive designs.

		$<\omega>$-orbits on Ω	
n	$\lvert\Omega\rvert$	**# orbits**	**Length**
3	3	1	3
4	8	1	8
5	40	2	5
		3	10
6	147	1	3
		12	12
7	616	6	7
		41	14
8	2408	1	8
		150	16
9	9747	19	9
		532	18
10	38760	2	5
		3	10
		1936	20

Table 1: $<\omega>$-orbits on Ω in $PG(2n-1,2)$

References

[1] F. Buekenhout, A. Delandsheer, J. Doyen, P.B. Kleidman, M.W. Liebeck and J. Saxl, *Linear spaces with flag-transitive automorphism groups*, Geom. Ded. **36** (1990) 89-94.

[2] W. Kantor, 2-*Transitive and flag-transitive designs*, Coding Theory, Design theory, Group Theory (Burlington, VT, 1990), Wiley-Intersci. Publ., New York, 1993.

[3] A. Munemasa, *Flag-transitive* 2-*designs arising from line-spreads in* $PG(2n-1,2)$, to appear in Geom. Dedicata.

2 2-Designs from spreads in $PG(2n-1,2)$

Let $\Sigma = PG(2n-1,2)$, the $(2n-1)$-dimensional projective geometry over $GF(2)$. Points of Σ are the 1-dimensional subspaces of $V(2n,2)$ which can be identified with $V(2n,2)\setminus\{0\}$. Hence, when $GF(2^{2n})$ is regarded as a $2n$-dimensional vector space over $GF(2)$, then we can identify the points of Σ with $GF(2^{2n})^\times$. A line of Σ is a 2-dimensional $GF(2)$-subspace of $GF(2^{2n})$ excluding 0.

Let β be a primitive element of $GF(2^{2n})^\times$. The multiplication by β is a permutation σ on $GF(2^{2n})^\times$, and this is the action of a Singer cycle on the points of Σ. When the Singer group $<\sigma>$ acts on the set of lines of Σ, all but one $<\sigma>$-orbits have length $2^{2n}-1$ and one orbit has length $(2^{2n}-1)/3$. The short orbit actually consists of the cosets $GF(2^{2n})^\times/GF(4)^\times$.

Throughout this paper, let $K = GF(2^{2n})$, $K^\times = <\beta>$, and $H = <\beta^3>$ be the subgroup of index 3 in $K^\times$. An orbit of a line L in $PG(2n-1,2)$ under subgroup of index 3 in the Singer group $<\sigma>$ is a spread if and only if L meets each of the coset of H in $K^\times$ at exactly one point. Using these lines we construct flag-transitive 2-$(2^{2n},4,1)$ designs.

Construction 1

Let L be a line of $PG(2n-1,2)$. We construct an incidence structure $\mathcal{D}_L = (\mathcal{P},\mathcal{B}_L)$ as follows:

$$\begin{aligned} Points: \mathcal{P} &= K \\ Blocks: \mathcal{B}_L &= \{\ a^3(L\cup\{0\})+b \mid a,b\in K, a\neq 0\}. \end{aligned} \tag{1}$$

In other words, the blocks are the images of $L\cup\{0\}$ under the group

$$AG^3L(1,2^{2n}) = \{z \longmapsto a^3z+b \mid a,b\in K, a\neq 0\}.$$

The incidence structure $\mathcal{D}_L$ is a 2-$(2^{2n},4,1)$ design if and only if $L^{<\sigma^3>}$ is a spread. The following theorem, due to Munemasa [3], gives the number of such lines.

Theorem 1 (Munemasa, 1998) *The number of lines in $PG(2n-1,2)$ whose orbit under the subgroup of index 3 in the Singer group is a spread is given by*

$$\frac{1}{27}(2^{2n}-1)(2^n+(-1)^{n+1})^2.$$

3 Isomorphism among designs

From the classification of flag-transitive designs, if a flag-transitive design $\mathcal{D}$ is a 2-$(2^{2n},4,1)$ design not isomorphic to $AG(n,4)$ then $Aut(\mathcal{D})$ is isomorphic to a subgroup of $A\Gamma L(1,2^{2n})$. From a proposition due to Munemasa [3], the design $\mathcal{D}_L$ is isomorphic to the affine space $AG(n,4)$ if and only if $n \not\equiv 0 \pmod 3$ and $L \in K^\times/GF(4)^\times$. Since our objective is to construct flag-transitive 2-$(2^{2n},4,1)$ designs whose automorphism group is a subgroup of $A\Gamma L(1,2^{2n})$, we shall be concerned with all lines satisfying Theorem 1 excluding the cosets $K^\times/GF(4)^\times$. Let $\mathcal{L}$ be the set of all such lines.

If $n \not\equiv 0 \pmod 3$, the number given in Theorem 1 includes the cosets $K^\times/GF(4)^\times$. Hence, the number of lines in $\mathcal{L}$ is given by

$$|\mathcal{L}| = \begin{cases} \frac{1}{27}(2^{2n}-1)(2^n+(-1)^{n+1})^2 & \text{if } n \equiv 0 \pmod 3 \\ \frac{1}{27}(2^{2n}-1)[(2^n+(-1)^{n+1})^2-9] & \text{if } n \not\equiv 0 \pmod 3 \end{cases}$$

By the isomorphism testing method described by Kantor in [2], if $L, L' \in \mathcal{L}$ then the designs $\mathcal{D}_L$ and $\mathcal{D}_{L'}$ are isomorphic if and only if L, L' belong to the same orbit under $\Gamma L(1,2^{2n})$. Therefore, the number of non-isomorphic designs $\mathcal{D}_L$, constructed from a line in $\mathcal{L}$ is equal to the number of $\Gamma L(1,2^{2n})$-orbits in $\mathcal{L}$.

4 $\Gamma L(1,2^{2n})$-orbits

The Frobenius automorphism $\omega : a \longmapsto a^2$ of K acts on the points of Σ under the identification of points with elements of $K^\times$. Let Ω be the set of all $<\sigma>$-orbits in $\mathcal{L}$. Since $\Gamma L(1,2^{2n}) \cong <\sigma> \rtimes <\omega>$, the number of $\Gamma L(1,2^{2n})$-orbits in $\mathcal{L}$ is equal to the number of $<\omega>$-orbits in Ω. From Theorem 1 and the fact that the length of each

$<\sigma>$-orbits in $\mathcal{L}$ is $2^{2n}-1$, the number of elements of Ω is given by

$$|\Omega| = \begin{cases} \frac{1}{27}(2^n + (-1)^{n+1})^2 & \text{if } n \equiv 0 \pmod 3 \\ \frac{1}{27}[(2^n + (-1)^{n+1})^2 - 9] & \text{if } n \not\equiv 0 \pmod 3 \end{cases}$$

Using GAP and MAGMA, we computed the number of $<\omega>$-orbits on Ω and the size of each orbit for $3 \le n \le 10$. The result is given in Table 1. For example, when $n = 5$, the table shows that there are two $<\omega>$-orbits on Ω of length 5 and three of length 10. Thus, there are a total of five $<\omega>$-orbits on Ω giving five nonisomorphic designs constructed from spreads of $PG(9,2)$.

We can easily see that for $\mathcal{O} \in \Omega$, the orbit of $\mathcal{O}$ under $<\omega>$ is of length r if and only if $Stab_{<\omega>}(\mathcal{O}) = <\omega^r>$. This occurs when $\mathcal{O}^{\omega^r} = \mathcal{O}$ but $\mathcal{O}^{\omega^k} \neq \mathcal{O}$ for $k|\ r$. In order to determine such orbits $\mathcal{O}$, we need the following propositions.

Proposition 2 *Let $\mathcal{O} \in \Omega$ and r an odd divisor of n. $\mathcal{O}^{\omega^r} = \mathcal{O}$ if and only if of the three lines in $\mathcal{O}$ containing 1, one line is fixed by ω^r, the other two are interchanged by ω^r and each of these two lines contain a root of*

$$x^{2^r+1} + 1 = 0.$$

Proof:

There exists three $<\sigma^3>$-orbits in $\mathcal{O}$. Since each of these $<\sigma^3>$-orbits is a spread there exists exactly one line containing 1 in each $<\sigma^3>$-orbit. Hence, there are three lines in $\mathcal{O}$ which contain 1.

Suppose $\mathcal{O}^{\omega^r} = \mathcal{O}$. Then for all lines $L \in \mathcal{O}$, $L^{\omega^r} \in \mathcal{O}$. There are two possibilities: $L^{\omega^r} = L$ and $L^{\omega^r} \neq L$. We wish to determine the lines L containing 1, which satisfy each case and we wish to show that $|L^{<\omega^r>}| = 2$ in the latter case.

Let $L = \{1, \alpha, 1+\alpha\} \in \mathcal{O}$, thus $L^{\omega^r} = \{1, \alpha^{2^r}, 1+\alpha^{2^r}\}$.

Case 1. $L^{\omega^r} = L$ if and only if $\alpha^{2^r} = \alpha$ or $\alpha^{2^r} = 1+\alpha$. The first case does not occur since if $\alpha = \beta^l$ then $\alpha^{(2^r-1)} = 1$ implies $2^{2n}-1|\ (2^r-1)l$ and so $2^r+1|\ l$. Since r is odd,

$3|\ 2^r+1$. Consequently, $3|\ l$, contradicting the fact that $\alpha \notin H$. Hence, only the case when α satisfies

$$x^{2^r}+x+1 \;=\; 0 \qquad (2)$$

occurs and $L = \{1, \alpha, \alpha^{2^r}\}$.

The other two lines of $\mathcal{O}$ containing 1: $\alpha^{-1}L$ and $(\alpha+1)^{-1}L$ do not contain an element which satisfies (2). In other words, only one line which contains 1 is left invariant by ω^r.

Case 2. If $L^{\omega^r} \neq L$, then we can choose $\alpha \in L$ such that $L^{\omega^r} = \alpha^{-1}L$. Consequently, $L^{\omega^r} = \alpha^{-1}L = \{1, \alpha^{-1}, 1+\alpha^{-1}\}$, and either $\alpha^{2^r} = \alpha^{-1}$ or $\alpha^{2^r} = 1+\alpha^{-1}$. The first possibility occurs when α satisfies

$$x^{2^r+1}+1 \;=\; 0 \qquad (3)$$

The second possibility can not occur since $\alpha^{2^r} = 1+\alpha^{-1}$ implies $\alpha+1 = \alpha^{2^r+1} \in H$, contradicting the fact that $L \cap H = \{1\}$. Thus, $L^{\omega^r} = \alpha^{-1}L$ if and only if α satisfies (3). Now, $L^{\omega^{2r}} = \{1, \alpha^{-2^r}, 1+\alpha^{-2^r}\}$, but $\alpha^{2^r+1}+1 = 0$ and multiplying both sides by α^{-2^r} gives $\alpha^{-2^r} = \alpha$. Hence, $L^{\omega^{2r}} = L$ and so $|L^{<\omega^r>}| = 2$.

Conversely, suppose $\mathcal{O} = L^{<\sigma>}$ where $L = \{1, \alpha, 1+a\}$ and α satisfies (3). Furthermore, L and $\alpha^{-1}L$ are interchanged by ω^r while $(\alpha+1)^{-1}L$ is left fixed by ω^r. If $L_1 \in \mathcal{O}$, then $L_1 = L^{\sigma^k}$ for some $k < 2^{2n}-1$. Moreover, since $<\sigma> \ \lhd\ \Gamma L(1, 2^{2n})$, ${L_1}^{\omega^r} = L^{\sigma^k\omega^r} = L^{\omega^r\sigma^m} = (\alpha^{-1}L)^{\sigma^m} \in \mathcal{O}$ for some $m < 2^{2n}-1$. Hence, $\mathcal{O}^{\omega^r} \subset \mathcal{O}$. Since $|\mathcal{O}^{\omega^r}| = |\mathcal{O}|$, $\mathcal{O}^{\omega^r} = \mathcal{O}$. □

From Proposition 2, we see that for $\mathcal{O} \in \Omega$, if $|\mathcal{O}^{<\omega>}| = r$ then there exists a line $L = \{1, \alpha, 1+\alpha\} \in \mathcal{O}$ such that α satisfies (3). We wish to determine if the converse is true, that is, if α satisfies (3) then $L = \{1, \alpha, 1+\alpha\} \in \mathcal{L}$. We need to take a closer look at the polynomial $f(x) = x^{2^r+1}+1$.

Since $x^{2^r+1}+1|\ x^{2^{2r}-1}+1$, if $x^{2^r+1}+1 = 0$ then $x \in GF(2^{2r})^\times$.

Now, some solutions to (3) are in H. To see this, we first need to determine the intersection between $GF(2^{2r})^\times$ and H. One can easily check that

$$GCD\left(\frac{2^{2n}-1}{3}, 2^{2r}-1\right) = \begin{cases} (2^{2r}-1) & \text{if } n/r \equiv 0 \pmod 3 \\ \frac{1}{3}(2^{2r}-1) & \text{if } n/r \not\equiv 0 \pmod 3 \end{cases}$$

The intersection between $GF(2^{2r})^\times$ and H is the set of all roots of the following polynomial:

$$GCD(x^{\frac{2^{2n}-1}{3}}+1, x^{2^{2r}-1}+1) = x^g + 1.$$

where $g = GCD(\frac{2^{2n}-1}{3}, 2^{2r}-1)$. Thus, when $n/r \equiv 0 \pmod 3$, $GF(2^{2r})^\times \cap H = GF(2^{2r})^\times$ and so, all solutions to (3) are in H. We have the following proposition.

Proposition 3 *If r is an odd divisor of n such that $n/r \equiv 0 \pmod 3$ then there does not exist an orbit $\mathcal{O} \in \Omega$ such that $|\mathcal{O}^{<\omega>}| = r$.*

Now, assume $n/r \not\equiv 0 \pmod 3$. Then $GF(2^{2r})^\times \cap H = (GF(2^{2r})^\times)^3$ and so, solutions to (3) which are in H must be the roots of

$$f(x) \quad = \quad GCD(x^{2^r+1}+1, x^{\frac{2^{2r}-1}{3}}+1) = x^{\frac{2^r+1}{3}}+1. \tag{4}$$

Next, we consider all solutions to (3) which are in $GF(2^2)^\times$. Since $3|\ 2^r+1$, $x^3+1|\ x^{2^r+1}+1$. But $x^3+1 = (x+1)(x^2+x+1)$ and so solutions to (3), different from 1, which are in $GF(2^2)^\times$ are the roots of $g(x) = x^2+x+1$. Hence, solutions to (3) which are not in $H \cup\ GF(2^2)^\times$ are the roots of

$$h(x) \quad = \quad \frac{x^{2^r+1}+1}{LCM(f(x), g(x))}.$$

For odd integers t, let

$$h_t(x) \quad = \quad \frac{x^{2^t+1}+1}{LCM(x^{\frac{2^t+1}{3}}+1, x^2+x+1)}.$$

and for r an odd divisor of n such that $n/r \not\equiv 0 \pmod 3$, define

$$s_r(x) = LCM(h_{r_1}(x), h_{r_2}(x), \ldots, h_{r_m}(x))$$

where $r_1, r_2, \ldots, r_m$ are proper divisors of r. We have the following proposition.

Proposition 4 *Let r be an odd divisor of n such that $n/r \not\equiv 0 \pmod 3$. Then $\mathcal{O}$ is an orbit in Ω with $|\mathcal{O}^{<\omega>}| = r$ if and only if $\mathcal{O}$ contains a line $L = \{1, \alpha, 1+\alpha\}$ such that α is a root of*

$$H_r(x) \quad = \quad \frac{x^{2^r+1}+1}{LCM(x^{\frac{2^r+1}{3}}+1, x^2+x+1, s_r(x)).} \tag{5}$$

Moreover, in this case, $|L^{<\omega^r>}| = 2$.

Proof:

Suppose $\mathcal{O}$ is an orbit in Ω with $|\mathcal{O}^{<\omega>}| = r$. Then $\mathcal{O}^{\omega^r} = \mathcal{O}$. From Proposition 2, there exists a line $L \in \mathcal{O}$ containing 1 and an element α satisfying

$$x^{2^r+1}+1 = 0.$$

Since $L \in \mathcal{L}$, α is not a root of $LCM(x^{\frac{2^r+1}{3}}+1, x^2+x+1)$. Moreover, $\mathcal{O}^{\omega^t} \neq \mathcal{O}$ for all proper divisors t of r. Thus, α is not a root of $x^{2^t+1}+1 = 0$ and so, α is not a root of $h_t(x)$ for all proper divisors t of r. Therefore, α is not a root of $s_r(x)$. So α is a root of

$$H_r(x) \quad = \quad \frac{x^{2^r+1}+1}{LCM(x^{\frac{2^r+1}{3}}+1, x^2+x+1, s_r(x)).}$$

Conversely, suppose $\mathcal{O}$ is the Singer group orbit containing a line $L = \{1, \alpha, 1+\alpha\}$ such that α is a root of $H_r(x)$ in (5). If $b = \alpha+1$ then $H_r(b+1) = 0$. Thus, $(b+1)^{2^r+1}+1 = 0$ and so $b^{2^r+1}+b^{2^r}+b = 0$. Consequently, $b^{2^r}(b+1+b^{-2^r+1}) = 0$. Since $\alpha \neq 1$, $b \neq 0$ and so, $b+1+b^{-2^r+1} = 0$. Hence, $\alpha = b^{-2^r+1}$.

The roots of $f(x) = x^{\frac{2^r+1}{3}}+1$ are the only roots of $x^{2^r+1}+1$ in H. Since α is not a root of $f(x)$, $\alpha \notin H$. Moreover, $\alpha = b^{-2^r+1}$ so $b = \alpha+1 \notin H$ and since r is odd, $-2^r+1 \equiv 2 \pmod 3$. Thus, α and $\alpha+1$ belong to different cosets of H in $K^\times$. Therefore, $L \in \mathcal{L}$ and $\mathcal{O} \in \Omega$.

Since α satisfies (3), $L^{\omega^r} = \alpha^{-1}L$ and $(\alpha+1)^{-1}L$ is left fixed by ω^r. From Proposition 2, $\mathcal{O}^{\omega^r} = \mathcal{O}$. Suppose $\mathcal{O}^{\omega^k} = \mathcal{O}$ for $k|r$. Then from Proposition 2, α is a root of $x^{2^k+1}+1 = 0$. But this is not possible since $x^{2^k+1}+1$ does not divide $H_r(x)$. Thus, $\mathcal{O}^{\omega^k} \neq \mathcal{O}$ for $k|r$. Consequently, $Stab_{<\omega>}(\mathcal{O}) = <\omega^r>$ which is equivalent to $|\mathcal{O}^{<\omega>}| = r$. □

5 Automorphism group of flag-transitive designs

From a line L in $PG(2n-1,2)$ satisfying Theorem 1 but not one of the cosets $K^\times/GF(4)^\times$, Constructions 1 yields flag-transitive 2-$(2^{2n},4,1)$ designs $\mathcal{D}_L$ whose automorphism group contains $AG^3L(1,2^{2n})$. We will also show in this section that $Aut(\mathcal{D}_L) < A\Gamma L(1,2^{2n})$.

Let r be a divisor of n such that $n/r \not\equiv 0 \pmod 3$ and consider the subgroup $<\omega^r>$ of the Frobenius group $<\omega>$. Define $A\Gamma^{3,r}L(1,2^{2n})$ as follows:

$$\begin{aligned} A\Gamma^{3,r}L(1,2^{2n}) &= \{z \mapsto a^3 z^{\psi^r} + b \mid a,b \in K, a \neq 0, \psi \in Aut(K)\} \\ &= AG^3L(1,2^{2n}) \rtimes <\omega^r> \end{aligned}$$

Theorem 5 *Let* $A = AG^3L(1,2^{2n})$, L *a line in* $PG(2n-1,2)$ *such that* $L^{<\sigma^3>}$ *is a spread,* $L \notin K^\times/GF(4)^\times$. $\mathcal{D}_L = (K,(L\cup\{0\})^A)$ *is a flag-transitive* 2-$(2^{2n},4,1)$ *design whose automorphism group is*

$$Aut(\mathcal{D}_L) \cong T \rtimes Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>}).$$

Proof:

Let $g \in T \cdot Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$, then there exists $\phi \in T$, and $\gamma \in Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$ such that $g = \phi\gamma$. Let B be a block of $\mathcal{D}_L$, that is $B = a^3(L\cup\{0\}) + b$ for some $a \in K^\times$ and $b \in K$. Let $\phi : z \longmapsto z + c$ where $c \in K$, then $B^g = B^{\phi\gamma} = (a^3(L\cup\{0\}) + b + c)^\gamma = (a^3(L\cup\{0\}))^\gamma + (b+c)^\gamma = a'^3(L\cup\{0\}) + d$ for some $a' \in K^\times$ and $d \in K$. Therefore, $B^g \in \mathcal{B}_L$ and since $|\mathcal{B}_L{}^g| = |\mathcal{B}_L|$, $\mathcal{B}_L{}^g = \mathcal{B}_L$. Thus, $g \in Aut(\mathcal{D}_L)$.

Let $g \in Aut(\mathcal{D}_L)$. There exists $h \in T$ such that $0^{hg} = 0$. Moreover, $hg \in Aut(\mathcal{D}_L)$ and $hg \in \Gamma L(1,2^{2n})$. Specifically, $hg \in (Aut(\mathcal{D}_L))_0$, the stabilizer of 0 in $Aut(\mathcal{D}_L)$, which is $Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Therefore, $g = h^{-1}hg$ with $h^{-1} \in T$ and $hg \in Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Thus, $g \in T \cdot Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Therefore, $Aut(\mathcal{D}_L) = T \cdot Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Since $T \lhd Aut(\mathcal{D}_L)$ and $T \cap Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>}) = 1$, $Aut(\mathcal{D}_L) \cong T \rtimes Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. $\square$

Corollary 6 *If the orbit of L under $\Gamma L(1,2^{2n})$ is of length $r(2^{2n}-1)$ then*

$$Aut(\mathcal{D}_L) \cong A\Gamma^{3,r}L(1,2^{2n}).$$

Proof:

If $|L^{\Gamma L(1,2^{2n})}| = r(2^{2n}-1)$ then $Stab_{\Gamma L(1,2^{2n})}(L) \cong <\omega^r>$. We wish to show that $Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>}) = G^3L(1,2^{2n}) \cdot Stab_{\Gamma L(1,2^{2n})}(L)$ where $G^3L(1,2^{2n}) = \{z \longmapsto a^3 z \mid a \in K^\times\}$.

Let $g \in G^3L(1,2^{2n}) \cdot Stab_{\Gamma L(1,2^{2n})}(L)$, that is, there exists $\phi \in G^3L(1,2^{2n})$ and $\delta \in Stab_{\Gamma L(1,2^{2n})}(L)$ such that $g = \phi\delta$. Now, $(L^{<\sigma^3>})^g = (L^{<\sigma^3>})^{\phi\delta} = (L^{<\sigma^3>})^\delta$. However, $\delta \in Stab_{\Gamma L(1,2^{2n})}(L) \cong <\omega^r>$ and so, for any $a^3L \in L^{<\sigma^3>}$, $(a^3L)^\delta = a'^3L \in L^{<\sigma^3>}$ for some $a' \in K^\times$. Thus, $(L^{<\sigma^3>})^\delta = L^{<\sigma^3>}$. Therefore, $g \in Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Hence, $G^3L(1,2^{2n}) \cdot Stab_{\Gamma L(1,2^{2n})}(L) \subset Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$.

Since $|(L^{<\sigma^3>})^{\Gamma L(1,2^{2n})}| = 3r$, we have, $|Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})| = (2^{2n}-1)(2n)/(3r) = |G^3L(1,2^{2n}) \cdot Stab_{\Gamma L(1,2^{2n})}(L)|$. Thus, $Stab_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>}) = G^3L(1,2^{2n}) \cdot Stab_{\Gamma L(1,2^{2n})}(L) \cong G^3L(1,2^{2n}) \rtimes Stab_{\Gamma L(1,2^{2n})}(L) \cong G^3L(1,2^{2n}) \rtimes <\omega^r> \cong \Gamma^{3,r}L(1,2^{2n})$, where $\Gamma^{3,r}L(1,2^{2n}) = \{z \longmapsto a^3 z^\psi \mid a \in K^\times, \psi \in <\omega^r>\}$. This implies that $Aut(\mathcal{D}_L) \cong T \rtimes \Gamma^{3,r}L(1,2^{2n}) \cong A\Gamma^{3,r}L(1,2^{2n})$. □

The last section provides a more explicit construction of a class of flag-transitive 2-$(2^{2n},4,1)$ designs. The construction is as follows:

Construction 2

Let r be an odd divisor of n such that $n/r \not\equiv 0 \pmod 3$. Consider a line L in $PG(2n-1,2)$ containing 1 and a root of $H_r(x)$ as given in Proposition 4. The 2-$(2^{2n},4,1)$ flag-transitive design $\mathcal{D}_L$, as in Construction 1, consists of the following:

$$Points:\ \mathcal{P} \ = \ K$$

$$Blocks:\ \mathcal{B}_L \ = \ (L \cup \{0\})^A$$

where $A = AG^3L(1,2^{2n})$.

The design $\mathcal{D}_L$ obtained from Construction 2 is constructed from a line L whose orbit under $\Gamma L(1, 2^{2n})$ is of length $r(2^{2n} - 1)$. Thus, its automorphism group is given by

$$Aut(\mathcal{D}_L) \cong A\Gamma^{3,r}L(1, 2^{2n}).$$

The number of pairwise nonisomorphic such designs can be obtained using the results of Proposition 4 as follows: let $d = deg(H_r(x))$, where $H_r(x)$ is the polynomial defined in (5). As usual, $\mathcal{L}$ is the set of lines in $PG(2n-1, 2)$ satisfying the conditions of Theorem 1 but not one of the cosets $K^\times/GF(4)^\times$. Then there are d lines in $\mathcal{L}$ which contain 1 and a solution to $H_r(x) = 0$. But if $L = \{1, \alpha, 1+\alpha\}$ such that α is a root of (5) then $\alpha^{-1}L$ is also one of the d lines. Since L and $\alpha^{-1}L$ belong to the same $<\sigma>$-orbit in $\mathcal{L}$, only $d/2$ of these d lines belong to different orbits. Let these lines be $L_1, L_2, \ldots, L_{d/2}$. Then $L_1{}^{<\sigma>}, L_2{}^{<\sigma>}, \ldots, L_{d/2}{}^{<\sigma>}$ are $<\sigma>$-orbits in $\mathcal{L}$ whose orbit under $<\omega>$ is of length r. Therefore, the number of $<\omega>$-orbits in Ω of length r is $d/2r$. This is also the number of $\Gamma L(1, 2^{2n})$-orbits in $\mathcal{L}$ of length $r(2^{2n} - 1)$. This gives $d/2r$ pairwise nonisomorphic such designs $\mathcal{D}_L$ whose automorphism group satisfies

$$Aut(\mathcal{D}_L) \cong A\Gamma^{3,r}L(1, 2^{2n}).$$

We have proved the following proposition.

Proposition 7 *Let r be an odd divisor of n such that $n/r \not\equiv 0 \pmod 3$ and $d = deg(H_r(x))$ where $H_r(x)$ is the polynomial defined in (5) . The number of nonisomorphic flag-transitive* 2-$(2^{2n}, 4, 1)$ *designs (from Construction 1) whose automorphism group is isomorphic to $A\Gamma^{3,r}L(1, 2^{2n})$ is $d/2r$.*

Acknowledgment

The author would like to thank Prof. Akihiro Munemasa for helpful discussions.