<table>
<thead>
<tr>
<th>Title</th>
<th>Construction of flag-transitive designs with line size 4 (Algebraic Combinatorics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Sarmiento, Jumela</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 1999, 1109, 141-151</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1999-08</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/63301">http://hdl.handle.net/2433/63301</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
Construction of flag-transitive designs with line size 4

Jumela Sarmiento
Graduate School of Mathematics
Kyushu University
Fukuoka, JAPAN

1 Introduction

$D=(\mathcal{P},B)$ is called a 2-(v,k,1) design if $\mathcal{P}$ is a set of v points and $B$ 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 $D$ is an incident point-block pair $(x,B)$, that is, $x \in \mathcal{P}$, $B \in B$ with $x \in B$.

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

$D$ 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 $(D,G)$, where $D$ is a 2-(v,k,1) design and $G$ is a group of automorphisms acting transitively on the flags of $D$. A classification of the pairs $(D,G)$ was announced in [1] and among the known ones, the case when $G$ is isomorphic to a subgroup of $AGammaL(1,v)$ 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 $AGammaL(1,v)$. Specifically, we wish to construct flag-transitive 2-$(2^{2n},4,1)$ designs such that

$$AG^3L(1,2^{2n}) < Aut(D) < AGammaL(1,2^{2n})$$

where $AG^3L(1,2^{2n}) = \{ z \mapsto a^3z + b | a,b \in GF(2^{2n}), a \neq 0 \}$. We hope to contribute to the complete classification of flag-transitive designs.
| n  | $|\Omega|$ | $<\omega>$-orbits on $\Omega$ | # 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 $\Omega$ in $PG(2n-1,2)$

References


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 $\Sigma$ 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 $\Sigma$ with $GF(2^{2n})^\times$. A line of $\Sigma$ is a 2-dimensional $GF(2)$-subspace of $GF(2^{2n})$ excluding 0.

Let $\beta$ be a primitive element of $GF(2^{2n})^\times$. The multiplication by $\beta$ is a permutation $\sigma$ on $GF(2^{2n})^\times$, and this is the action of a Singer cycle on the points of $\Sigma$. When the Singer group $\langle \sigma \rangle$ acts on the set of lines of $\Sigma$, all but one $\langle \sigma \rangle$-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 $\langle \sigma \rangle$ 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 $\mathcal{D}_L = (P, B_L)$ as follows:

Points: $P = K$

Blocks: $B_L = \{ a^3(L \cup \{0\}) + b \mid a, b \in K, a \neq 0 \}$.  \(1\)

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

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

The incidence structure $\mathcal{D}_L$ is a 2-$(2^{2n}, 4, 1)$ design if and only if $L^{\langle \sigma^3 \rangle}$ 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 $D$ is a 2-$(2^{2n}, 4, 1)$ design not isomorphic to $AG(n, 4)$ then $Aut(D)$ is isomorphic to a subgroup of $A\Gamma L(1,2^{2n})$. From a proposition due to Munemasa [3], the design $D_L$ is isomorphic to the affine space $AG(n, 4)$ if and only if $n \not\equiv 0 \pmod{3}$ and $L \in K^x/GF(4)^x$. 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 $K^x/GF(4)^x$. Let $L$ be the set of all such lines.

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

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

By the isomorphism testing method described by Kantor in [2], if $L, L' \in L$ then the designs $D_L$ and $D_{L'}$ 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 $D_L$, constructed from a line in $L$ is equal to the number of $\Gamma L(1,2^{2n})$-orbits in $L$.

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

The Frobenius automorphism $\omega : a \mapsto a^2$ of $K$ acts on the points of $\Sigma$ under the identification of points with elements of $K^x$. Let $\Omega$ be the set of all $<\sigma>$-orbits in $L$. Since $\Gamma L(1,2^{2n}) \cong <\sigma> \triangleright <\omega>$, the number of $\Gamma L(1,2^{2n})$-orbits in $L$ is equal to the number of $<\omega>$-orbits in $\Omega$. From Theorem 1 and the fact that the length of each
<σ>-orbits in \( L \) is \( 2^{2n} - 1 \), the number of elements of \( \Omega \) is given by

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

Using GAP and MAGMA, we computed the number of <ω>-orbits on \( \Omega \) and the size of each orbit for \( 3 \leq n \leq 10 \). The result is given in Table 1. For example, when \( n = 5 \), the table shows that there are two <ω>-orbits on \( \Omega \) of length 5 and three of length 10. Thus, there are a total of five <ω>-orbits on \( \Omega \) 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 <ω> is of length \( r \) if and only if \( \text{Stab}_{\Delta <\omega>}(\mathcal{O}) = <\omega^r> \). This occurs when \( \mathcal{O}^{\omega^r} = \mathcal{O} \) but \( \mathcal{O}^{\omega^k} \neq \mathcal{O} \) for \( k \neq r \). 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 \( \omega^r \), the other two are interchanged by \( \omega^r \) and each of these two lines contain a root of

\[
x^{2^r+1} + 1 = 0.
\]

**Proof:**

There exists three <σ³>-orbits in \( \mathcal{O} \). Since each of these <σ³>-orbits is a spread there exists exactly one line containing 1 in each <σ³>-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 \( 2^{2n} - 1 \mid (2^r - 1)l \) and so \( 2^r + 1 \mid l \). Since \( r \) is odd,
$3|2^r+1$. Consequently, $3|l$, contradicting the fact that $\alpha \notin H$. Hence, only the case when $\alpha$ satisfies

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

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 $\omega^r$.

**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 $\alpha$ satisfies

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

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 $\alpha$ 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 $\alpha^{-2^r}$ gives $\alpha^{-2^r} = \alpha$. Hence, $L^{\omega^{2r}} = L$ and so $|L^{\omega^r}| = 2$.

Conversely, suppose $\mathcal{O} = L^{<\sigma>}$ where $L = \{1, \alpha, 1 + \alpha\}$ and $\alpha$ satisfies (3). Furthermore, $L$ and $\alpha^{-1}L$ are interchanged by $\omega^r$ while $(\alpha+1)^{-1}L$ is left fixed by $\omega^r$. If $L_1 \in \mathcal{O}$, then $L_1 = L^{\sigma^k}$ for some $k < 2^{2n} - 1$. Moreover, since $<\sigma> \triangleleft \Gamma L(1,2^{2n})$, $L_1^{\omega^r} = L^{\sigma^k\omega^r} = L^{\omega^r\sigma^m} = (\alpha^{-1}L)^{\sigma^m} \in \mathcal{O}$ 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 $|\mathcal{O}^{<\omega^r>| = r$ then there exists a line $L = \{1, \alpha, 1 + \alpha\} \in \mathcal{O}$ such that $\alpha$ satisfies (3). We wish to determine if the converse is true, that is, if $\alpha$ satisfies (3) then $L = \{1, \alpha, 1 + \alpha\} \in L$. We need to take a closer look at the polynomial $f(x) = x^{2^r+1} + 1$.

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

Now, some solutions to (3) are in $H$. To see this, we first need to determine the
intersection between $GF(2^{2r})^x$ 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 $GF(2^{2r})^x$ 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 $n/r \equiv 0 \pmod{3}$, $GF(2^{2r})^x \cap H = GF(2^{2r})^x$ 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 $O \in \Omega$ such that $|O^{<\omega}>| = r$.

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

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

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

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

For odd integers $t$, let

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

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 \( \Omega \) with \( |\mathcal{O}^{\omega^r}| = r \) if and only if \( \mathcal{O} \) contains a line \( L = \{1, \alpha, 1+\alpha\} \) such that \( \alpha \) is a root of

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

Moreover, in this case, \( |L^{\omega^r}| = 2 \).

Proof:

Suppose \( \mathcal{O} \) is an orbit in \( \Omega \) with \( |\mathcal{O}^{\omega^r}| = r \). Then \( \mathcal{O}^{\omega^r} = \mathcal{O} \). From Proposition 2, there exists a line \( L \in \mathcal{O} \) containing 1 and an element \( \alpha \) satisfying

\[
x^{2^{r}+1} + 1 = 0.
\]

Since \( L \in \mathcal{L} \), \( \alpha \) 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, \( \alpha \) is not a root of \( x^{2^t+1} + 1 = 0 \) and so, \( \alpha \) is not a root of \( h_t(x) \) for all proper divisors \( t \) of \( r \). Therefore, \( \alpha \) is not a root of \( s_r(x) \). So \( \alpha \) is a root of

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

Conversely, suppose \( \mathcal{O} \) is the Singer group orbit containing a line \( L = \{1, \alpha, 1+\alpha\} \) such that \( \alpha \) 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 \( b^{2^r+1} + b^2 + b = 0 \). Consequently, \( b^2 (b+1+b^{-2^r+1}) = 0 \). 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 \( \alpha \) 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, \( \alpha \) and \( \alpha + 1 \) belong to different cosets of \( H \) in \( K^x \). Therefore, \( L \in \mathcal{L} \) and \( \mathcal{O} \in \Omega \).

Since \( \alpha \) satisfies (3), \( L^{\omega^r} = \alpha^{-1}L \) and \( (\alpha+1)^{-1}L \) is left fixed by \( \omega^r \). From Proposition 2, \( \mathcal{O}^{\omega^r} = \mathcal{O} \). Suppose \( \mathcal{O}^{\omega^k} = \mathcal{O} \) for \( k|r \). Then from Proposition 2, \( \alpha \) 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, \( Stab_{\triangleleft \mathit{0}}(\mathcal{O}) = \langle \omega^r \rangle \) which is equivalent to \( |\mathcal{O}^{\omega^r}| = r \). □
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 $K^x/\text{GF}(4)^x$, Constructions 1 yields flag-transitive $2-(2^{2n},4,1)$ designs $D_L$ whose automorphism group contains $AG^3L(1,2^{2n})$. We will also show in this section that $\text{Aut}(D_L) < A\Gamma L(1,2^{2n})$.

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:

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

**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, $L \notin K^x/\text{GF}(4)^x$. $D_L = (K,(L \cup \{0\})^A)$ is a flag-transitive $2-(2^{2n},4,1)$ design whose automorphism group is

$$\text{Aut}(D_L) \cong T \triangleleft \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>}).$$

**Proof:**

Let $g \in T \cdot \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$, then there exists $\phi \in T$, and $\gamma \in \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$ such that $g = \phi \gamma$. Let $B$ be a block of $D_L$, that is $B = a^3(L \cup \{0\}) + b$ for some $a \in K^x$ and $b \in K$. Let $\phi: z \mapsto z + c$ 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 $a' \in K^x$ and $d \in K$. Therefore, $B^g \in B_L$ and since $|B_L^g| = |B_L|$, $B_L^g = B_L$. Thus, $g \in \text{Aut}(D_L)$.

Let $g \in \text{Aut}(D_L)$. There exists $h \in T$ such that $0^{hg} = 0$. Moreover, $hg \in \text{Aut}(D_L)$ and $hg \in \Gamma L(1,2^{2n})$. Specifically, $hg \in (\text{Aut}(D_L))_0$, the stabilizer of 0 in $\text{Aut}(D_L)$, which is $\text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Therefore, $g = h^{-1}hg$ with $h^{-1} \in T$ and $hg \in \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Thus, $g \in T \cdot \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Therefore, $\text{Aut}(D_L) = T \cdot \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$. Since $T \triangleleft \text{Aut}(D_L)$ and $T \cap \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>}) = 1$, $\text{Aut}(D_L) \cong T \triangleleft \text{Stab}_{\Gamma L(1,2^{2n})}(L^{<\sigma^3>})$.
Corollary 6  If the orbit of \( L \) under \( \Gamma L(1, 2^{2n}) \) is of length \( r(2^{2n} - 1) \) then

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

Proof:

If \( |L^{\Gamma L(1, 2^{2n})}| = r(2^{2n} - 1) \) then \( \text{Stab}_{\Gamma L(1, 2^{2n})}(L) \cong \langle \omega^r \rangle \). We wish to show that \( \text{Stab}_{\Gamma L(1, 2^{2n})}(L^{<\sigma^r>}) = G^3 L(1, 2^{2n}) \cdot \text{Stab}_{\Gamma L(1, 2^{2n})}(L) \) where \( G^3 L(1, 2^{2n}) = \{ z \mapsto a^3 z | a \in K^x \} \).

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

Since \( |(L^{<\sigma^r>})^{\Gamma L(1, 2^{2n})}| = 3r \), we have, \( |\text{Stab}_{\Gamma L(1, 2^{2n})}(L^{<\sigma^r>})| = (2^{2n} - 1)(2n)/(3r) = |G^3 L(1, 2^{2n}) \cdot \text{Stab}_{\Gamma L(1, 2^{2n})}(L)|. \) Thus, \( \text{Stab}_{\Gamma L(1, 2^{2n})}(L^{<\sigma^r>}) = G^3 L(1, 2^{2n}) \cdot \text{Stab}_{\Gamma L(1, 2^{2n})}(L) \cong G^3 L(1, 2^{2n}) \cdot \langle \omega^r \rangle \cong G^3 L(1, 2^{2n}) \cdot \langle \omega^r \rangle \cong \Gamma^{3,r} L(1, 2^{2n}) \), where \( \Gamma^{3,r} L(1, 2^{2n}) = \{ z \mapsto a^3 z^\psi | a \in K^x, \psi \in \langle \omega^r \rangle \} \). This implies that \( \text{Aut}(\mathcal{D}_L) \cong T \cdot \Gamma^{3,r} L(1, 2^{2n}) \cong \Gamma^{3,r} L(1, 2^{2n}). \) \( \square \)

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 \( A = AG^3 L(1, 2^{2n}) \).
The design $D_L$ 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

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

The number of pairwise nonisomorphic such designs can be obtained using the results of Proposition 4 as follows: let $d = \text{deg}(H_r(x))$, 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 $K^x/\text{GF}(4)^x$. 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 $\alpha$ is a root of (5) then $\alpha^{-1}L$ is also one of the $d$ lines. Since $L$ and $H_r(x)$ 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 $\Omega$ 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 $D_L$ whose automorphism group satisfies

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

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 $d = \text{deg}(H_r(x))$ 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.