JOURNAL OF COMBINATORIAL THEORY, Series A 38, 192-202 (1985)

Steiner Triple Systems with a Doubly Transitive Automorphism Group*

MARSHALL HALL, JR.

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Communicated by the Managing Editors

April 11, 1983

1. INTRODUCTION

In 1960 the author [5] made the conjecture that a Steiner Triple System S(v) with a doubly transitive automorphism group G is necessarily either an affine space over GF(3) or a projective space over GF(2). The truth of this conjecture is established in this paper.¹

W. G. Burnside [1] showed that a doubly transitive permutation group has a transitive normal subgroup which is either an elementary Abelian *p*-group, or a non-Abelian simple group. In his 1972 M.Sc. dissertation at Oxford J. I. Hall [4] showed that in the first case S(v) is an affine space over GF(3), and this result is given in Section 3. In the second case it is shown in Section 4 that S(v) is the projective space over GF(2). This proof depends on the classification of the finite simple groups and a listing of doubly transitive groups by Peter Cameron [2]. G is in almost every case the group PSL(d, 2). The only exception is the doubly transitive representation of A_7 on 15 points.

2. STRUCTURE OF DOUBLY TRANSITIVE PERMUTATION GROUPS

Burnside [1, p. 202] has shown the following:

THEOREM 2.1. If G is a finite doubly transitive group on v points, then either (i) G contains a transitive normal subgroup A of order $p^r = v$, and A is elementary Abelian, or (ii) G contains a normal subgroup H where H is transitive and H is simple-non Abelian.

 \ast This research was supported in part by the National Science Foundation under Grant MCS 82-17596.

¹ It has been reported to me that a similar result has been found independently by William Kantor and also by Ernest Shult. But this paper is my proof of my conjecture.

For Steiner triple systems S with a doubly transitive automorphism group G we shall show in the first case that S(v) is the affine geometry AG(r, 3) and $v = 3^r$ and in the second case that S(v) is the projective geometry PG(s, 2) and $v = 2^{s+1} - 1$. The proof of the first case is due to J. I. Hall in his 1972 Oxford dissertation for the Master of Science degree. As this has not been published elsewhere, the proof will be given in Section 3. In the second case in Section 4 we have $H \subseteq G \subseteq Aut(H)$ and the classification of the finite simple groups will be used.

3. G HAS A NORMAL ELEMENTARY ABELIAN SUBGROUP

In this section we shall assume that the Steiner triple system S(v) has a group of automorphisms G doubly transitive on the v points of S(v) and that G has an elementary Abelian subgroup A of order p' = v, transitive and regular on the v points.

THEOREM 3.1. Let S(v) be a Steiner triple system with a group of automorphisms G which is doubly transitive on the points of S(v) and suppose that G has a regular normal subgroup A which is elementary Abelian of order $p^r = v$. Then S is the affine geometry AG(r, 3), p = 3 and A is the translation group of this geometry.

The proof of this theorem will depend on some preliminary results. In a Steiner system a triangle is a set of three points which are not in a triple.

THEOREM 3.2. Let S be a Steiner triple system in which for every point x there is an involution α_x of S which has x as its only fixed point. Then every triangle of S generates an S(9). Conversely suppose that S is a Steiner triple system in which every triangle generates an S(9). Then for every point x of S there is an involution α_x of S which has x as its only fixed point. Also if $x \neq y$ $(\alpha_x \alpha_y)^3 = 1$.

Proof. Suppose for each point x of S there is an involution α_x which has x for its only fixed point. If an involution interchanges points a and b and if abc is a triple then clearly the involution fixes c. Hence the involution α_x interchanges y and z if and only if xyz is a triple. Thus α_x is completely determined by the point x and the triples containing x. Let 1, 2, 4 be a triangle of S. Then the following triples are determined:

Then we have involutions α_1, α_2 with

$$a_1 = (1)(2, 3)(4, 5)(6, 7),$$

$$a_2 = (2)(1, 3)(4, 6).$$
(3.2)

Applying a_1 to 2, 4, 6 we have (2, 4, 6) $a_1 = 3$, 5, 7, a new triple. Thus 2, 5, 7 is not a triple and there must be a triple 2, 5, 8. Let 9 be the third point of the triple 1, 8, 9. We now have triples

and also involutions

$$a_{1} = (1)(2, 3)(4, 5)(6, 7)(8, 9),$$

$$a_{2} = (2)(1, 3)(4, 6)(5, 8),$$

$$a_{3} = (3)(1, 2)(5, 7),$$

$$a_{4} = (4)(1, 5)(2, 6),$$

$$a_{5} = (5)(1, 4)(2, 8)(3, 7).$$

(3.4)

We now find further triples by applying the involutions

$$(2, 5, 8) a_1 = 3, 4, 9,$$

$$(1, 2, 3) a_5 = 4, 8, 7,$$

$$(4, 8, 7) a_1 = 5, 6, 9.$$

(3.5)

This adds to our information giving triples

194

and involutions

$$a_{1} = (1)(2, 3)(4, 5)(6, 7)(8, 9),$$

$$a_{2} = (2)(1, 3)(4, 6)(5, 8),$$

$$a_{3} = (3)(1, 2)(4, 9)(5, 7),$$

$$a_{4} = (4)(1, 5)(2, 6)(3, 9)(7, 8),$$

$$a_{5} = (5)(1, 4)(2, 8)(3, 7)(6, 9).$$

(3.7)

We now find

$$(1, 4, 5) a_3 = 2, 9, 7, (2, 9, 7) a_1 = 3, 8, 6.$$
(3.8)

This yields the triples of a complete S(9)

1, 2, 3	2, 4, 6	3, 4, 9	4, 7, 8	5, 6, 9	
1, 4, 5	2, 5, 8	3, 5, 7			(2.0)
1, 6, 7	2, 7, 9	3, 6, 8			(3.9)
1, 8, 9					

$$a_{1} = (1)(2, 3)(4, 5)(6, 7)(8, 9),$$

$$a_{2} = (2)(1, 3)(4, 6)(5, 8)(7, 9),$$

$$a_{3} = (3)(1, 2)(4, 9)(5, 7)(6, 8),$$

$$a_{4} = (4)(1, 5)(2, 6)(\overline{3}, 9)(7, 8),$$

$$a_{5} = (5)(1, 4)(2, 8)(3, 7)(6, 9),$$

$$a_{6} = (6)(1, 7)(2, 4)(3, 8)(5, 9),$$

$$a_{7} = (7)(1, 6)(2, 9)(3, 5)(4, 8),$$

$$a_{8} = (8)(1, 9)(2, 5)(3, 6)(4, 7),$$

$$a_{9} = (9)(1, 8)(2, 7)(3, 4)(5, 6).$$
(3.10)

This completes the proof of the first part of the theorem since we have shown that given the involutions, the triangle 1, 2, 4 generates the S(9) of (3.9).

For the converse part of the theorem suppose that S is a Steiner triple system in which every triangle generates an S(9). Let 1 be a point of S and let a_1 be the permutation which fixes 1 and interchanges x and y if 1, x, y is

a triple. We must prove that a_1 is an automorphism of S, namely, that a_1 maps triples of S onto triples of S. This is trivial for every triple through 1. Hence consider a triple, say, 2, 4, 6, not through 1. Let 3, 5, 7 be the third points of the triples containing 1, 2; 1, 4; 1, 6, respectively.

Thus we have

By hypothesis the triangle 1, 2, 4 generates an S(9) whose points are 1,..., 7 as above and two further points 8, 9. Thus 1, 8, 9 is a triple. If 2, 5, 7 were a triple then we would have to have 2, 8, 9 as a triple and 8, 9 would appear in two triples, a conflict. Thus 2, 5 is in a triple with one of 8, 9, say, 8. The remaining triple with 2 must be 2, 7, 9. This gives triples

We easily find that the only possible way to complete (3.12) to an S(9) is to add the further triples which appear in (3.9). Thus with $a_1 = (1)(2, 3)(4, 5)(6, 7)(8, 9)$ we find $(2, 4, 6) a_1 = 3, 5, 7$ and 3, 5, 7 is indeed a triple of S. This proves that a_1 is an automorphism of S and the proof of our theorem is complete.

Finally, suppose that $x \neq y$, and that x, y, z is a triple. Then

$$\alpha_x \alpha_y \alpha_x = \alpha_z$$
 and $\alpha_y \alpha_x \alpha_y = \alpha_z$ (3.13)

giving

$$(\alpha_x \alpha_y)^3 = \alpha_z^2 = 1.$$
 (3.14)

THEOREM 3.3. Suppose that S(v) has a sharply doubly transitive automorphism group G of order v(v-1) so that in G only the identity fixes as many as two points. Then S(v) is an affine AG(r, 3), and the translation group A of AG(r, 3) is a regular normal subgroup of G of order $3^r = v$.

Proof. Here G is a Frobenius group and it is well known that the identity and the v-1 elements of G displacing all points form a transitive regular normal elementary Abelian subgroup A of order $p^r = v$ for some prime p. Since v-1 is even G contains an involution α_x fixing a single

196

point. Since A is transitive and regular the conjugates of α_x under A give for every point w of S an involution α_w which has w as its only fixed point. Thus the hypothesis of Theorem 3.2 holds. If $x \neq y$ we have $(\alpha_x \alpha_y)^3 = 1$. We cannot have $\alpha_x \alpha_y = 1$ as $\alpha_x \neq \alpha_y$. Hence $\alpha_x \alpha_y$ is an element of order 3. Clearly $\alpha_x \alpha_y$ does not fix x or y. If $\alpha_x \alpha_y$ fixed $r \neq x, y$ then

$$\alpha_x = \cdots (rs) \cdots, \qquad \alpha_v = \cdots (sr) \cdots$$

and $\alpha_x \alpha_y$ would fix both r and s which is impossible in G. Hence $\alpha_x \alpha_y$ fixes no point and so is an element of the transitive regular normal Abelian subgroup A of order p^r. Thus p = 3 and $|A| = 3^r = v$.

Now suppose that 1, 2, 3 is a triple of S. Then $a_1 = (1)(2, 3) \cdots$ and $a_2 = (2)(1, 3) \cdots$ so that $a_1 a_2 = (1, 3, 2) \cdots = a \in A$ and (1, 3, 2) is a cycle of $a \in A$. Clearly (1, 2, 3) is a cycle of $a^{-1} \in A$. In general if x, y, z is a triple of S then (x, y, z) is a cycle of some $a \in A$ and (x, z, y) is a cycle of $a^{-1} \in A$. Each of the v - 1 nonidentity elements of A contains v/3 three cycles. Hence together they contain v(v-1)/3 three cycles and for each of the (v-1)/6 triples of S there are two 3 cycles. This accounts for all 3 cycles in A so that every 3 cycle appearing in an element of A comes from a triple of S(v). Since A is elementary Abelian, A is a translation group for S(v) which must then be the affine geometry AG(r, 3).

THEOREM 3.4. Let S(v) be a Steiner triple system on points 1, 2,..., v and let G be a doubly transitive group of automorphisms of S(v). Let $H = G_{1,2}$, and let F(H) be the fixed points of H. Then the action of $N_G(H)$ on F(H) is a sharply doubly transitive group on F(H).

Proof. Let |F(H)| = m and without loss of generality suppose $F(H) = \{1, 2, ..., m\}$. Then if $r, s \in F(H)$ we will have $G_{r,s} \supseteq G_{1,2}$. But as G is doubly transitive we have $|G_{r,s}| = |G_{1,2}|$ so that $G_{r,s} = G_{1,2}$. Hence if $x \in G$ $x = \binom{1,2...}{r_{s,...}}$ then $x^{-1}G_{1,2}x = G_{r,s} = G_{1,2} = H$ and $x^{-1}Hx = H$. Thus $N_G(H)$ is doubly transitive in its action on F(H). If $y = \binom{1,2...}{1,2...} \in N_G(H)$ and if y moved some point $r \in F(H)$ then as $y \in G_{1,2}r$ would not be in F(H). Hence in $N_G(H)$ no element except the identity fixes as many as 2 points of F(H). This proves our theorem.

We are now in a position to prove our Main Theorem 3.1. Here S(v) is a Steiner triple system on v points and its doubly transitive automorphism group G contains a transitive regular normal Abelian subgroup A of order $p^r = v$ for some prime p.

Let $H = G_{1,2}$. Then from Theorem 3.4 $N_G(H)$ is a sharply doubly transitive group on F(H). If |F(H)| = m the order of $N_G(H)$ on F(H) is m(m-1). Now F(H) is a Steiner triple system on m points and by Theorem 3.3, F(H) is an affine (3, s) space with $3^s = m$ (possibly s = 1 and m = 3). If 1, 2, 3 is a triple then $3 \in F(H)$. Let $a = (\dots, 1, 2, \dots)$ be the unique element of A taking 1 into 2. Then for $h \in H = G_{1,2} h^{-1}ah = (..., 1, 2, ...) \in A$ and so $h^{-1}ah = a$. Hence H centralizes a and so F(H) is a union of orbits of a. Since $a^p = 1$ it follows that p divides $|F(h)| = m = 3^s$. Thus p = 3, and A is of order $3^r = v$.

Now a = (1, 2, t),... As $h^{-1}ah = a$ for $h \in H$ it follows that $t \in F(H)$, and by Theorem 3.3 that (1, 2, t) is a triple of F(H), since $a \in N_G(H)$. Hence (1, 2, t) = (1, 2, 3). Now $a^{-1} = (1, 3, 2),...$ Since G is doubly transitive there will be an element $g \in G$ such that $g^{-1}(1, 2, 3) g = (x, y, z)$ if x, y, z is an arbitrary triple of S. As A is normal in G there will be a $b \in A$ with b = ... (x, y, z) Hence every triple of S(x, y, z) gives two 3-cycles in A, namely, (x, y, z) and (x, z, y). As before each of the v - 1 nonidentity elements of A contains v/3 cycles. Hence in all there are v(v-1)/3 3-cycles in A and these consist precisely of two 3 cycles for each of the v(v-1)/6triples in S(v). Thus every 3-cycle in A corresponds to a triple of S(v) and as A is elementary Abelian, it is the translation group of the necessarily affine triple system S(v) = AG(r, 3). This completes the proof of Theorem 3.1.

4. G HAS A SIMPLE NON-ABELIAN NORMAL SUBGROUP

Peter Cameron [2] has given a list of the doubly transitive groups containing a minimal normal subgroup T which is simple non-Abelian. In his list n is the degree of the doubly transitive group and k is the maximal degree of transitivity of a group with socle T. Here is his list.

Т	n	k	Remarks
$A_n, n \ge 5$	n	n	Two representations if $n = 6$
$PSL(d, q), d \ge 2$	$(q^d - 1)/(q - 1)$		$(d, q) \neq (2, 2), (2, 3)$ Two representations
PSU(3,q)	$q^{3} + 1$	2	if d > 2 q > 2
$^{2}B_{2}(q)$ (Suzuki)	$q^2 + 1$		$q = 2^{2 \cdot a + 1} > 2$
${}^{2}G_{2}(q)$ (Ree)	$q^{3} + 1$		$q = 3^{2a+1} > 3$
PSp(2d, 2)	$2^{2d-1} + 2^{d-1}$	2	d > 2
PSp(2d, 2)	$2^{2d-1} - 2^{d-1}$	2	d > 2
PSL(2, 11)	11	2	Two representations
PSL(2, 8)	28	2	
A_7	15	2	Two representations
M_{11} (Mathieu)	11	4	-

M_{11} (Mathieu)	12	3		
M_{12} (Mathieu)	12	5	Two representations	
M_{22} (Mathieu)	22	3		
M_{23} (Mathieu)	23	4		
M_{24} (Mathieu)	24	5		
Higman Sims	176	2	Two representations	
CO_3 (Conway)	276	2		(4.1)

If G is one of these groups and is the automorphism group of a Steiner triple system S(n), then we must have $n \equiv 1$ or 3 (mod 6) and $G_{1,2}$ must fix a third point, namely, the third point of a triple 1, 2, x.

Hence for A_n on *n* points we have $n \ge 7$ but this group is triply transitive and $G_{1,2}$ does not fix a third point.

For PSL(d, q) if q = 2, $n = 2^d - 1$ and this is the projective space PG(d-1, 2) which is a Steiner triple system. This is the projective case of the conjecture. If q > 2, then without loss of generality we may suppose the representation to be on the points of PG(d, q). The group will have a subgroup fixing a line of q + 1 points and so these must form a Steiner system with $q = 2^{2t+1}$. But the subgroup taking the line into itself is triply transitive on the q + 1 > 3 points which is impossible since the subgroup fixing two points must fix a third point. This disposes of the groups PSL(d, q).

For PSU(3, q), $n = q^3 + 1$ so that if we have $n \equiv 1$ or 3 (mod 6) necessarily q is an odd power of 2, $q = 2^{2a+1} > 2$. This case will be discussed later.

For ${}^{2}B_{2}(q)$ the Suzuki groups of degree $n = q^{2} + 1$ with $q = 2^{2a+1} > 2$ we have $n \equiv 2 \pmod{3}$ which is impossible. For ${}^{2}G_{2}(q)$ with $n = q^{3} + 1$ and $q = 3^{2a+1} > 3$, n is even which is impossible.

Of the remaining cases the only one for which the degree *n* is congruent to 1 or 3 mod 6 is the representation of A_7 on 15 points.

The array (the plane of order 2)

by $\alpha = (1, 2, 3, 4, 5, 6, 7)$ and $\beta = (3, 4, 5, 6, 7)$ which generate A_7 we get for the 15 arrays appropriately numbered

$$\alpha = (1)(2, 4, 10, 3, 6, 11, 8)(5, 9, 13, 7, 15, 14, 12), \beta = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15).$$

$$(4.3)$$

The involution $\tau = (3, 5)(6, 7)$ has the representation

$$\tau = (1)(6)(14)(2,5)(3,4)(7,10)(8,9)(11,12)(13,15).$$
(4.4)

Hence if $G = \langle \alpha, \beta \rangle$ on the 15 points 1,..., 15 is the automorphism group of an S(15) then 1, 6, 14 must be one of the triples. Under the action of G this leads to 35 triples which are the projective geometry PG(3, 2). The second representation comes from this, the first, by an outer automorphism of A_7 in S_7 and is essentially the same as this.

Now let us consider the group PSU(3, q) of order $(q^3 + 1) q^3(q^2 - 1)$ with $n = q^3 + 1$ points with q an odd power of 2, q > 2. G as a permutation group is necessarily the identical representation and an irreducible representation of degree q^3 . This is the "Steinberg character" and is unique. Hence G is the representation of PSU(3, q) on the $q^3 + 1$ isotropic points.

PSU(3, q) is given by 3 by 3 matrices X over F_{q^2} in terms of the involutory automorphism of F_{q^2} , $x \to x^q = \bar{x}$. Here X belongs to PSU(3, q) if and only if

$$X\bar{X}^T = I. \tag{4.5}$$

We have observed that if $q^3 + 1 = v$ has $v \equiv 1$ or 3 (mod 6) then q must be an odd power of 2. For q = 2 there is a group but it is solvable. Here $F_{q^2} = F_4$ and we take as the elements of F_4 0, 1, a, b where $a^2 = b$, $b^2 = a$, ab = 1 and b = a + 1.

In general a point (x, y, z) is isotropic if and only if

$$x\bar{x} + y\bar{y} + z\bar{z} = 0. \tag{4.6}$$

The $2^3 + 1 = 9$ isotropic points for PSU(3, 2) are

$$1 = (0, 1, 1),$$

$$2 = (1, 1, 0),$$

$$3 = (1, 0, 1),$$

$$4 = (1, a, 0),$$

$$5 = (1, 0, a),$$

$$6 = (1, b, 0),$$

$$7 = (1, 0, b),$$

$$8 = (0, 1, a),$$

$$9 = (0, 1, b).$$

(4.7)

The group PSU(3, 2) is generated by

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & a & b \\ 1 & b & a \end{bmatrix} \quad \text{and} \quad R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$
(4.8)

The involution $\tau = M^2$

$$\tau = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$
(4.9)

has the following action on the 9 points:

$$\tau = (1)(2, 3)(4, 5)(6, 7)(8, 9).$$
 (4.10)

Hence the triples containing 1 must be

The action of G on these triples gives exactly the triples of S(9) as in (3.9).

Now consider cases in which $q = 2^{2a+1} > 2$ and $v = q^3 + 1 = 2^{6a+3}$. Here τ of (4.9) is an involution in PSU(3, q). What are the fixed points of τ ?

$$(x, y, z) \tau = (x, z, y).$$
 (4.12)

If (x, z, y) = t(x, y, z) for some t, then t = 1 and y = z, (x, y, z) = (x, y, y). If this is an isotropic point, then

$$x\bar{x} + y\bar{y} + y\bar{y} = 0$$
 or $x\bar{x} = 0.$ (4.13)

But $x\bar{x}=0$ implies x=0 so that a fixed point is (0, y, y) = (0, 1, 1) = 1. Hence τ is an involution in G which has point 1 as its only fixed point. By the transitivity of G for every point x there is a unique involution α_x which has x as its only fixed point. From Theorem 3.2 every triangle of S(v)generates an S(9). But it has been shown by B. Fischer [3] that if every triangle of S(v) generates an $S(9)^2$ then $v = 3^r$, a power of 3. Hence we must have

$$q^3 + 1 = 3^r. (4.14)$$

 2 This is also a consequence of Theorem 4.5 of the author's [6]. But this approach involves the complicated theory of Moufang loops.

Here $(q+1)(q^2-q+1)=3^r$ so that $q=3^s-1$ for some s. Then $q^2-q+1=3^{2s}-3\cdot 3^s+3$. Here if s>1 $3^{2s}-3^{s+1}+3$ is not a power of 3 and so $q=2^{2a+1}>2$ is not possible. This completes all cases. Our result is

THEOREM 4.1. If a Steiner triple system S(v) has a doubly transitive automorphism group G where G has a normal subgroup H which is transitive and simple non-Abelian then S(v) is the projective space PG(d-1, 2) and G is PSL(d, 2), d > 2 on $2^d - 1$ points except for the single cases in which G is A_7 acting on the 15 points of PG(3, 2).

References

- 1. W. G. BURNSIDE, "The Theory of Groups," 2nd. ed., Cambridge Univ. Press, London/New York, 1911.
- 2. P. J. CAMERON, Finite permutation groups and finite simple groups, Bull. London Math. Soc. 13 (1981), 1-22.
- 3. B. FISCHER, Eine Kennenzeichnung der symmetrischen Gruppen von Grade 6 und 7, Math. Z. 95 (1967), 288–298.
- 4. J. I. HALL, "Steiner Triple Systems and 2-Transitive Groups," Master of Science dissertation, Oxford University, 1972.
- 5. M. HALL, JR., Automorphisms of Steiner triple systems, Proc. Sympos. Pure Math. 6 (1962), 47-66.
- M. HALL, JR., Group theory and block designs, in "Proceedings, International Conference on Theory of Groups, Australian National University, Canberra, August 1965," pp. 115-144, Gordon & Breach, New York, 1967.