Note

Solvable block transitive automorphism groups of $2-(v,5,1)$ designs

Wenwen Tong*, Huiling Li

Department of Mathematics, Zhejiang University, Hangzhou, Zhejiang 310027, People’s Republic of China

Received 7 December 2000; received in revised form 28 June 2002; accepted 8 July 2002

Abstract

Let $G$ be a solvable block transitive automorphism group of a $2-(v,5,1)$ design and suppose that $G$ is not flag transitive. We will prove that

(1) if $G$ is point imprimitive, then $v=21$, and $G \leq Z_{21}:Z_6$;

(2) if $G$ is point primitive, then $G \leq A_{11}(1,v)$ and $v = p^a$, where $p$ is a prime number with $p \equiv 21 \pmod{40}$, and $a$ an odd integer.

© 2002 Elsevier Science B.V. All rights reserved.

Keywords: Design; Block transitive

1. Introduction

A $2-(v,k,1)$ design $\mathcal{D}$ is a pair consisting of a finite set $\Omega$ of $v$ points and a collection of $k$-subsets of $\Omega$, called blocks, such that any two points lie in a unique block. Every point of $\Omega$ is on exactly $r=(v-1)/(k-1)$ blocks. A flag of $\mathcal{D}$ is a point-block pair, such that the point is on the block. We will always assume that $2 \leq k < v$.

The classification of block transitive $2-(v,3,1)$ designs was completed more than ten years ago [4,6,9,11]. In [3] Camina and Siemons classified $2-(v,4,1)$ designs with a block transitive, solvable group of automorphisms. In [10] we proved that if a

* Supported by National Science Foundation of China and National Science Foundation of Zhejiang Province of China.

* Corresponding author.

E-mail address: tww@math.zju.edu.cn (W. Tong).
block transitive group of automorphisms of a $2-(v,4,1)$ design is unsolvable, then it is flag transitive. Since all flag transitive $2-(v,k,1)$ designs have been determined up to the one-dimensional affine case (see [1]), the classification of block transitive $2-(v,4,1)$ designs is completed. Now we consider $2-(v,5,1)$ designs with a solvable block transitive group of automorphisms. Our main result is as follows.

**Theorem 1.1.** Let $G$ be a solvable block transitive automorphism group of a $2-(v,5,1)$ design. If $G$ is not flag transitive, then one of the following holds:

1. if $G$ is point imprimitive, then $v=21$, and $G \cong Z_{21}:Z_6$;
2. if $G$ is point primitive, then $G \not\cong AGL(1,v)$ and $v = p^a$, where $p$ is a prime number with $p \equiv 21 \pmod{40}$, and $a$ an odd integer.

We do not know any example in case (2). But we conjecture that such $2-(v,5,1)$ design exist if $p$ is big enough.

The second section describes the notation and contains a number of preliminary results. The third section contains the proof of our main theorem.

### 2. Preliminary results

If $\mathcal{D}$ is a $2-(v,5,1)$ design defined on the point set $\Omega$ then $b$ will denote the number of blocks and $r$ will denote the number of blocks through a given point. Let $B$ be a block and $G$ an automorphism group of $\mathcal{D}$. Then $G_B$ will be the block stabilizer and $G_{(B)}$ the pointwise stabilizer of the block $B$. Also $G^B$ will denote the group induced by $G_B$ on the points of $B$, and so $G^B \cong G_B/G_{(B)}$.

We will omit the proofs of all lemmas in this section.

If $X$ is a set we define $X^{(2)} = \{(x,y) \mid x \neq y \in X\}$. The following lemma is quoted from [10].

**Lemma 2.1.** Let $\mathcal{D}$, $G$ be as above. If $\psi_1,\ldots,\psi_t$ are the orbits of $G_B$ on the set $B^{(2)}$ and $\Psi_1,\ldots,\Psi_t$ are the orbits of $G$ on the set $\Omega^{(2)}$, then the map $\sigma$, which maps $\psi_i$ to $\Psi_j$, if $\psi_i \subseteq \Psi_j$, is a bijection between $\{\psi_i \mid i=1,2,\ldots,s\}$ and $\{\Psi_j \mid i=1,2,\ldots,t\}$. In particular $s = t$. Thus the rank of $G$ is $s + 1$ and if $\psi_i^o = \Psi_l$ then $|\Psi_l| = b|\psi_l|$.

The following three lemmas quoted from [3] are very useful in our proof of the theorem.

**Lemma 2.2.** Let $G$ be a block transitive automorphism group of a $2-(v,k,1)$ design. Let $B$ be a block and $T$ be a Sylow 2-subgroup of $G_B$. If $T$ fixes more than one point on $B$ then the number of blocks is odd.

**Lemma 2.3.** Let $G$ be a block transitive automorphism group of a $2-(v,k,1)$ design. Let $B$ be a block and assume that each non-trivial element of $G^B$ fixes at most one point of $B$. Then either $G$ has odd order or $G$ is flag transitive.
Lemma 2.4. Let $G$ be a block transitive automorphism group of a $2-(v,k,1)$ design with $k > 2$. Let $B$ be a block and assume that $G^B$ has order 2. Then the number of blocks is odd and $G^B$ fixes at least two points of $B$.

In the next section we will use the concept of intersection matrices given in [8]. The definition of intersection matrices is as follows.

Let $G$ be a transitive permutation group on a finite set $\Omega$, and $s$ the rank of $G$. This means that if $\omega \in \Omega$ then $\Omega$ decomposes into exactly $s$ $G_\omega$-orbits,

$$\Omega = G_0^\omega(\omega) \cup G_1^\omega(\omega) \cup \cdots \cup G_{s-1}^\omega(\omega), \quad G_0^\omega(\omega) = \{\omega\},$$

where $G_\omega$ denotes the stabilizer of $\omega$. The lengths $l_i = |G_i^\omega|$, $i = 0, 1, \ldots, s - 1$ are called the subdegrees of $G$.

The intersection numbers relative to $G_m^\omega$ are defined by

$$\mu_{ij}^m = |G_m^\omega(\beta) \cap G_i^\omega(\omega)|, \quad \beta \in G_j^\omega(\omega).$$

It is evident that these numbers depend only on $m$, $i$, and $j$, and we see that

$$\sum_i \mu_{ij}^m = l_m, \quad \sum_m \mu_{ij}^m = l_i, \quad \mu_{ij}^m = \mu_{mj}^i,$$

and

$$\mu_{i0}^m = \delta_{im} l_m, \quad \mu_{0i}^m = \delta_{im'}$$

(where $G_m'$ is the suborbit paired with $G_m$). Moreover,

$$l_i \mu_{ij}^m = l_i \mu_{ji}^{m'} \quad \text{and} \quad l_i \mu_{ij}^{(k)} = l_j \mu_{ij}^{(k)} = l_k \mu_{jk}^{(i)}.$$

The $s \times s$ matrix $M_m = (\mu_{ij}^m)_{i,j}$ will be called the intersection matrix of $G_m$. These matrices generate an algebra which is isomorphic to the centralizer algebra. In particular, if $G$ has rank $\leq 5$ then this algebra is commutative (see [12]).

The following lemma will be used when $G$ is imprimitive.

Lemma 2.5 (Delandtsheer and Doyen [5]). Let $G$ be a block transitive automorphism group of a $2-(v,k,\lambda)$ design. If $v > \left[\frac{k}{2}\right] - 1$ then $G$ is point primitive.

It is necessary to introduce another useful definition which is quoted from [7]. A factor $t$ of $q^n - 1$ is called $q$-primitive if $t > 0$ and $(t, q^i - 1) = 1$ for all $i$, $i | n$, $0 < i < n$.

Lemma 2.6 (Hering [7]). $q^n - 1$ has a $q$-primitive factor $t \neq 1$, unless $n = 1$ and $q = 2$; $n = 2$ and $q + 1 = 2^i$ for some $i$, or $n = 6$ and $q = 2$.

Lemma 2.7 (Hering [7]). Let $K$ be the finite field $GF(q)$, where $q = p^n$, $p$ is a prime number. Let $V$ be an $n$-dimensional vector space over the field $K$ and $G = GL(n, q)$. If
Since 3 factor

\[ U \text{ is a solvable subgroup of } G, \text{ and its order is a multiple of the maximal } q\text{ -primitive factor } t \text{ of } q^n - 1, \text{ then } U \text{ is isomorphic to a subgroup of } \Gamma L(1,q^n), \text{ or} \]

\[ n = 2 \quad \text{and} \quad q + 1 = 2^i, \]

\[ n = 2 \quad \text{and} \quad q + 1 = 3 \times 2^i, \]

\[ n = 4 \quad \text{and} \quad q = 3 \text{ or} \]

\[ n = 6 \quad \text{and} \quad q = 2. \]

Let \( X, Y \) be groups. We use the symbol \( X : Y \) to denote the semi-direct product of \( X \) and \( Y \). The other notation and terminology used in this paper are standard in group theory.

**3. Proof of the theorem**

Let \( D, G \) be as above. If \( B \) is a block, then \(|B| = 5\). If \( 5|\nu \), then by Camina–Gagen’s Theorem (see [2]), \( G \) is flag transitive. In the following we suppose that \( G \) is not flag transitive. Then \( 5|\nu - 1 \) (because \( 5|\nu(\nu - 1) \) but \( 5 \) is not a factor of \( \nu \)) and \( 4|\nu - 1 \) (because \( r = (\nu - 1)/4 \)), and so \( \nu \equiv 1 \pmod{20} \). Thus if we let \( b' = (\nu - 1)/20 \), then \( b = vb' \). Now we fix a block \( B \) and suppose \( B = \{1,2,3,4,5\} \).

We divide the proof into four steps.

**Step 1**: The structure of \( G^B \) and the rank and subdegrees of \( G \) can be listed as follows:

<table>
<thead>
<tr>
<th>Type of ( G^B )</th>
<th>Rank of ( G )</th>
<th>Subdegrees</th>
<th>Parity of ( b' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>((1)) \langle 1 \rangle</td>
<td>21</td>
<td>(1, b', \ldots, b')</td>
<td>odd</td>
</tr>
<tr>
<td>((2)) \langle (1,2) \rangle</td>
<td>14</td>
<td>(1, 2b', \ldots, 5b', b', \ldots, b')</td>
<td>odd</td>
</tr>
<tr>
<td>((3)) \langle (1,2,3) \rangle</td>
<td>9</td>
<td>(1, b', b', 3b', \ldots, 3b')</td>
<td>odd</td>
</tr>
<tr>
<td>((4)) \langle (1,2), (3,4) \rangle</td>
<td>9</td>
<td>(1, 4b', 4b', 4b', 4b', 4b', 4b')</td>
<td>?</td>
</tr>
<tr>
<td>((5)) \langle (1,2), (1,2,3) \rangle</td>
<td>8</td>
<td>(1, b', b', b', 3b', 3b', 3b', 3b', 3b', 3b', 6b')</td>
<td>odd</td>
</tr>
<tr>
<td>((6)) \langle (1,2), (3,4,5) \rangle</td>
<td>6</td>
<td>(1, 2b', 3b', 3b', 6b', 6b')</td>
<td>odd</td>
</tr>
<tr>
<td>((7)) \langle (1,2,3), (1,2)(4,5) \rangle</td>
<td>5</td>
<td>(1, b', 6b', 6b', 6b', 6b')</td>
<td>?</td>
</tr>
<tr>
<td>((8)) \langle (1,2,3), (1,2), (4,5) \rangle</td>
<td>5</td>
<td>(1, 2b', 6b', 6b', 6b')</td>
<td>?</td>
</tr>
<tr>
<td>((9)) \langle (1,2,3), (1,3) \rangle</td>
<td>5</td>
<td>(1, 6b', 4b', 4b', 4b')</td>
<td>?</td>
</tr>
<tr>
<td>((10)) (A_4)</td>
<td>4</td>
<td>(1, 4b', 4b', 12b')</td>
<td>?</td>
</tr>
<tr>
<td>((11)) (S_4)</td>
<td>4</td>
<td>(1, 4b', 4b', 12b')</td>
<td>?</td>
</tr>
</tbody>
</table>

**Proof.** Since \( G \) is not flag transitive, \( G^B \) is an intransitive group on \( B \). We can easily list all possible such groups and by Lemma 2.1 we can determine the rank and
subdegrees of \(G\). Note that \(G^B \not\cong \langle (1,2)(3,4) \rangle, \langle (1,2)(3,4), (1,3)(2,4) \rangle \) or \(\langle (1,2,3,4) \rangle\), since in all these cases every nonidentity element of \(G^B\) has just one fixed point and so by Lemma 2.3 \(G\) is of odd order or \(G\) is flag transitive, which conflicts with our hypothesis. In cases (1) and (3), \(G\) is of odd order, so \(b'\) is odd. The oddness of \(b'\) in cases (2), (5) and (6) is implied by Lemma 2.2.

Step 2: The rank of \(G\) is greater than 5, that is, cases (7)–(11) in Step 1 do not occur.

Proof. In cases (7) and (8) \(G\) is of rank 5 and the subdegrees are \(1, 2b', 6b', 6b'\); in case (9) \(G\) is of rank 5 and the subdegrees are \(1, 8b', 4b', 4b', 4b',\) and in cases (10) and (11) \(G\) is of rank 4 and the subdegrees are \(1, 4b', 4b', 12b'\). By checking the orbits of \(G^B\) on the set of ordered pairs of points of \(B\), we know in each of the above cases that \(G\) has two suborbits paired to each other.

Now suppose that \(G\) is of rank 5 and \(A_1, \ldots, A_5\) are the suborbits of \(G\) with \(|A_1| = 1, |A_2| = |A_3| = 6b' ,\) and \(|A_5| = 2b'\), and \(A_2\) and \(A_3\) are paired to each other. Let \(M_2\) and \(M_3\) be the intersection matrices of \(G\) associated with \(A_2\) and \(A_3\), respectively. Then \(M_2\) and \(M_3\) have the following forms:

\[
M_2 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 \\
6b' & x & y & z & 3u \\
0 & p & * & * & * \\
0 & q & * & * & * \\
0 & t & * & * & *
\end{pmatrix}, \quad M_3 = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & x & p & q & 3t \\
6b' & y & * & * & * \\
0 & z & * & * & * \\
0 & u & * & * & *
\end{pmatrix},
\]

where \(p, q, t, u, x, y, z\) are integers. Since the rank of \(G\) is 5, \(M_2 M_3 = M_3 M_2\). Comparing the (2,2) entries of \(M_2 M_3\) and \(M_3 M_2\), we get

\[6b' + x^2 + y^2 + z^2 + 3u^2 = x^2 + p^2 + q^2 + 3t^2.\]

Since the column sums of \(M_2\) and \(M_3\) are all equal to \(6b'\), we get

\[1 + x + y + z + u = x + p + q + t.\]

By reducing modulo 2, we get

\[x^2 + y^2 + z^2 + u^2 \equiv x^2 + p^2 + q^2 + t^2 \pmod{2},\]

\[1 + x + y + z + u \equiv x + p + q + t \pmod{2}.\]

But this system of congruences has no integer solution.

By the same method we can show that the other cases do not occur either.

Step 3: If \(G\) has a regular normal subgroup \(N\) which is elementary abelian, then case (4) in Step 1 does not occur.

Proof. Let \(|N| = p^n\) with \(p\) prime. In this case we may identify the point set \(\Omega\) with the subgroup \(N\), and \(\Omega\) can be regarded as an \(n\)-dimensional vector space over the
field \(GF(p)\). Thus the points of \(\mathcal{D}\) are the vectors of \(\Omega\). The blocks of \(\mathcal{D}\) are sets of vectors, and \(G \leq AGL(n, p)\).

Take \(B = \{0, v_1, v_2, v_3, v_4\}\), where \(0\) is the zero vector, and suppose that \(G^B = \{(v_1, v_2), (v_3, v_4)\}\). If \(v = v_1 + v_2\) then \(G_B\) fixes \(v\). If \(v \neq 0\), then let \(D\) be the block containing \(0\) and \(v\). Thus \(G_B \leq G_{0,v} < G_D\) and \(G_{0,v} \neq G_D\). Since \(|G_B| = |G_D|\), this is a contradiction. Hence \(v_1 + v_2 = 0\). Since \(N \leq \text{Aut} \mathcal{D}\), \(v_1 + B = \{v_1 + v \mid v \in B\}\) is also a block. But \(0\) and \(v_1\) are in \(v_1 + B\), and so \(v_1 + B = B\). Since \(|B| = 5\) and \(0 \in B\), \(B = \langle v_1 \rangle\), a subgroup of \(N\). So \(5 \mid v\), and \(G\) is flag transitive, a contradiction.

**Step 4:** The conclusion of the theorem.

**Proof.** We first suppose that \(G\) is imprimitive on \(\Omega\). Since any subdegree (different from 1) of \(G\) is a multiple of \(b' = (v - 1)/20\), the length of any imprimitivity block is of the form \(1 + xb'\) for some integer \(x\). Thus \(1 + xb' = 1 + 20b'\). From this we only get three possibilities for the values of \(v\) and \(b' : (v, b') = (21, 1), (81, 4)\) and \((361, 18)\).

Suppose \((v, b') = (361, 18)\). Since \(361 > \lceil \frac{2}{3} \rceil^2\), this is impossible by Lemma 2.5.

Suppose \((v, b') = (81, 4)\). Then \(b'\) is even so that case (4) in Step 1 occurs. Therefore \(G\) has rank 9 and subdegrees \(1, 8, 8, 8, 8, 8, 8, 16, 16\). Let \(x \in C_1, C_2, \ldots, C_r\) be a complete set of imprimitivity blocks, where \(x \in \Omega\). Then \(r = 9\) and \(|C_i| = 9\) for \(1 \leq i \leq 9\). So \(C_1 - \{x\}\) is an orbit of \(G_x\) and \(G_{C_1}\) is doubly transitive on \(C_1\). If \(|A_i \cap C_j| \neq 0\), then for all \(x_1 \in A_i \cap C_j\) and \(x_2 \in A_i \cap C_j\), we have \(x_1 = x_2\), for some \(g \in G_x\). So \(|A_i \cap C_j| = |A_i \cap C_i|\), \(C_i = C_j\), and \(|A_i \cap C_j| \mid |A_i|\). Since \(|C_i| = 9\) is odd, there must be an orbit \(A_i\) of \(G_x\) such that \(|A_i \cap C_i|\) is odd. Thus \(|A_i \cap C_i| = 1\) and \(G_{C_1}\) is transitive on \(\{C_1, C_2, \ldots, C_9\}\). The set \(\{x, \beta\mid x \neq \beta, x, \beta \in C_i\) for some \(i, 1 \leq i \leq 9\) has size 324, and \(G\) is transitive on it since \(G_{C_1}\) is doubly transitive on \(C_1\). Hence for any block \(B\) of \(\mathcal{D}\), \(B\) intersects just one \(C_i\) in two points, and intersects the other three imprimitivity blocks in one point each. Now we consider the following subset of the set of block-point pairs:

\[\mathcal{B}_1 = \{(B, \gamma) \mid \gamma \in B, B \text{ is a block, } \gamma \notin C_1, \text{ and } |B \cap C_1| = 2\}.\]

Clearly

\[\mathcal{B}_1 = \mathcal{B}_{12} \cup \mathcal{B}_{13} \cup \cdots \cup \mathcal{B}_{19},\]

where

\[\mathcal{B}_{1j} = \{(B, \gamma) \mid (B, \gamma) \in \mathcal{B}_1, \gamma \in C_j\}, \quad j = 2, 3, \ldots, 9.\]

Since \(G_{C_1}\) is transitive on \(\mathcal{B}_1\), we have \(|\mathcal{B}_1| = 36 \times 3 = 108\). Since \(G_{C_1}\) is transitive on \(\{C_2, C_3, \ldots, C_9\}\), we have \(|\mathcal{B}_{1j}| = |\mathcal{B}_{11}|\). This leads to \(108 \equiv 0 \pmod{8}\), a contradiction. Thus \(v = 81\) is impossible.

Hence the only possibility is \((v, b') = (21, 1)\). In this case \(\mathcal{D}\) is the unique projective plane of order 4, and \(G \leq P\Gamma L(3, 4)\) is solvable. It is not hard to conclude that \(G \leq \mathbb{Z}_{21} : \mathbb{Z}_6\).

Finally we suppose that \(G\) is primitive on \(\Omega\). Then \(G\) has an elementary abelian regular normal subgroup \(N\), and \(v = p^a\) for some prime number \(p\) and an integer \(a\).
We identify $\Omega$ with $N$ and regard $\Omega$ as an $a$-dimensional vector space over $GF(p)$. If $0$ denotes the zero vector of $\Omega$, then $G_0 \leq GL(a, p)$. By Steps 2 and 3, $b' = (v - 1)/20$ is odd, so $p^a - 1 \equiv 4 \pmod{8}$, and so $a$ is odd. This implies that if $a > 1$, then the prime number 5 is not a $p$-primitive prime factor of $p^a - 1$. Hence the maximal $p$-primitive factor $t$ of $p^a - 1$ divides $b' = (p^a - 1)/20$, and so also divides the order of $G_0$. Thus by Lemma 2.7, $G_0 \leq \Gamma L(1, p^a)$ and so $G \leq \Gamma L(1, p^a)$. Since if $a > 1$ is odd, then $(p^a - 1)/(p - 1)$ is odd, $p \equiv 1 \pmod{20}$, and by the oddness of $b'$, we know that $(p - 1)/20$ is odd. So we have $p \equiv 21 \pmod{40}$.

Thus the proof of the theorem is complete.

References